

7715068



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 19, 2019

**THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS
OF:**

APPLICATION NUMBER: 10/049,101
FILING DATE: July 23, 2002
PATENT NUMBER: 7475246
ISSUE DATE: January 06, 2009



Certified by

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

10/049101

JC13 Rec'd PGT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
 Applicable through 10/31/2002. CMB 0604-0032
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2002

Patent fees are subject to annual revision.

Complete if Known

| | |
|-----------------------|------------------------|
| Application Number: | PCT/US00/21189 |
| Filing Date: | 02/08/2002 |
| First Named Inventor: | Scott Moskowitz et al. |
| Examiner Name: | |
| Group Art Unit: | |
| Attorney Docket No.: | 80408.0011 |

TOTAL AMOUNT OF PAYMENT (\$)

| METHOD OF PAYMENT | | FEE CALCULATION (continued) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---------------------------|--|-----------------|--|---------------------------|-----------------------|-----------------|----------|--------|-----------------------|-----|--------------------|--|--------------------|-----------------------------------|-----|------|---|--|---------------------------------------|-----|-----|-----|------------------|---|-----|-----|-------|-----|--|---|-----|-----|-----|-----|------------------------|--|--------------|-----|-------|------|--------|---|--|-----|-----|-----|----|--|--|-----|-----|-----|-----|---|--|-----|-----|-----|-----|--|--|-----|-------|-----|-----|---|--|-----|-------|-----|-----|--|--|-----|-----|-----|-----|------------------|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--------------------------|--|-----|-------|-----|-------|---|--|-----|-----|-----|----|----------------------------------|--|-----|-------|-----|-----|------------------------------------|--|-----|-------|-----|-----|--------------------------------|--|-----|-----|-----|-----|--------------------|--|-----|-----|-----|-----|-----------------|--|-----|-----|-----|-----|---------------------------|--|-----|----|-----|----|-------------------------------------|--|-----|-----|-----|-----|--|--|-----|----|-----|----|--|--|-----|-----|-----|-----|---|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|---|--|-----|-----|-----|-----|---|--|
| <p>1. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:</p> <p>Deposit Account Number: 50-1120</p> <p>Deposit Account Name: Wiley Rein & Fielding, LLP Floyd Chapman</p> <p><input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR 1.17 and 1.17</p> <p><input type="checkbox"/> Applicant claims ownership date: See 37 CFR 1.27</p> | | <p>3. ADDITIONAL FEES</p> <table border="1"> <thead> <tr> <th>Fee Code</th> <th>Large Entity Fee (\$)</th> <th>Small Entity Fee (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>105</td> <td>130</td> <td>205</td> <td>00</td> <td>Stoolage - late filing fee on priority</td> <td></td> </tr> <tr> <td>107</td> <td>50</td> <td>227</td> <td>25</td> <td>Surcharge - late provisional filing fee on power sheet</td> <td></td> </tr> <tr> <td>139</td> <td>130</td> <td>129</td> <td>130</td> <td>Non-English specification</td> <td></td> </tr> <tr> <td>147</td> <td>2,520</td> <td>147</td> <td>2,520</td> <td>Fee filing a request for ex parte reexamination</td> <td></td> </tr> <tr> <td>172</td> <td>920</td> <td>112</td> <td>920</td> <td>Requesting publication of SIR prior to Examiner action</td> <td></td> </tr> <tr> <td>173</td> <td>1,840</td> <td>119</td> <td>1,840</td> <td>Requesting publication of SIR after Examiner action</td> <td></td> </tr> <tr> <td>115</td> <td>110</td> <td>215</td> <td>05</td> <td>Extension for reply within first month</td> <td></td> </tr> <tr> <td>116</td> <td>400</td> <td>218</td> <td>200</td> <td>Extension for reply within second month</td> <td></td> </tr> <tr> <td>117</td> <td>920</td> <td>217</td> <td>400</td> <td>Extension for reply within third month</td> <td></td> </tr> <tr> <td>118</td> <td>1,440</td> <td>218</td> <td>720</td> <td>Extension for reply within fourth month</td> <td></td> </tr> <tr> <td>128</td> <td>1,980</td> <td>228</td> <td>980</td> <td>Extension for reply within fifth month</td> <td></td> </tr> <tr> <td>119</td> <td>320</td> <td>210</td> <td>180</td> <td>Notice of Appeal</td> <td></td> </tr> <tr> <td>120</td> <td>320</td> <td>220</td> <td>180</td> <td>Filing a brief in support of an appeal</td> <td></td> </tr> <tr> <td>121</td> <td>280</td> <td>224</td> <td>140</td> <td>Request for oral hearing</td> <td></td> </tr> <tr> <td>138</td> <td>1,510</td> <td>138</td> <td>1,510</td> <td>Petition to institute a public use proceeding</td> <td></td> </tr> <tr> <td>140</td> <td>110</td> <td>240</td> <td>55</td> <td>Petition to revive - unavoidable</td> <td></td> </tr> <tr> <td>141</td> <td>1,250</td> <td>240</td> <td>640</td> <td>Petition to revive - unintentional</td> <td></td> </tr> <tr> <td>142</td> <td>1,280</td> <td>242</td> <td>640</td> <td>Utility surcharge (to recover)</td> <td></td> </tr> <tr> <td>143</td> <td>400</td> <td>242</td> <td>230</td> <td>Division issue fee</td> <td></td> </tr> <tr> <td>144</td> <td>620</td> <td>244</td> <td>310</td> <td>Plant issue fee</td> <td></td> </tr> <tr> <td>122</td> <td>150</td> <td>122</td> <td>150</td> <td>Patents in Fee Commission</td> <td></td> </tr> <tr> <td>123</td> <td>50</td> <td>123</td> <td>50</td> <td>Processing fee under 37 CFR 1.17(g)</td> <td></td> </tr> <tr> <td>125</td> <td>180</td> <td>125</td> <td>180</td> <td>Submission of Information Disclosure Sheet</td> <td></td> </tr> <tr> <td>551</td> <td>40</td> <td>551</td> <td>40</td> <td>Financing each patent assignment per property (times number of properties)</td> <td></td> </tr> <tr> <td>145</td> <td>780</td> <td>246</td> <td>370</td> <td>Filing a submission after final rejection (37 CFR § 1.129(p))</td> <td></td> </tr> <tr> <td>146</td> <td>780</td> <td>249</td> <td>370</td> <td>For each additional invention to be examined (37 CFR § 1.129(b))</td> <td></td> </tr> <tr> <td>179</td> <td>740</td> <td>378</td> <td>370</td> <td>Request for Continued Examination (RCE)</td> <td></td> </tr> <tr> <td>169</td> <td>300</td> <td>169</td> <td>000</td> <td>Request for expedited examination of a design application</td> <td></td> </tr> </tbody> </table> | | Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | 105 | 130 | 205 | 00 | Stoolage - late filing fee on priority | | 107 | 50 | 227 | 25 | Surcharge - late provisional filing fee on power sheet | | 139 | 130 | 129 | 130 | Non-English specification | | 147 | 2,520 | 147 | 2,520 | Fee filing a request for ex parte reexamination | | 172 | 920 | 112 | 920 | Requesting publication of SIR prior to Examiner action | | 173 | 1,840 | 119 | 1,840 | Requesting publication of SIR after Examiner action | | 115 | 110 | 215 | 05 | Extension for reply within first month | | 116 | 400 | 218 | 200 | Extension for reply within second month | | 117 | 920 | 217 | 400 | Extension for reply within third month | | 118 | 1,440 | 218 | 720 | Extension for reply within fourth month | | 128 | 1,980 | 228 | 980 | Extension for reply within fifth month | | 119 | 320 | 210 | 180 | Notice of Appeal | | 120 | 320 | 220 | 180 | Filing a brief in support of an appeal | | 121 | 280 | 224 | 140 | Request for oral hearing | | 138 | 1,510 | 138 | 1,510 | Petition to institute a public use proceeding | | 140 | 110 | 240 | 55 | Petition to revive - unavoidable | | 141 | 1,250 | 240 | 640 | Petition to revive - unintentional | | 142 | 1,280 | 242 | 640 | Utility surcharge (to recover) | | 143 | 400 | 242 | 230 | Division issue fee | | 144 | 620 | 244 | 310 | Plant issue fee | | 122 | 150 | 122 | 150 | Patents in Fee Commission | | 123 | 50 | 123 | 50 | Processing fee under 37 CFR 1.17(g) | | 125 | 180 | 125 | 180 | Submission of Information Disclosure Sheet | | 551 | 40 | 551 | 40 | Financing each patent assignment per property (times number of properties) | | 145 | 780 | 246 | 370 | Filing a submission after final rejection (37 CFR § 1.129(p)) | | 146 | 780 | 249 | 370 | For each additional invention to be examined (37 CFR § 1.129(b)) | | 179 | 740 | 378 | 370 | Request for Continued Examination (RCE) | | 169 | 300 | 169 | 000 | Request for expedited examination of a design application | |
| Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 130 | 205 | 00 | Stoolage - late filing fee on priority | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 | 50 | 227 | 25 | Surcharge - late provisional filing fee on power sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 139 | 130 | 129 | 130 | Non-English specification | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 147 | 2,520 | 147 | 2,520 | Fee filing a request for ex parte reexamination | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 172 | 920 | 112 | 920 | Requesting publication of SIR prior to Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 173 | 1,840 | 119 | 1,840 | Requesting publication of SIR after Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 115 | 110 | 215 | 05 | Extension for reply within first month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 116 | 400 | 218 | 200 | Extension for reply within second month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 117 | 920 | 217 | 400 | Extension for reply within third month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 118 | 1,440 | 218 | 720 | Extension for reply within fourth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 128 | 1,980 | 228 | 980 | Extension for reply within fifth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 119 | 320 | 210 | 180 | Notice of Appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 120 | 320 | 220 | 180 | Filing a brief in support of an appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 121 | 280 | 224 | 140 | Request for oral hearing | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 138 | 1,510 | 138 | 1,510 | Petition to institute a public use proceeding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 140 | 110 | 240 | 55 | Petition to revive - unavoidable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 141 | 1,250 | 240 | 640 | Petition to revive - unintentional | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 142 | 1,280 | 242 | 640 | Utility surcharge (to recover) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 143 | 400 | 242 | 230 | Division issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 144 | 620 | 244 | 310 | Plant issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 122 | 150 | 122 | 150 | Patents in Fee Commission | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 123 | 50 | 123 | 50 | Processing fee under 37 CFR 1.17(g) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 125 | 180 | 125 | 180 | Submission of Information Disclosure Sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 551 | 40 | 551 | 40 | Financing each patent assignment per property (times number of properties) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 145 | 780 | 246 | 370 | Filing a submission after final rejection (37 CFR § 1.129(p)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 146 | 780 | 249 | 370 | For each additional invention to be examined (37 CFR § 1.129(b)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 179 | 740 | 378 | 370 | Request for Continued Examination (RCE) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169 | 300 | 169 | 000 | Request for expedited examination of a design application | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. <input type="checkbox"/> Payment Enclosed:</p> <p><input type="checkbox"/> Check <input type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other</p> | | <p>1. BASIC FILING FEE</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (E)</th> <th>Small Entity Fee Code (E)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>101</td> <td>280</td> <td>101</td> <td>170</td> <td>Utility filing fee</td> <td>370.00</td> </tr> <tr> <td>106</td> <td>350</td> <td>100</td> <td>100</td> <td>Design filing fee</td> <td></td> </tr> <tr> <td>107</td> <td>350</td> <td>107</td> <td>350</td> <td>Plant filing fee</td> <td></td> </tr> <tr> <td>108</td> <td>740</td> <td>100</td> <td>170</td> <td>Rescued filing fee</td> <td></td> </tr> <tr> <td>114</td> <td>100</td> <td>114</td> <td>00</td> <td>Provisional filing fee</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (1)</td> <td>(\$)</td> <td>370.00</td> </tr> </tbody> </table> | | Large Entity Fee Code (E) | Small Entity Fee Code (E) | Fee Description | Fee Paid | 101 | 280 | 101 | 170 | Utility filing fee | 370.00 | 106 | 350 | 100 | 100 | Design filing fee | | 107 | 350 | 107 | 350 | Plant filing fee | | 108 | 740 | 100 | 170 | Rescued filing fee | | 114 | 100 | 114 | 00 | Provisional filing fee | | SUBTOTAL (1) | | | (\$) | 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (E) | Small Entity Fee Code (E) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 101 | 280 | 101 | 170 | Utility filing fee | 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 106 | 350 | 100 | 100 | Design filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 | 350 | 107 | 350 | Plant filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 108 | 740 | 100 | 170 | Rescued filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 114 | 100 | 114 | 00 | Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (1) | | | (\$) | 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. EXTRA CLAIM FEES</p> <table border="1"> <thead> <tr> <th>Total Claims</th> <th>Extra Claims</th> <th>Fee from below</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>47</td> <td>20*</td> <td>27</td> <td>188.00</td> </tr> <tr> <td>1</td> <td>3**</td> <td>4</td> <td>168.00</td> </tr> <tr> <td colspan="3">Multiple Dependent</td> <td>0.00</td> </tr> </tbody> </table> | | Total Claims | Extra Claims | Fee from below | Fee Paid | 47 | 20* | 27 | 188.00 | 1 | 3** | 4 | 168.00 | Multiple Dependent | | | 0.00 | <p>2. SUBTOTAL (2) (\$)</p> <p>622.00</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total Claims | Extra Claims | Fee from below | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 47 | 20* | 27 | 188.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 3** | 4 | 168.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Multiple Dependent | | | 0.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Large Entity Small Entity</p> <table border="1"> <thead> <tr> <th>Fee Code (E)</th> <th>Fee Code (E)</th> <th>Fee Code (E)</th> <th>Fee Description</th> </tr> </thead> <tbody> <tr> <td>103</td> <td>78</td> <td>203</td> <td>8</td> <td>Claiming excess of 20</td> </tr> <tr> <td>102</td> <td>84</td> <td>202</td> <td>42</td> <td>Independent claims in excess of 3</td> </tr> <tr> <td>104</td> <td>290</td> <td>204</td> <td>140</td> <td>Multiple dependent claim, if not paid</td> </tr> <tr> <td>105</td> <td>84</td> <td>205</td> <td>42</td> <td>Rescued independent claims over original patent</td> </tr> <tr> <td>110</td> <td>18</td> <td>210</td> <td>9</td> <td>Remove claims in excess of 20 and over original patent</td> </tr> </tbody> </table> | | Fee Code (E) | Fee Code (E) | Fee Code (E) | Fee Description | 103 | 78 | 203 | 8 | Claiming excess of 20 | 102 | 84 | 202 | 42 | Independent claims in excess of 3 | 104 | 290 | 204 | 140 | Multiple dependent claim, if not paid | 105 | 84 | 205 | 42 | Rescued independent claims over original patent | 110 | 18 | 210 | 9 | Remove claims in excess of 20 and over original patent | <p>3. SUBTOTAL (3) (\$)</p> <p>637.00</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fee Code (E) | Fee Code (E) | Fee Code (E) | Fee Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 | 78 | 203 | 8 | Claiming excess of 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 102 | 84 | 202 | 42 | Independent claims in excess of 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 104 | 290 | 204 | 140 | Multiple dependent claim, if not paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 84 | 205 | 42 | Rescued independent claims over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 110 | 18 | 210 | 9 | Remove claims in excess of 20 and over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|-------------------|-------------------------|---------------------------------|--------------|
| SUBMITTED BY | | Complete if applicable | |
| Name (Print/Type) | Floyd B. Chapman | Registration No. (Member/Agent) | 40,555 |
| Signature | <i>Floyd B. Chapman</i> | Telephone | 202/719-7000 |
| | | Date | 02/08/2002 |

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Duration: Your Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

10/049101
 JG13 Rec'd PCT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | | |
|--|--------------------------|--------------------------------|
| FEE TRANSMITTAL for FY 2002 | Complete if Known | |
| | Application Number | PCT/US00/01189 |
| | Filing Date | 02/08/2002 |
| | First Named Inventor | Scott Moskowitz et al. |
| | Examiner Name | |
| | Group Art Unit | |
| TOTAL AMOUNT OF PAYMENT (\$) | | Attorney Docket No. 80408.0011 |

| <p>METHOD OF PAYMENT</p> <p>1. <input type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:</p> <p>Deposit Account Number: 50-1120</p> <p>Deposit Account Name: Wiley Rein & Fielding, LLP Floyd Chapman</p> <p><input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17</p> <p><input type="checkbox"/> Refund/credits (mail only state - See 37 CFR 1.27)</p> <p>2. <input checked="" type="checkbox"/> Payment Enclosed: <input type="checkbox"/> Check <input checked="" type="checkbox"/> Credit Card <input type="checkbox"/> Money Order <input type="checkbox"/> Other</p> <p style="text-align: center;">FEE CALCULATION</p> <p>1. BASIC FILING FEE</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>101 140</td> <td>301 370</td> <td>Utility filing fee</td> <td></td> </tr> <tr> <td>106 330</td> <td>206 165</td> <td>Design filing fee</td> <td></td> </tr> <tr> <td>107 510</td> <td>307 385</td> <td>Plant filing fee</td> <td></td> </tr> <tr> <td>108 740</td> <td>308 370</td> <td>Reissuance fee</td> <td></td> </tr> <tr> <td>114 160</td> <td>304 30</td> <td>Provisional filing fee</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (1) (\$)</td> <td></td> </tr> </tbody> </table> <p>2. EXTRA CLAIM FEES</p> <table border="1"> <thead> <tr> <th>Total Claims</th> <th>Extra Claims</th> <th>Fee from 100%</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>70**</td> <td>3**</td> <td>X</td> <td></td> </tr> <tr> <td>Independent Claims</td> <td>-3**</td> <td>X</td> <td></td> </tr> <tr> <td>Multiple Dependent</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>103 18</td> <td>203 9</td> <td>Claims in excess of 20</td> <td></td> </tr> <tr> <td>102 84</td> <td>202 42</td> <td>Independent claims in excess of 3</td> <td></td> </tr> <tr> <td>104 280</td> <td>204 140</td> <td>Multiple dependent claims, if not paid</td> <td></td> </tr> <tr> <td>109 84</td> <td>209 42</td> <td>** Reissue independent claims over original patent</td> <td></td> </tr> <tr> <td>110 18</td> <td>210 9</td> <td>* Reissue claims in excess of 20 over original patent</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (2) (\$)</td> <td></td> </tr> </tbody> </table> <p>*For number previously paid, if granted. For Reissues, see below.</p> | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 101 140 | 301 370 | Utility filing fee | | 106 330 | 206 165 | Design filing fee | | 107 510 | 307 385 | Plant filing fee | | 108 740 | 308 370 | Reissuance fee | | 114 160 | 304 30 | Provisional filing fee | | SUBTOTAL (1) (\$) | | | | Total Claims | Extra Claims | Fee from 100% | Fee Paid | 70** | 3** | X | | Independent Claims | -3** | X | | Multiple Dependent | | | | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 103 18 | 203 9 | Claims in excess of 20 | | 102 84 | 202 42 | Independent claims in excess of 3 | | 104 280 | 204 140 | Multiple dependent claims, if not paid | | 109 84 | 209 42 | ** Reissue independent claims over original patent | | 110 18 | 210 9 | * Reissue claims in excess of 20 over original patent | | SUBTOTAL (2) (\$) | | | | <p>3. ADDITIONAL FEES</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>105 120</td> <td>205 65</td> <td>Exchange - like filing fee or paid</td> <td></td> </tr> <tr> <td>127 80</td> <td>327 25</td> <td>Surcharge - late provisional filing fee or cover sheet</td> <td></td> </tr> <tr> <td>139 130</td> <td>139 130</td> <td>Non-English specification</td> <td></td> </tr> <tr> <td>147 2,520</td> <td>147 2,520</td> <td>For filing a request for accelerated examination</td> <td></td> </tr> <tr> <td>112 920*</td> <td>112 520*</td> <td>Requesting publication of SIR prior to Examiner action</td> <td></td> </tr> <tr> <td>113 1,840*</td> <td>113 1,840*</td> <td>Requesting publication of SIR after Examiner action</td> <td></td> </tr> <tr> <td>115 110</td> <td>215 55</td> <td>Extension for reply within first month</td> <td></td> </tr> <tr> <td>116 400</td> <td>216 200</td> <td>Extension for reply within second month</td> <td></td> </tr> <tr> <td>117 920</td> <td>217 360</td> <td>Extension for reply within third month</td> <td></td> </tr> <tr> <td>118 1,440</td> <td>218 720</td> <td>Extension for reply within fourth month</td> <td></td> </tr> <tr> <td>125 1,060</td> <td>225 980</td> <td>Extension for reply within fifth month</td> <td></td> </tr> <tr> <td>119 320</td> <td>219 160</td> <td>Notice of Appeal</td> <td></td> </tr> <tr> <td>120 320</td> <td>220 160</td> <td>Filing a brief in support of an appeal</td> <td></td> </tr> <tr> <td>121 280</td> <td>221 140</td> <td>Request for oral hearing</td> <td></td> </tr> <tr> <td>138 1,510</td> <td>138 1,510</td> <td>Petition to institute a public use proceeding</td> <td></td> </tr> <tr> <td>140 110</td> <td>240 55</td> <td>Petition to revive - allowable</td> <td></td> </tr> <tr> <td>141 1,280</td> <td>241 640</td> <td>Petition to revive - unallowable</td> <td>640.00</td> </tr> <tr> <td>142 1,280*</td> <td>242 640</td> <td>Utility issue fee (or reissue)</td> <td></td> </tr> <tr> <td>143 480</td> <td>243 240</td> <td>Design issue fee</td> <td></td> </tr> <tr> <td>144 620</td> <td>344 310</td> <td>Plant issue fee</td> <td></td> </tr> <tr> <td>122 300</td> <td>122 150</td> <td>Petitions to the Commissioner</td> <td></td> </tr> <tr> <td>129 50</td> <td>123 50</td> <td>Processing fee under 37 CFR 1.17(g)</td> <td></td> </tr> <tr> <td>126 180</td> <td>126 180</td> <td>Examination of Information Disclosure Sheet</td> <td></td> </tr> <tr> <td>581 40</td> <td>381 30</td> <td>Recording each patent assignment per property times number of properties</td> <td></td> </tr> <tr> <td>148 740</td> <td>370 370</td> <td>Filing a submission after final rejection (37 CFR § 1.129(a))</td> <td></td> </tr> <tr> <td>100 780</td> <td>349 170</td> <td>For each additional invention to be examined (37 CFR § 1.129(b))</td> <td></td> </tr> <tr> <td>170 140</td> <td>370 370</td> <td>Request for Continued Examination (RCE)</td> <td></td> </tr> <tr> <td>169 300</td> <td>169 300</td> <td>Request for expedited examination of a design application</td> <td></td> </tr> <tr> <td colspan="3">Other fee (specify)</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (3) (\$)</td> <td>640.00</td> </tr> </tbody> </table> | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 105 120 | 205 65 | Exchange - like filing fee or paid | | 127 80 | 327 25 | Surcharge - late provisional filing fee or cover sheet | | 139 130 | 139 130 | Non-English specification | | 147 2,520 | 147 2,520 | For filing a request for accelerated examination | | 112 920* | 112 520* | Requesting publication of SIR prior to Examiner action | | 113 1,840* | 113 1,840* | Requesting publication of SIR after Examiner action | | 115 110 | 215 55 | Extension for reply within first month | | 116 400 | 216 200 | Extension for reply within second month | | 117 920 | 217 360 | Extension for reply within third month | | 118 1,440 | 218 720 | Extension for reply within fourth month | | 125 1,060 | 225 980 | Extension for reply within fifth month | | 119 320 | 219 160 | Notice of Appeal | | 120 320 | 220 160 | Filing a brief in support of an appeal | | 121 280 | 221 140 | Request for oral hearing | | 138 1,510 | 138 1,510 | Petition to institute a public use proceeding | | 140 110 | 240 55 | Petition to revive - allowable | | 141 1,280 | 241 640 | Petition to revive - unallowable | 640.00 | 142 1,280* | 242 640 | Utility issue fee (or reissue) | | 143 480 | 243 240 | Design issue fee | | 144 620 | 344 310 | Plant issue fee | | 122 300 | 122 150 | Petitions to the Commissioner | | 129 50 | 123 50 | Processing fee under 37 CFR 1.17(g) | | 126 180 | 126 180 | Examination of Information Disclosure Sheet | | 581 40 | 381 30 | Recording each patent assignment per property times number of properties | | 148 740 | 370 370 | Filing a submission after final rejection (37 CFR § 1.129(a)) | | 100 780 | 349 170 | For each additional invention to be examined (37 CFR § 1.129(b)) | | 170 140 | 370 370 | Request for Continued Examination (RCE) | | 169 300 | 169 300 | Request for expedited examination of a design application | | Other fee (specify) | | | | SUBTOTAL (3) (\$) | | | 640.00 |
|---|----------------------------|--|-----------------|----------|---------|---------|--------------------|--|---------|---------|-------------------|--|---------|---------|------------------|--|---------|---------|----------------|--|---------|--------|------------------------|--|--------------------------|--|--|--|--------------|--------------|---------------|----------|------|-----|---|--|--------------------|------|---|--|--------------------|--|--|--|----------------------------|----------------------------|-----------------|----------|--------|-------|------------------------|--|--------|--------|-----------------------------------|--|---------|---------|--|--|--------|--------|--|--|--------|-------|---|--|--------------------------|--|--|--|---|----------------------------|----------------------------|-----------------|----------|---------|--------|------------------------------------|--|--------|--------|--|--|---------|---------|---------------------------|--|-----------|-----------|--|--|----------|----------|--|--|------------|------------|---|--|---------|--------|--|--|---------|---------|---|--|---------|---------|--|--|-----------|---------|---|--|-----------|---------|--|--|---------|---------|------------------|--|---------|---------|--|--|---------|---------|--------------------------|--|-----------|-----------|---|--|---------|--------|--------------------------------|--|-----------|---------|----------------------------------|--------|------------|---------|--------------------------------|--|---------|---------|------------------|--|---------|---------|-----------------|--|---------|---------|-------------------------------|--|--------|--------|-------------------------------------|--|---------|---------|---|--|--------|--------|--|--|---------|---------|---|--|---------|---------|--|--|---------|---------|---|--|---------|---------|---|--|---------------------|--|--|--|--------------------------|--|--|--------|
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 101 140 | 301 370 | Utility filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 106 330 | 206 165 | Design filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 510 | 307 385 | Plant filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 108 740 | 308 370 | Reissuance fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 114 160 | 304 30 | Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (1) (\$) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total Claims | Extra Claims | Fee from 100% | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70** | 3** | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Independent Claims | -3** | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Multiple Dependent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 18 | 203 9 | Claims in excess of 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 102 84 | 202 42 | Independent claims in excess of 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 104 280 | 204 140 | Multiple dependent claims, if not paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 109 84 | 209 42 | ** Reissue independent claims over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 110 18 | 210 9 | * Reissue claims in excess of 20 over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (2) (\$) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 120 | 205 65 | Exchange - like filing fee or paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 127 80 | 327 25 | Surcharge - late provisional filing fee or cover sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 139 130 | 139 130 | Non-English specification | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 147 2,520 | 147 2,520 | For filing a request for accelerated examination | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 112 920* | 112 520* | Requesting publication of SIR prior to Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 113 1,840* | 113 1,840* | Requesting publication of SIR after Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 115 110 | 215 55 | Extension for reply within first month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 116 400 | 216 200 | Extension for reply within second month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 117 920 | 217 360 | Extension for reply within third month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 118 1,440 | 218 720 | Extension for reply within fourth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 125 1,060 | 225 980 | Extension for reply within fifth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 119 320 | 219 160 | Notice of Appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 120 320 | 220 160 | Filing a brief in support of an appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 121 280 | 221 140 | Request for oral hearing | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 138 1,510 | 138 1,510 | Petition to institute a public use proceeding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 140 110 | 240 55 | Petition to revive - allowable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 141 1,280 | 241 640 | Petition to revive - unallowable | 640.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 142 1,280* | 242 640 | Utility issue fee (or reissue) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 143 480 | 243 240 | Design issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 144 620 | 344 310 | Plant issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 122 300 | 122 150 | Petitions to the Commissioner | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 129 50 | 123 50 | Processing fee under 37 CFR 1.17(g) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 126 180 | 126 180 | Examination of Information Disclosure Sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 581 40 | 381 30 | Recording each patent assignment per property times number of properties | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 148 740 | 370 370 | Filing a submission after final rejection (37 CFR § 1.129(a)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 100 780 | 349 170 | For each additional invention to be examined (37 CFR § 1.129(b)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 170 140 | 370 370 | Request for Continued Examination (RCE) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169 300 | 169 300 | Request for expedited examination of a design application | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Other fee (specify) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (3) (\$) | | | 640.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|---------------------|-------------------------|-----------------------------------|--------------|
| SUBMITTED BY | | Complete if applicable | |
| Name (Print/Type) | Floyd B. Chapman | Registration No. (Attorney/Agent) | 40,555 |
| Signature | <i>Floyd B. Chapman</i> | Telephone | 202/719-7000 |
| | | Date | 02/08/2002 |

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2838.

Bestand Hour Statement: This form is estimated to take 3-7 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

DUPLICATE

Attorney Docket No.: 80408.0011

ASSIGNMENT FOR PATENT APPLICATION

WHEREAS, WE, Scott A. Moskowitz whose address is 16711 Collins Avenue, #2505, Miami, Florida 33160 and Michael Berry whose address is 12401 Princess Jeanne, Albuquerque, New Mexico 87112 have invented a new and useful invention and improvements to the subject matter of:

A SECURE PERSONAL CONTENT SERVER

described in an application for United States Letters Patent filed on **February 4, 2002**, and accorded Application No. **10/049,101**;

AND, WHEREAS, **Blue Spike**, a corporation organized under the laws of the State of Florida, having a place of business located at **16711 Collins Avenue, #2505, Miami, FL 33160** (hereinafter "ASSIGNEE"), is desirous of acquiring certain rights to said invention and under the applications, which corresponds to International Application No. PCT/US00/21189, which claims priority to U.S. Provisional Application No. 60/213,489 filed June 23, 2000, which claims priority to U.S. Provisional Application No. 60/147,134 filed August 4, 1999;

NOW, THEREFORE, in consideration of the sum of One Dollar (\$1.00) or the equivalent thereof, and other good and valuable consideration, receipt of which is hereby acknowledged, we do hereby sell, assign and transfer unto said ASSIGNEE, its successors, assigns and legal representatives, our entire right, title and interest in and throughout the United States of America (including its territories and dependencies) and all countries foreign thereto in and to said invention and improvements, said United States application, any other United States applications, including provisional, divisional, renewal, substitute, continuation, reexamination and reissue applications, based in whole or in part on said United States application or in whole or in part on said invention and improvements, any foreign applications, including international and regional applications, based in whole or in part on any of the aforesaid United States applications or in whole or in part on said invention and improvements, and in and to any and all letters patent, including extensions thereof, of any country which have been or may be granted on any of the aforesaid applications or on said invention and improvements or any parts thereof;

AND WE hereby authorize, **Wiley Rein & Fielding LLP**, whose address is **1776 K Street, NW, Washington, D.C., 20006**, to insert hereon any identification necessary or desirable for recordation of this document, including the filing date and application number of said application when known;

AND WE hereby agree for ourselves and our heirs, executors and administrators to execute without further consideration any further documents and instruments which may be necessary, lawful and proper in the prosecution of said above-referenced applications or in the preparation or prosecution of any continuing, substitute, divisional, renewal, reexamination or reissue application or in any amendments, extensions or interference proceedings, that may be necessary to secure to ASSIGNEE its interest and title in and to said invention or any parts thereof, and in and to said several patents or any of them;

WILEY REIN & FIELDING LLP
1776 K STREET, N.W.
WASHINGTON, D.C. 20006
202.719.7000 (TELEPHONE) 202.719.7000 (FACSIMILE)

DUPLICATE

Attorney Docket No: 80408.0011

AND WE hereby covenant for ourselves and our legal representatives, and agree with said ASSIGNEE, its successors and assigns, that we have granted no right or license to make, use, sell or offer to sell said invention, to anyone except said ASSIGNEE, that prior to the execution of this deed, our right, title and interest in said invention has not been otherwise encumbered, and that we have not and will not execute any instrument in conflict therewith;

AND WE do hereby authorize and request the United States Commissioner for Patents to issue any and all letters patent, which may be granted upon said United States applications, or upon said invention or any parts thereof when granted, to said ASSIGNEE.

IN WITNESS WHEREOF, we have hereunto set our hands and seals.

Date

SCOTT A. MOSKOWITZ

6/29/02

Date



MICHAEL BERRY

County of _____)
State of _____)

On this _____ day of _____, 2002, before me a Notary Public in and for the County and State aforesaid, personally appeared SCOTT A. MOSKOWITZ, who is personally known to me or who produced _____ as identification, and who signed and sealed the foregoing instrument, and acknowledged the same to be of his free act and deed.

(Seal)

Notary Public:
My Commission Expires: _____

.....
County of _____)
State of _____)

On this _____ day of _____, 2002, before me a Notary Public in and for the County and State aforesaid, personally appeared MICHAEL BERRY, who is personally known to me or who produced _____ as identification, and who signed and sealed the foregoing instrument, and acknowledged the same to be of his free act and deed.

(Seal)

Notary Public:
My Commission Expires: _____

WILEY BEHN & FELDING LLP
1776 K STREET, N.W.
WASHINGTON, D.C. 20006
202.719.7000 (TELEPHONE) 202.719.7049 (FACSIMILE)

DUPLICATE

Attorney Docket No.: 00408.0011

ASSIGNMENT FOR PATENT APPLICATION

WHEREAS, WE, Scott A. Moskowitz whose address is 16711 Collins Avenue, #2505, Miami, Florida 33160 and Michael Berry whose address is 12401 Princess Jeanne, Albuquerque, New Mexico 87112 have invented a new and useful invention and improvements to the subject matter of:

A SECURE PERSONAL CONTENT SERVER

described in an application for United States Letters Patent filed on **February 4, 2002**, and accorded Application No. **10/049,101**;

AND, WHEREAS, **Blue Spike**, a corporation organized under the laws of the State of Florida, having a place of business located at **16711 Collins Avenue, #2505, Miami, FL 33160** (hereinafter "ASSIGNEE"), is desirous of acquiring certain rights to said invention and under the applications, which corresponds to International Application No. PCT/US00/21189, which claims priority to U.S. Provisional Application No. 60/213,489 filed June 23, 2000, which claims priority to U.S. Provisional Application No. 60/147,134 filed August 4, 1999;

NOW, THEREFORE, in consideration of the sum of One Dollar (\$1.00) or the equivalent thereof, and other good and valuable consideration, receipt of which is hereby acknowledged, we do hereby sell, assign and transfer unto said ASSIGNEE, its successors, assigns and legal representatives, our entire right, title and interest in and throughout the United States of America (including its territories and dependencies) and all countries foreign thereto in and to said invention and improvements, said United States application, any other United States applications, including provisional, divisional, renewal, substitute, continuation, reexamination and reissue applications, based in whole or in part on said United States application or in whole or in part on said invention and improvements, any foreign applications, including international and regional applications, based in whole or in part on any of the aforesaid United States applications or in whole or in part on said invention and improvements, and in and to any and all letters patent, including extensions thereof, of any country which have been or may be granted on any of the aforesaid applications or on said invention and improvements or any parts thereof;

AND WE hereby authorize, **Wiley Rein & Fielding LLP**, whose address is **1776 K Street, NW, Washington, D.C., 20006**, to insert hereon any identification necessary or desirable for recordation of this document, including the filing date and application number of said application when known;

AND WE hereby agree for ourselves and our heirs, executors and administrators to execute without further consideration any further documents and instruments which may be necessary, lawful and proper in the prosecution of said above-referenced applications or in the preparation or prosecution of any continuing, substitute, divisional, renewal, reexamination or reissue application or in any amendments, extensions or interference proceedings, that may be necessary to secure to ASSIGNEE its interest and title in and to said invention or any parts thereof, and in and to said several patents or any of them;

WILEY REIN & FIELDING LLP
1776 K STREET, N.W.
WASHINGTON, D.C. 20006
202.778.7000 (TELEPHONE) 202.778.7049 (FACSIMILE)

DUPLICATE

Attorney Docket No: 80408.0011

AND WE hereby covenant for ourselves and our legal representatives, and agree with said ASSIGNEE, its successors and assigns, that we have granted no right or license to make, use, sell or offer to sell said invention, to anyone except said ASSIGNEE, that prior to the execution of this deed, our right, title and interest in said invention has not been otherwise encumbered, and that we have not and will not execute any instrument in conflict therewith;

AND WE do hereby authorize and request the United States Commissioner for Patents to issue any and all letters patent, which may be granted upon said United States applications, or upon said invention or any parts thereof when granted, to said ASSIGNEE.

IN WITNESS WHEREOF, we have hereunto set our hands and seals.

7/19/02
Date

Scott A. Moskowitz
SCOTT A. MOSKOWITZ

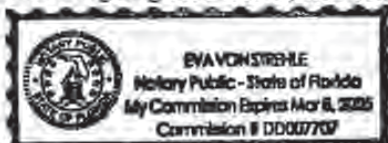
Date

MICHAEL BERRY

County of DADE)
State of FLORIDA)

On this 19 day of JULY, 2002, before me a Notary Public in and for the County and State aforesaid, personally appeared SCOTT A. MOSKOWITZ, who is personally known to me or who produced FL DL as identification, and who signed and sealed the foregoing instrument, and acknowledged the same to be of his free act and deed.

(Seal)



Evon Strehle
Notary Public:
My Commission Expires: _____

County of _____)
State of _____)

On this _____ day of _____, 2002, before me a Notary Public in and for the County and State aforesaid, personally appeared MICHAEL BERRY, who is personally known to me or who produced _____ as identification, and who signed and sealed the foregoing instrument, and acknowledged the same to be of his free act and deed.

(Seal)

Notary Public:
My Commission Expires: _____

PATENT APPLICATION SERIAL NO. 10/049101

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

02/12/2002 NGUYEN 00000131 501129 10049101

| | |
|-----------|-----------|
| 02 FC:959 | 370.00 CH |
| 03 FC:967 | 99.00 CH |
| 04 FC:965 | 168.00 CH |

PTO-1556
(5/87)

*U.S. GPO: 2000-468-987/39595

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 2001

Application or Docket Number

10/049101

CLAIMS AS FILED - PART I

| | (Column 1) | (Column 2) |
|----------------------------------|--------------------------|--------------|
| TOTAL CLAIMS | | |
| FOR | NUMBER FILED | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS | 30 minus 20 = * | 10 |
| INDEPENDENT CLAIMS | 7 minus 3 = * | 4 |
| MULTIPLE DEPENDENT CLAIM PRESENT | <input type="checkbox"/> | |

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE OR

OTHER THAN SMALL ENTITY

| RATE | FEE | OR | RATE | FEE |
|-----------|-----|----|-----------|-----|
| BASIC FEE | 370 | OR | BASIC FEE | |
| X\$ 9= | 90 | OR | X\$18= | |
| X42= | 168 | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL | 628 | OR | TOTAL | |

CLAIMS AS AMENDED - PART II

| | (Column 1) | (Column 2) | (Column 3) |
|-------------|---|------------------------------------|---------------|
| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | Minus ** | = |
| | Independent | Minus *** | = |
| | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | |

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| | (Column 1) | (Column 2) | (Column 3) |
|-------------|---|------------------------------------|---------------|
| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | Minus ** | = |
| | Independent | Minus *** | = |
| | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| | (Column 1) | (Column 2) | (Column 3) |
|-------------|---|------------------------------------|---------------|
| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | Minus ** | = |
| | Independent | Minus *** | = |
| | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Best Available Copy

*Check & Box
Dependent Specimens*

**MULTIPLE DEPENDENT CLAIM
FEE CALCULATION SHEET
(FOR USE WITH P.O. FORM TO-976)**

SERIAL NO. 10/049101 FILING DATE _____
 APPLICANT(S) _____

| CLAIMS | | | | | | | | | | |
|--------------|----------|------|---------------------|------|---------------------|------|---|---|---|------|
| | AS FILED | | AFTER 1st AMENDMENT | | AFTER 2nd AMENDMENT | | 1 | 2 | 3 | |
| | IND. | DEP. | IND. | DEP. | IND. | DEP. | | | | IND. |
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |
| 5 | | | | | | | | | | |
| 6 | | | | | | | | | | |
| 7 | | | | | | | | | | |
| 8 | | | | | | | | | | |
| 9 | | | | | | | | | | |
| 10 | | | | | | | | | | |
| 11 | | | | | | | | | | |
| 12 | | | | | | | | | | |
| 13 | | | | | | | | | | |
| 14 | | | | | | | | | | |
| 15 | | | | | | | | | | |
| 16 | | | | | | | | | | |
| 17 | | | | | | | | | | |
| 18 | | | | | | | | | | |
| 19 | | | | | | | | | | |
| 20 | | | | | | | | | | |
| 21 | | | | | | | | | | |
| 22 | | | | | | | | | | |
| 23 | | | | | | | | | | |
| 24 | | | | | | | | | | |
| 25 | | | | | | | | | | |
| 26 | | | | | | | | | | |
| 27 | | | | | | | | | | |
| 28 | | | | | | | | | | |
| 29 | | | | | | | | | | |
| 30 | | | | | | | | | | |
| 31 | | | | | | | | | | |
| 32 | | | | | | | | | | |
| 33 | | | | | | | | | | |
| 34 | | | | | | | | | | |
| 35 | | | | | | | | | | |
| 36 | | | | | | | | | | |
| 37 | | | | | | | | | | |
| 38 | | | | | | | | | | |
| 39 | | | | | | | | | | |
| 40 | | | | | | | | | | |
| 41 | | | | | | | | | | |
| 42 | | | | | | | | | | |
| 43 | | | | | | | | | | |
| 44 | | | | | | | | | | |
| 45 | | | | | | | | | | |
| 46 | | | | | | | | | | |
| 47 | | | | | | | | | | |
| 48 | | | | | | | | | | |
| 49 | | | | | | | | | | |
| 50 | | | | | | | | | | |
| 51 | | | | | | | | | | |
| 52 | | | | | | | | | | |
| 53 | | | | | | | | | | |
| 54 | | | | | | | | | | |
| 55 | | | | | | | | | | |
| 56 | | | | | | | | | | |
| 57 | | | | | | | | | | |
| 58 | | | | | | | | | | |
| 59 | | | | | | | | | | |
| 60 | | | | | | | | | | |
| 61 | | | | | | | | | | |
| 62 | | | | | | | | | | |
| 63 | | | | | | | | | | |
| 64 | | | | | | | | | | |
| 65 | | | | | | | | | | |
| 66 | | | | | | | | | | |
| 67 | | | | | | | | | | |
| 68 | | | | | | | | | | |
| 69 | | | | | | | | | | |
| 70 | | | | | | | | | | |
| 71 | | | | | | | | | | |
| 72 | | | | | | | | | | |
| 73 | | | | | | | | | | |
| 74 | | | | | | | | | | |
| 75 | | | | | | | | | | |
| 76 | | | | | | | | | | |
| 77 | | | | | | | | | | |
| 78 | | | | | | | | | | |
| 79 | | | | | | | | | | |
| 80 | | | | | | | | | | |
| 81 | | | | | | | | | | |
| 82 | | | | | | | | | | |
| 83 | | | | | | | | | | |
| 84 | | | | | | | | | | |
| 85 | | | | | | | | | | |
| 86 | | | | | | | | | | |
| 87 | | | | | | | | | | |
| 88 | | | | | | | | | | |
| 89 | | | | | | | | | | |
| 90 | | | | | | | | | | |
| 91 | | | | | | | | | | |
| 92 | | | | | | | | | | |
| 93 | | | | | | | | | | |
| 94 | | | | | | | | | | |
| 95 | | | | | | | | | | |
| 96 | | | | | | | | | | |
| 97 | | | | | | | | | | |
| 98 | | | | | | | | | | |
| 99 | | | | | | | | | | |
| 100 | | | | | | | | | | |
| TOTAL IND. | 7 | | | | | | | | | |
| TOTAL DEP. | 123 | | | | | | | | | |
| TOTAL CLAIMS | 130 | | | | | | | | | |

Best Available Copy

#2

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | |
|---|--|
| PETITION FOR REVIVAL OF AN INTERNATIONAL APPLICATION FOR PATENT DESIGNATING THE U.S. ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(b) | Docket Number (Optional) 80408.0011 |
| <p>First named inventor: Scott A. MOSKOWITZ et al.</p> <p>International (PCT) Application No.: PCT/US00/21189 U.S. Application No.: (if known)</p> <p>Filed: August 4, 2000</p> <p>Title: A SECURE PERSONAL CONTENT SERVER</p> <p>Attention: PCT Legal Staff Attn: Boris Milaf Box PCT Assistant Commissioner for Patents Washington, D.C. 20231</p> | |
| <p>RECEIVED</p> <p>15 APR 2002</p> <p>Legal Staff International Division</p> | |
| <p>The above-identified application became abandoned as to the United States because the fees and documents required by 35 U.S.C. 371(c) were not filed prior to the expiration of the time set in 37 CFR 1.494(b) or (c) or 1.495(b) or (c) as applicable. The date of abandonment is the day after the date on which the 35 U.S.C. 371(c) requirements were due. See 37 CFR 1.494(g) or 1.495(h).</p> | |
| <p>APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION</p> | |
| <p>NOTE: A grantable petition requires the following items:</p> <ol style="list-style-type: none"> (1) Petition fee (2) Proper reply (3) Terminal disclaimer with disclaimer fee--required for all international applications having an international filing date before June 8, 1995; and (4) Statement that the entire delay was unintentional. | |
| <p>1. Petition fee</p> <p><input checked="" type="checkbox"/> Small entity - fee \$ <u>640.00</u> (37 CFR 1.17(m)). Applicant claims small entity status. See 37 CFR 1.27.</p> <p><input type="checkbox"/> Other than small entity - fee \$ _____ (37 CFR 1.17(m))</p> | |
| <p>2. Proper reply</p> <p>A. The proper reply (the missing 35 U.S.C. 371(c) requirement(s) in the form of <u>Request to enter National Stage under 371, filing fee and copy of appln.</u> (identify type of reply):</p> <p><input type="checkbox"/> has been filed previously on _____</p> <p><input checked="" type="checkbox"/> is enclosed herewith.</p> | |

(Page 1 of 2)

Burden Hour Statement: This form is estimated to take 1.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

02/12/2002 HNGUYEN 00000131 501129 10049101

01 FC:241

640.00 0P

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

3. Terminal disclaimer with disclaimer fee

- Since this international application has an international filing date on or after June 8, 1995, no terminal disclaimer is required.
- A terminal disclaimer (and disclaimer fee (37 CFR 1.20(d)) of \$_____ for a small entity or \$_____ for other than a small entity) disclaiming the required period of time is enclosed herewith (see PTO/SB/63).

4. Statement. The entire delay in filing the required reply from the due date for the required reply until the filing of a grantable petition under 37 CFR 1.137(b) was unintentional.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

February 8, 2002
Date

Floyd B. Chapman
Signature

Floyd B. Chapman
Typed or printed name

Telephone
Number: (202) 719-7000

Wiley Rien & Fielding, LLP
Address
1776 K Street, N.W., Washington, D.C.

- Enclosures: Response
 Fee Payment
 Terminal Disclaimer Form
 Credit Card Payment Form

DOCKETED

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
CHAPMAN, Floyd, B.
Baker Botts, LLP
The Warner
1299 Pennsylvania Avenue, N.W.
Washington, DC 20004
ETATS-UNIS D'AMERIQUE

RECEIVED
APR 06 2001
BROBECK

| | | | |
|---|---|---|--|
| Date of mailing (day/month/year) 15 March 2001 (15.03.01) | | IMPORTANT NOTICE | |
| Applicant's or agent's file reference 066112.0139 031838.0013 | | | |
| International application No. PCT/US00/21189 | International filing date (day/month/year) 04 August 2000 (04.08.00) | Priority date (day/month/year) 04 August 1999 (04.08.99) | |
| Applicant BLUE SPIKE, INC. et al | | | |

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
EP,JP

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 15 March 2001 (15.03.01) under No. WO 01/18628

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

| | |
|---|--|
| <p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No. (41-22) 740.14.35</p> | <p>Authorized officer J. Zahra</p> <p>Telephone No. (41-22) 338.83.38</p> |
|---|--|

PCT PATENT APPLICATION

Application No.: PCT/US00/21189 Date: March 2, 2001
Client/Matter No.: 031838.0013 Client: Blue Spike, Inc.
Inventor(s): Scott Moskowitz et al. Atty/Sec.: FBC/KLL/eab

Title: A SECURE PERSONAL CONTENT SERVER

**The following has been received in the U.S. Patent and Trademark Office
on the date stamped hereon:**

- PCT CHAPTER II DEMAND AND FEE CALCULATION SHEET
- Charged Deposit Account in the amount of \$627.00

DOCKETED



The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ US

PCT DEMAND

CHAPTER II

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

| | | |
|---|--|---|
| For International Preliminary Examining Authority use only | | |
| Identification of IPEA | | Date of receipt of DEMAND |
| Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION | | Applicant's or agent's file reference |
| | | 031838.0013 |
| International application No. | International filing date (day/month/year) | (Earliest) Priority date (day/month/year) |
| PCT/US00/21189 | 4 August 2000 | 4 August 1999 |
| Title of invention | | |
| A SECURE PERSONAL CONTENT SERVER | | |
| Box No. II APPLICANT(S) | | |
| Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)</i> | | Telephone No.: |
| Blue Spike, Inc. 16711 Collins Avenue, #2505 Miami, Florida 33160 USA | | Facsimile No.: |
| | | Telex No.: |
| | | |
| State (that is, country) of nationality: | | State (that is, country) of residence: |
| US | | US |
| Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)</i> | | |
| Scott A. Moskowitz 16711 Collins Avenue, #2505 Miami, Florida 33160 USA | | |
| State (that is, country) of nationality: | | State (that is, country) of residence: |
| US | | US |
| Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)</i> | | |
| Michael Berry 12401 Princess Jeanne Albuquerque, New Mexico 87112 USA | | |
| State (that is, country) of nationality: | | State (that is, country) of residence: |
| US | | US |
| <input type="checkbox"/> Further applicants are indicated on a continuation sheet. | | |

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

- The following person is agent common representative
- and has been appointed earlier and represents the applicant(s) also for international preliminary examination.
- is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.
- is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

Floyd B. Chapman
Intellectual Property Department
Brobeck, Phleger & Harrison LLP
1333 H Street, N.W., Suite 800
Washington, D.C. 20005, US

Telephone No.:

202-220-6000

Facsimile No.:

202-220-5200

Teleprinter No.:

- Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION**Statement concerning amendments:***

1. The applicant wishes the international preliminary examination to start on the basis of:

- the international application as originally filed
- the description as originally filed
 as amended under Article 34
- the claims as originally filed
 as amended under Article 19 (together with any accompanying statement)
 as amended under Article 34
- the drawings as originally filed
 as amended under Article 34
2. The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.
3. The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examinations: ENGLISH

- which is the language in which the international application was filed.
- which is the language of a translation furnished for the purposes of international search.
- which is the language of publication of the international application.
- which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby elects all eligible States *(that is, all States which have been designated and which are bound by Chapter II of the PCT)* excluding the following States which the applicant wishes not to elect:

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- | | |
|--|--------|
| 1. translation of international application | sheets |
| 2. amendments under Article 34 | sheets |
| 3. copy (or, where required, translation) of amendments under Article 19 | sheets |
| 4. copy (or, where required, translation) of statement under Article 19 | sheets |
| 5. letter | sheets |
| 6. other (specify) | sheets |

For International Preliminary Examining Authority use only

| received | not received |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |

The demand is also accompanied by the item(s) marked below:

- | | |
|--|---|
| 1. <input checked="" type="checkbox"/> fee calculation sheet | 4. <input type="checkbox"/> statement explaining lack of signature |
| 2. <input type="checkbox"/> separate signed power of attorney | 5. <input type="checkbox"/> nucleotide and/or amino acid sequence listing in computer readable form |
| 3. <input type="checkbox"/> copy of general power of attorney, reference number, if any. | 6. <input type="checkbox"/> other (specify): |

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

By: Floyd B. Chapman
Floyd B. Chapman, Agent for Applicants

For International Preliminary Examining Authority use only

- Date of actual receipt of DEMAND:
- Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
- The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. The applicant has been informed accordingly.
- The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
- Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

PCT

FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

| | | | |
|---|--|--------|--------------|
| International application No. PCT/US00/21189 | For International Preliminary Examining Authority use only Date Stamp of the IPEA | | |
| Applicant's or agent's file reference 031838.0013 | | | |
| Applicant BLUE SPIKE, INC. | | | |
| Calculation of prescribed fees | | | |
| 1. Preliminary examination fee | 490.00 P | | |
| 2. Handling fee (<i>Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.</i>) | 137.00 H | | |
| 3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box | <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">627.00</td> </tr> <tr> <td style="text-align: center;">TOTAL</td> </tr> </table> | 627.00 | TOTAL |
| 627.00 | | | |
| TOTAL | | | |
| Mode of Payment | | | |
| <input checked="" type="checkbox"/> authorization to charge deposit account with the IPEA (see below) | <input type="checkbox"/> cash | | |
| <input type="checkbox"/> cheque | <input type="checkbox"/> revenue stamps | | |
| <input type="checkbox"/> postal money order | <input type="checkbox"/> coupons | | |
| <input type="checkbox"/> bank draft | <input type="checkbox"/> other (specify) | | |
| Deposit Account Authorization (<i>this mode of payment may not be available at all IPEAs</i>) | | | |
| The IPEA/ US | <input checked="" type="checkbox"/> is hereby authorized to charge the total fees indicated above to my deposit account. | | |
| | <input checked="" type="checkbox"/> (<i>this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit</i>) is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account. | | |
| _____ Deposit Account Number | _____ Date (day/month/year) | | |
| | _____ Signature Floyd B. Chapman | | |

Form PCT/IPEA/401 (Annex) (July 1998; reprint July 2000)

See Notes to the fee calculation sheet

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
15 March 2001 (15.03.2001)

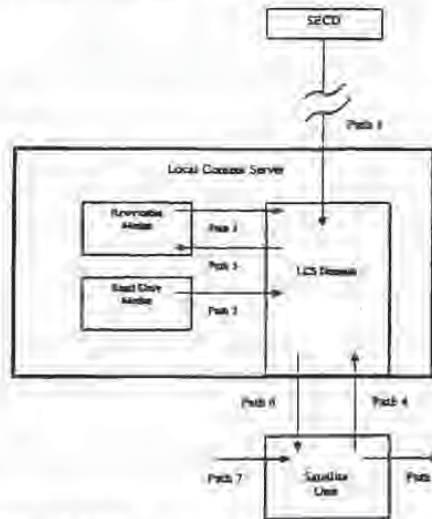
PCT

(10) International Publication Number
WO 01/18628 A2

- (51) International Patent Classification: G06F
- (72) Inventors: and
- (75) Inventors/Applicants (for US only): MOSKOWITZ, Scott, A. (US/US); 16711 Collins Avenue #2505, Miami, FL 33160 (US). BERRY, Michael (US/US); 12401 Princess Jeanne, Albuquerque, NM 87112 (US).
- (21) International Application Number: PCT/US00/21189
- (74) Agents: CHAPMAN, Floyd, B. et al.: Baker Bots, LLP, The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).
- (22) International Filing Date: 4 August 2000 (04.08.2000)
- (81) Designated States (national): JP, US.
- (25) Filing Language: English
- (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- (26) Publication Language: English
- (30) Priority Data:
 - 60/147,134 4 August 1999 (04.08.1999) US
 - 60/213,489 23 June 2000 (23.06.2000) US
- (71) Applicant (for all designated States except US): BLUE SPIKE, INC. (US/US); 16711 Collins Avenue #2505, Miami, FL 33160 (US).
- Published:
 - Without international search report and to be republished upon receipt of that report.

(Continued on next page)

(54) Title: A SECURE PERSONAL CONTENT SERVER



(57) Abstract: A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS, and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected.

(Continued on next page)

WO 01/18628 A2



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

to the system through the interface, which SUs are capable of receiving and transmitting digital content; at least one SU; and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit. A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.



A SECURE PERSONAL CONTENT SERVER

Field of Invention

The present invention relates to the secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to
5 make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security.

Authentication, verification and authorization are all handled with a combination of cryptographic and steganographic protocols to achieve efficient, trusted, secure exchange of digital information.

Cross-Reference To Related Application

This application is based on and claims the benefit of pending U.S. Patent Application Serial No. 60/147,134, filed 08/04/99, entitled, "A Secure Personal Content Server" and pending U.S. Patent Application Serial No. 60/213,489, filed
10 06/23/2000, entitled "A Secure Personal Content Server."

This application also incorporates by reference the following applications:
15 pending U.S. Patent Application Serial No. 08/999,766, filed 7/23/97, entitled "Steganographic Method and Device"; pending U.S. Patent Application Serial No. 08/772,222, filed 12/20/96, entitled "Z-Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 09/456,319, filed
20 12/08/99, entitled "Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 08/674,726, filed 7/2/96, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management"; pending U.S. Patent Application Serial No. 09/545,589, filed 04/07/2000, entitled "Method and System
25 for Digital Watermarking"; pending U.S. Patent Application Serial No. 09/046,627, filed 3/24/98, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed 04/02/98, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No.
30 09/281,279, filed 3/30/99, entitled "Optimization Methods for the Insertion, Protection, and Detection..."; U.S. Patent Application Serial No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and

Cryptographic Systems" (which is a continuation-in-part of PCT application No. PCT/US00/06522, filed 14 March 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed 24 March 1999); and pending U.S. Application No. 60/169,274, filed 12/7/99, entitled "Systems, Methods And Devices For Trusted Transactions." All of the patent applications previously identified in this paragraph are hereby incorporated by reference, in their entireties.

Background of the Invention

The music industry is at a critical inflection point. Digital technology enables anyone to make perfect replica copies of musical recordings from the comfort of their home, or as in some circumstances, in an offshore factory. Internet technology enables anyone to distribute these copies to their friends, or the entire world. Indeed, virtually any popular recording is already likely available in the MP3 format, for free if you know where to look.

How the industry will respond to these challenges and protect the rights and livelihoods of copyright owners and managers and has been a matter of increasing discussion, both in private industry forums and the public media. Security disasters like the cracking of DVD-Video's CSS security system have increased doubt about the potential for effective robust security implementations. Meanwhile, the success of non-secure initiatives such as portable MP3 players lead many to believe that these decisions may have already been made.

Music consumers have grown accustomed to copying their music for their own personal use. This fact of life was written into law in the United States via the Audio Home Recording Act of 1992. Millions of consumers have CD players and purchase music in the Compact Disc format. It is expected to take years for a format transition away from Red Book CD Audio to reach significant market penetration.

Hence, a need exists for a new and improved system for protecting digital content against unauthorized copying and distribution.

Summary of the Invention

A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a

plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, which SUs are capable of receiving and transmitting digital content; at least one SU; and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit.

A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably be embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.

Another embodiment of the method of the present invention comprises: connecting a Satellite Unit to an local content server (LCS), sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU; analyzing the message to confirm that the SU is authorized to use the LCS; retrieving a copy of the

requested content data set; assessing whether a secured connection exists between the LCS and the SU; if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and delivering
5 the content data set to the SU for its use.

The SU may also request information that is located not on the LCS, but on an SECD, in which case, the LCS will request and obtain a copy from the SECD, provided the requesting SU is authorized to access the information.

Digital technology offers economies of scale to value-added data not
10 possible with physical or tangible media distribution. The ability to digitize information both reduces the cost of copying and enables perfect copies. This is an advantage and a disadvantage to commercial publishers who must weigh the cost reduction against the real threat of unauthorized duplication of their value-added data content. Because cost reduction is an important business consideration,
15 securing payment and authenticating individual copies of digital information (such as media content) presents unique opportunities to information service and media content providers. The present invention seeks to leverage the benefits of digital distribution to consumers and publishers alike, while ensuring the development and persistence of trust between all parties, as well as with any third parties involved,
20 directly or indirectly, in a given transaction.

In another approach that is related to this goal, there are instances where transactions must be allowed to happen after perceptually-based digital information can be authenticated. (Perceptually based information is information whose value is in large part, based upon its ability to be perceived by a human, and includes for
25 example, acoustic, psychoacoustic, visual and psychovisual information.) The process of authenticating before distributing will become increasingly important for areas where the distributed material is related to a trust-requiring transaction event. A number of examples exist. These include virtual retailers (for example, an on-line music store selling CDs and electronic versions of songs); service providers (for
30 example, an on-line bank or broker who performs transactions on behalf of a consumer); and transaction providers (for example, wholesalers or auction houses). These parties have different authentication interests and requirements. By using the

teachings of this application, these interests and requirements may be separated and then independently quantified by market participants in shorter periods of time.

All parties in a transaction must authenticate information that is perceptually observable before trust between the parties can be established. In today's world, information (including perceptually rich information) is typically digitized, and as a result, can easily be copied and redistributed, negatively impacting buyers, sellers and other market participants. Unauthorized redistribution confuses authenticity, non-repudiation, limit of ability and other important "transaction events." In a networked environment, transactions and interactions occur over a transmission line or a network, with buyer and seller at different points on the line or network. While such electronic transactions have the potential to add value to the underlying information being bought and sold (and the potential to reduce the cost of the transaction), instantaneous piracy can significantly reduce the value of the underlying data, if not wholly destroy it. Even the threat of piracy tends to undermine the value of the data that might otherwise exist for such an electronic transaction.

Related situations range from the ability to provably establish the "existence" of a virtual financial institution to determining the reliability of an "electronic stamp." The present invention seeks to improve on the prior art by describing optimal combinations of cryptographic and steganographic protocols for "trusted" verification, confidence and non-repudiation of digitized representations of perceptually rich information of the actual seller, vendor or other associated institutions which may not be commercial in nature (confidence building with logo's such as the SEC, FDIC, Federal Reserve, FBI, etc. apply). To the extent that an entity plays a role in purchase decisions made by a consumer of goods and services relating to data, the present invention has a wide range of beneficial applications. One is enabling independent trust based on real world representations that are not physically available to a consumer or user. A second is the ability to match informational needs between buyers and sellers that may not be universally appealing or cost effective in given market situations. These include auction models based on recognition of the interests or demand of consumers and market participants—which make trading profitable by focusing specialized buyers and

5 sellers. Another use for the information matching is to establish limits on the liability of such institutions and profit-seeking entities, such as insurance providers or credit companies. These vendors lack appropriate tools for determining intangible asset risk or even the value of the information being exchanged. By encouraging separate and distinct "trust" arrangements over an electronic network, profitable market-based relationships can result.

10 The present invention can make possible efficient and openly accessible markets for tradable information. Existing transaction security (including on-line credit cards, electronic cash or its equivalents, electronic wallets, electronic tokens, etc.) which primarily use cryptographic techniques to secure a transmission channel--but are not directly associated or dependent on the information being sold--fails to meet this valuable need. The present invention proposes a departure from the prior art by separating transactions from authentication in the sale of digitized data. Such data may include videos, songs, images, electronic stamps, electronic trademarks, and electronic logos used to ensure membership in some institutional body whose purpose is to assist in a dispute, limit liability and provide indirect guidance to consumers and market participants, alike.

20 With an increasingly anonymous marketplace, the present invention offers invaluable embodiments to accomplish "trusted" transactions in a more flexible, transparent manner while enabling market participants to negotiate terms and conditions. Negotiation may be driven by predetermined usage rules or parameters, especially as the information economy offers potentially many competitive marketplaces in which to transact, trade or exchange among businesses and consumers. As information grows exponentially, flexibility becomes an advantage to market participants, in that they need to screen, filter and verify information before making a transaction decision. Moreover, the accuracy and speed at which decisions can be made reliably enables confidence to grow with an aggregate of "trusted transactions". "Trusted transactions" beget further "trusted transactions" through experience. The present invention also provides for improvements over the prior art in the ability to utilize different independently important "modules" to enable a "trusted transaction" using competitive cryptographic and steganographic elements, as well as being able to support a wide variety of perceptually-based

media and information formats. The envisioned system is not bound by a proprietary means of creating recognition for a good or service, such as that embodied in existing closed system. Instead, the flexibility of the present invention will enable a greater and more diverse information marketplace.

5 The present invention is not a "trusted system", *per se*, but "trusted transactions" are enabled, since the same value-added information that is sought may still be in the clear, not in a protected storage area or closed, rule-based "inaccessible virtual environment".

10 A related additional set of embodiments regards the further separation of the transaction and the consumer's identification versus the identification of the transaction only. This is accomplished through separated "trusted transactions" bound by authentication, verification and authorization in a transparent manner. With these embodiments, consumer and vendor privacy could be incorporated. More sophisticated relationships are anticipated between parties, who can mix information
15 about their physical goods and services with a transparent means for consumers, who may not be known to the seller, who choose not to confide in an inherently closed "trusted system" or provide additional personal information or purchasing information (in the form of a credit card or other electronic payment system), in
20 advance of an actual purchase decision or ability to observe (audibly or visibly) the content in the clear. This dynamic is inconsistent with the prior art's emphasis on access control, not transparent access to value-added information (in the form of goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

25 These embodiments may include decisions about availability of a particular good or service through electronic means, such as the Internet, or means that can be modularized to conduct a transaction based on interconnection of various users (such as WebTV, a Nintendo or Sony game console with network abilities, cellular phone, PalmPilot, etc.). These embodiments may additionally be implemented in traditional
30 auction types (including Dutch auctions). Consumers may view their anonymous marketplace transactions very differently because of a lack of physical human interactions, but the present invention can enable realistic transactions to occur by maintaining open access and offering strict authentication and verification of the

information being traded. This has the effect of allowing legacy relationships, legacy information, and legacy business models to be offered in a manner which more closely reflects many observable transactions in the physical world. The tremendous benefits to sellers and consumers is obvious; existing transactions need not reduce their expectations of security. As well, the ability to isolate and quantify aspects of a transaction by module potentially allows for better price determinations of intangible asset insurance, transaction costs, advertising costs, liability, etc. which have physical world precedent.

It is contemplated that the publisher and/or owner of the copyrights will want to dictate restrictions on the ability of the purchaser to use the data being sold. Such restrictions can be implemented through the present invention, which presents a significant advantage over the prior art (which attempts to effect security through access control and attempted tight reigns over distribution). See US Pat. No. 5,428,606 for a discussion on democratizing digital information exchange between publishers and subscribers of said information.

A goal for providers of value-added content is to maximize profits for the sale of their content. Marketing and promotion of the informational content cannot be eliminated, considering the ever increasing amount of information vying for consumers and other market participant's attention. Nonetheless, in a market where the goods are speculatively valued, marketing budgets are inherently constrained, as you are trying to create demand for a product with little inherent value. Where such markets have participants, both buyers and sellers and their respective agents, with access to the same information in real time, market mechanisms efficiently price the market goods or services. These markets are characterized by "price commoditization" so buyers and sellers are limited to differentiating their offerings by selection and service. If the markets are about information itself, it has proven more difficult to accurately forecast the target price where sellers can maximize their profits. Quality and quantity provide different evaluation criteria of selection and service relating to the information being traded. The present invention regards a particular set of implementations of value-added content security in markets which may include unsecured and secure versions of the same value-added data (such as

songs, video, research, pictures, electronic logos, electronic trademarks, value-added information, etc.).

Transactions for value-added information can occur without any physical location. So, there is a need for a secure personal content server for which the value added information can be offered for transactions in a manner similar to real world transactions. One feature is to offer seemingly similar value added information in differing quality settings. These settings have logical relationships with fidelity and discreteness and are determined by market participants. Another issue is that because purchasers may be anonymous to sellers, it is more important to have a particular value-added information object available so that market participants can fulfill their role as consumers.

One fundamental weakness of current information markets is the lack of mechanisms to ensure that buyers and sellers can reach pricing equilibrium. This deficit is related to the "speculative", "fashion", and "vanity" aspects of perceptual content (such as music, video, and art or some future recognition to purchasers). For other goods and services being marketed to an anonymous marketplace, market participants may never see (and indeed, may choose to never see, an actual location where the transaction may physically occur. A physical location may simply not exist. There are a number of such virtual operations in business today, which would benefit from the improvements offered under the present system.

The present invention also seeks to provide improvements to the art in enabling a realistic model for building trust between parties (or their agents) not in a "system", per se. Because prior art systems lack any inherent ability to allow for information to flow freely to enable buyers and sellers to react to changing market conditions. The present invention can co-exist with these "trusted systems" to the extent that all market participants in a given industry have relatively similar information with which to price value-added data. The improvement over such systems, however, addresses a core features in most data-added value markets: predictions, forecasts, and speculation over the value of information is largely an unsuccessful activity for buyers and sellers alike. The additional improvement is the ability to maintain security even with unsecured or legacy versions of value-added information available to those who seek choices that fit less quantitative criteria—

"aesthetic quality" of the information versus "commercial price". Purchase or transaction decisions can be made first by authenticating an electronic version of a song, image, video, trademark, stamp, currency, etc.

5 Additional anticipated improvements include the ability to support varying pricing models such as auctions that are difficult or impossible to accomplish under existing prior art that leaves all access and pricing control with the seller alone, and the separation of the transaction from the exchange of the value-added information, which gives more control to buyers over their identities and purchasing habits, (both sensitive and separately distinct forms of "unrelated" value-added information).
10 Essentially, no system known in the art allows for realistic protocols to establish trust between buyers and sellers in a manner more closely reflecting actual purchasing behavior of consumers and changing selling behavior of sellers. The goal in such transactions is the creation of trust between parties as well as "trusted relationships" with those parties. The present invention is an example of one such system for media content where the "aesthetic" or "gestalt" of the underlying
15 content and its characteristics is a component of buying habits. Without an ability to open distribution systems to varying buyers and sellers, media content may be priced at less than maximum economic value and buyers may be deprived of a competitive, vigorous marketplace for exciting media content from many different creative
20 participants.

To the extent that recognition plays such a key role in an information economy, value-added data should be as accessible as possible to the highest number of market participants in the interests of furthering creativity and building a competitive marketplace for related goods and services. This is to the benefit of
25 both buyers and sellers as well as the other participants in such an economic ecosystem. The Internet and other transmission-based transactions with unknown parties presents a number of challenges to information vendors who wish to develop customer relations, trust and profitable sales. The information economy is largely an anonymous marketplace, thus, making it much more difficult to identify consumers and sellers.
30 The present invention provides remedies to help overcome these weaknesses.

The present invention is concerned with methods and systems which enable secure, paid exchange of value-added information, while separating transaction protocols. The present invention improves on existing means for distribution control by relying on authentication, verification and authorization that may be flexibly
5 determined by both buyers and sellers. These determinations may not need to be predetermined, although pricing matrix and variable access to the information opens additional advantages over the prior art. The present invention offers methods and protocols for ensuring value-added information distribution can be used to facilitate trust in a large or relatively anonymous marketplace (such as the Internet's World
10 Wide Web).

We now define components of the preferred embodiments for methods, systems, and devices.

Definitions:

Local Content Server (LCS): A device or software application which can
15 securely store a collection of value-added digital content. The LCS has a unique ID.

Secure Electronic Content Distributor (SECD): An entity, device or software application which can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. In cryptographic terms, the SECD acts as a "certification authority" or its equivalent. SECDs may have differing
20 arrangements with consumers and providers of value-added information. (The term "content" is used to refer generally to digital data, and may comprise video, audio, or any other data that is stored in a digital format).

Satellite Unit (SU): A portable medium or device which can accept secure digital content from a LCS through a physical, local connection and which can either
25 play or make playable the digital content. The SU may have other functionality as it relates to manipulating the content, such as recording. The SU has a unique ID. An SU may be a CD player, a video camera, a backup drive, or other electronic device which has a storage unit for digital data.

LCS Domain: A secure medium or area where digital content can be stored,
30 with an accompanying rule system for transfer of digital content in and out of the LCS Domain. The domain may be a single device or multiple devices—all of which have some common ownership or control. Preferably, a LCS domain is linked to a

single purchasing account. Inside the domain, one can enjoy music or other digital data without substantial limitations—as typically a license extends to all personal use.

5 SecureChannel™: A secure channel to pass individualized content to differentiate authentic content from legacy or unauthorized, pirated content. For example, the Secure Channel may be used as an auxiliary channel through which members of the production and distribution chain may communicate directly with individual consumers. Preferably, the Secure Channel is never exposed and can only be accessed through legitimate methods. SecureChannel may carry a value-adding component (VAC). The ability to provide consumers with value adding features will serve to give consumers an incentive to purchase new, secure hardware and software that can provide the additional enhanced services. The SecureChannel may also include protected associated data—data which is associated with a user and/or a particular set of content.

15 Standard Quality: A transfer path into the LCS Domain which maintains the digital content at a predetermined reference level or degrades the content if it is at a higher quality level. In an audio implementation, this might be defined as Red Book CD Quality (44100 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of a subset of VAC's or a quality level associated with particular VAC's. If a VAC is not in the subset, it is not passed. If a VAC is above the defined quality level, it is degraded.

20 Low Quality: A transfer path into the LCS Domain which degrades the digital content to a sub-reference level. In an audio implementation, this might be defined as below CD Quality (for instance, 32000 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of an absence of VAC's or a degraded quality level associated with particular VAC's.

25 High Quality: A transfer path into the LCS Domain which allows digital content of any quality level to pass unaltered. This transfer path can alternately be defined in terms of a complete set of VAC's or the highest quality level available associated with particular VAC's.

30 Rewritable Media: An mass storage device which can be rewritten (e.g. hard drive, CD-RW, Zip cartridge, M-O drive, etc...)

Read-Only Media: A mass storage device which can only be written once (e.g. CD-ROM, CD-R, DVD, DVD-R, etc...). Note: pre-recorded music, video, software, or images, etc. are all "read only" media.

Unique ID: A Unique ID is created for a particular transaction and is unique to that transaction (roughly analogous to a human fingerprint). One way to generate a Unique ID is with a one-way hash function. Another way is by incorporating the hash result with a message into a signing algorithm will create a signature scheme. For example, the hash result may be concatenated to the digitized, value added information which is the subject of a transaction. Additional uniqueness may be observed in a hardware device so as to differentiate that device, which may be used in a plurality of transactions, from other similar devices.

Value-added: Value-added information is differentiated from non-commoditized information in terms of its marketability or demand, which can vary, obviously, from each market that is created for the information. By way of example, information in the abstract has no value until a market is created for the information (i.e., the information becomes a commodity). The same information can be packaged in many different forms, each of which may have different values. Because information is easily digitized, one way to package the "same" information differently is by different levels of fidelity and discreteness. Value is typically bounded by context and consideration.

Authentication: A receiver of a "message" (embedded or otherwise within the value-added information) should be able to ascertain the original of the message (or by effects, the origin of the carrier within which the message is stored). An intruder should not be able to successfully represent someone else. Additional functionality such as Message Authentication Codes (MAC) could be incorporated (a one-way hash function with a secret key) to ensure limited verification or subsequent processing of value-added data.

Verification: In cryptographic terms, "verification" serves the "integrity" function to prevent an intruder from substituting false messages for legitimate ones. In this sense, the receiver of the message (embedded or otherwise present within the value-added information) should be assured that the message was not modified or altered in transit.

One-way hash function: One-way hash functions are known in the art. A hash function is a function which converts an input into an output, which is usually a fixed-sized output. For example, a simple hash function may be a function which accepts a digital stream of bytes and returns a byte consisting of the XOR function of all of the bytes in the digital stream of input data. Roughly speaking, the hash function may be used to generate a "fingerprint" for the input data. The hash function need not be chosen based on the characteristics of the input. Moreover, the output produced by the hash function (i.e., the "hash") need not be secret, because in most instances it is not computationally feasible to reconstruct the input which yielded the hash. This is especially true for a "one-way" hash function--one that can be used to generate a hash value for a given input string, but which hash cannot be used (at least, not without great effort) to create an input string that could generate the same hash value.

Authorization: A term which is used broadly to cover the acts of conveying official sanction, permitting access or granting legal power to an entity.

Encryption: For non digitally-sampled data, encryption is data scrambling using keys. For value-added or information rich data with content characteristics, encryption is typically slow or inefficient because content file sizes tend to be generally large. Encrypted data is called "ciphertext".

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the value-added or information rich data at the inherent granularity of the file format. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. Scrambling is efficient for larger media files and can be used to provide content in less than commercially viable or referenced quality levels. Scrambling is not as secure as encryption for these applications, but provides more fitting manipulation of media rich content in the context of secured distribution. Scrambled data is also called "ciphertext" for the purposes of this invention. Encryption generally acts on the data as a whole, whereas scrambling is applied often to a particular subset of the data concerned with the granularity of the data, for instance the file formatting. The result is that a smaller amount of data is "encoded" or "processed" versus strict encryption, where all of the data is "encoded" or "processed." By way of example, a cable TV signal

can be scrambled by altering the signal which provides for horizontal and vertical tracking, which would alter only a subset of the data, but not all of the data—which is why the audio signal is often untouched. Encryption, however, would generally so alter the data that no recognizable signal would be perceptually appreciated.

- 5 Further, the scrambled data can be compared with the unscrambled data to yield the scrambling key. The difference with encryption is that the ciphertext is not completely random, that is, the scrambled data is still perceptible albeit in a lessened quality. Unlike watermarking, which maps a change to the data set, scrambling is a transfer function which does not alter or modify the data set.

10 **Detailed Discussion of Invention**

- The LCS Domain is a logical area inside which a set of rules governing content use can be strictly enforced. The exact rules can vary between implementations, but in general, unrestricted access to the content inside the LCS Domain is disallowed. The LCS Domain has a set of paths which allow content to enter the domain under different circumstances. The LCS Domain also has paths which allow the content to exit the domain.

- A simple example provides insight into the scope of an LCS domain. If an LCS is assigned to an individual, then all music, video, and other content data which has lawfully issued to the individual may be freely used on that persons LCS domain (though perhaps “freely” is misleading, as in theory, the individual has purchased a license). A LCS Domain may comprise multiple SUs, for example, a video player, a CD player, etc. An individual may be authorized to take a copy of a song and play it in another's car stereo, but only while the individual's device or media is present. Once the device is removed, the friend's LCS will no longer have a copy of the music to play.

- The act of entering the LCS Domain includes a verification of the content (an authentication check). Depending upon the source of the content, such verification may be easier or harder. Unvalidateable content will be subjected to a quality degradation. Content that can be validated but which belongs to a different LCS Domain will be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between domains.

When content leaves the LCS Domain, the exiting content is embedded with information to uniquely identify the exiting content as belonging to the domain from which the content is leaving. It is allowed to leave at the quality level at which the content was originally stored in the LCS Domain (i.e. the quality level determined by the validation path). For example, the exiting content may include an embedded digital watermark and an attached hash or digital signature; the exiting content may also include a time stamp—which itself may be embedded or merely attached). Once it has exited, the content cannot return to the domain unless both the watermark and hash can be verified as belonging to this domain. The presence of one or the other may be sufficient to allow re-entry, or security can be set to require the presence of more than one identification signal.

This system is designed to allow a certifiable level of security for high-quality content while allowing a device to also be usable with unsecured content at a degraded quality level. The security measures are designed such that a removal of the watermark constitutes only a partial failure of the system. The altered content (i.e., the content from which the watermark has been removed or the content in which the watermark has been degraded) will be allowed back into the LCS Domain, but only at a degraded quality level, a result of the watermark destruction and subsequent obscurity to the system, consumers will not be affected to the extent that the unauthorized content has only been degraded, but access has not been denied to the content. Only a complete forgery of a cryptographically-secure watermark will constitute a complete failure of the system. For a discussion on such implementations please see US Pat. No. 5,613,004, US Pat No. 5,687,236, US Pat. No. 5,745,569, US Pat. No. 5,822,432, US Pat. No. 5,889,868, US Pat. No. 5,905,800, included by reference in their entirety and pending U.S. patent applications with Serial No. 09/046,627 "Method for Combining Transfer Function..."; Serial No. 09/053,628 "Multiple Transform Utilization and Application for Secure Digital Watermarking"; Serial No. 08/775,216 "Steganographic Method and Device"; Serial No. 08/772,222 "Z-Transform Implementation ..."; Serial No. 60/125990 "Utilizing Data Reduction in Steganographic and Cryptographic Systems".

Provable security protocols can minimize this risk. Thus the embedding system used to place the watermark does not need to be optimized for robustness, only for imperceptibility (important to publishers and consumers alike) and security (more important to publishers than to consumers). Ideally, as previously disclosed, security should not obscure the content, or prevent market participants from accessing information, which in the long term, should help develop trust or create relationships.

The system can flexibly support one or more "robust" watermarks as a method for screening content to speed processing. Final validation, however, relies upon the fragile, secure watermark and its hash or digital signature (a secure time stamp may also be incorporated). Fragile watermarks, meaning that signal manipulations would affect the watermark, may be included as a means to affect the quality of the content or any additional attributes intended to be delivered to the consumer.

15 **LCS Functions**

The LCS provides storage for content, authentication of content, enforcement of export rules, and watermarking and hashing of exported content. Stored content may be on an accessible rewritable medium, but it must be stored as ciphertext (encrypted or scrambled), not plain text, to prevent system-level extraction of the content. This is in contrast to the prior art which affix or otherwise attach meta-data to the content for access control by the variously proposed systems.

Typically, an LCS receives secured data from one or more SECDs. The SECD transfers content only after it has been secured. For example, the SECD may use an individualized cryptographic container to protect music content while in transit. Such a container may use public/private key cryptography, ciphering and/or compression, if desired.

The LCS may be able to receive content from a SECD, and must be able to authenticate content received via any of the plurality of implemented paths. The LCS must monitor and enforce any rules that accompany received content, such as number of available copies. Finally, it is preferred for the LCS to watermark all exported material (with the exception of Path 6 - see below) and supply a hash made from the unique ID of the LCS and the content characteristics (so as to be

maintained perceptually within the information and increase the level of security of the watermark).

SU Functions

5 The SU enables the content to be usable away from the LCS. The SU is partially within the LCS Domain. A protocol must exist for the SU and LCS to authenticate any connection made between them. This connection can have various levels of confidence set by the level of security between the SU and LCS and determinable by a certification authority or its equivalent, an authorized site for the content, for example. The transfer of content from the SU to the LCS without
10 watermarking is allowed. However, all content leaving the SU must be watermarked. Preferably, the SU watermark contains a hash generated from the SU's Unique ID and the content characteristics of the content being transferred. If the content came from a LCS, the SU watermark must also be generated based, in part, upon the hash received from the LCS. The LCS and SU watermarking
15 procedures do not need to be the same. However, the LCS must be able to read the SU watermarks for all different types of SU's with which it can connect. The SU does not need to be able to read any LCS watermarks. Each LCS and SU must have separate Unique IDs.

Sample Embodiment

20 **BRIEF DESCRIPTION OF THE DRAWINGS**

For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

25 FIG. 1 shows in block diagram form a system for one embodiment of an LCS, showing the possible paths for content to enter and exit the system.

FIG. 2 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the rewritable media.

FIG. 3 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the read-only media.

30 FIG. 4 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the satellite unit.

FIG. 5 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain.

FIG. 6 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain from the read-only media.

5 FIG. 7 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the SU to a receiver other than the LCS.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment of the present invention and its advantages are best understood by referring to FIGs. 1 through 7 of the drawings, like numerals 10 being used for like and corresponding parts of the various drawings.

FIG. 1 is a block diagram showing the components of a sample LCS system and showing the possible paths for content to enter and leave the LCS. In the embodiment of Figure 1, the LCS is a general purpose computing device such as a PC with software loaded to emulate the functions of a LCS. The LCS of Figure 1 15 has a Rewritable media (such as a hard drive), a Read-Only media (such as a CD-ROM drive), and software to control access (which software, in effect, defines the "LCS Domain"). The Secure Electronic Content Distributor (SECD) is connected via a network (such as the Internet, intranet, cable, satellite link, cellular communications network, or other commonly accepted network). The Satellite 20 Unite (SU) is a portable player which connects to the LCS and/or to other players where applicable (for example by way of a serial interface, USB, IEEE 1394, infrared, or other commonly used interface protocol). FIG. 1 also identifies seven (7) path ways.

Path 1 depicts a secure distribution of digital content from a SECD to a LCS. 25 The content can be secured during the transmission using one or more 'security protocols' (e.g., encryption or scrambling). Moreover, a single LCS may have the capability to receive content transmissions from multiple SECDs, and each SECD may use the same security protocols or different security protocols. In the context of FIG. 1, however, only a single SECD is displayed. It is also contemplated that the 30 same SECD may periodically or randomly use different security protocols. A typical security protocol uses an asymmetric cryptographic system, an example being a public key cryptography system where private and public key pairs allow the

LCS to authenticate and accept the received content. Another security protocol may involve the ability to authenticate the received content using a signature scheme.

In FIG. 2, content enters the LCS Domain from the rewritable media (such as a hard drive). This communication path is identified as Path 2 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the quality of the content is downgraded to Low Quality before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain. Optionally, if a watermark is present, the hash may be checked as further verification; and if the hash matches, the content is allowed in at High Quality. If it does not match, the content is rejected. If the extracted watermark does not match the expected watermark, then the content is denied access to the LCS Storage (i.e., the content is rejected).

In FIG. 3, content enters the LCS Domain from the Read-Only media. This communication path is identified as Path 3 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the LCS attempts to further analyze the content using other methods (i.e., other than watermarking) to try and verify the content for originality. If the content cannot be verified or is deemed to have been altered, then the content is downgraded to Standard Quality (or even Low Quality) before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, or in the event that the content is verified by means other than the watermark, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain (which is likely to be High Quality). For example, the Read-Only media may also contain a media-based identifier which verifies the content as an original, as opposed to a copy—and hence, a non-watermark method may be used to verify authenticity.

Optionally, even in the event of a watermark match, a hash may be checked as further verification; and if the hash matches, the content is allowed in at High

Quality, but if there is no match, the content is rejected. If the extracted watermark does not match the expected watermark, or if the LCS is unable to identify any other method for verifying the content's authenticity, then the content may be denied access to the LCS Storage (i.e., the content may be rejected), or if preferred by the user, the content may be permitted into the system at a degraded quality level. It is the user's prerogative to decide how the system will treat non-authenticated content, as well as legacy content.

In FIG. 4, content enters the LCS Domain from the satellite unit. This communication path is identified as Path 4 on FIG. 1. Content from an SU is marked with an SU watermark before exiting the SU. The LCS analyzes the content from the SU for watermarks, and in particular to determine if there is a watermark that matches that of the LCS. If the watermarks match, the content is permitted access to the LCS at the highest quality level. If there is a mismatch, then the content is denied access (i.e., the content is rejected). If the content does not contain a watermark, the quality is downgraded to Low Quality before permitting access to the LCS. Optionally, even in the event of a watermark match, a hash may be checked as further verification, and access at the highest quality level may depend upon both a match in watermarks and a match in hashes.

In FIG. 5, content is shown leaving the LCS Domain. This communication path is identified as Path 5 on FIG. 1. Content is retrieved from the LCS storage and then the content may be watermarked with a watermark that is unique to the LCS (for example, one that is based upon the LCS's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc. After watermarking, the content may be permitted to exit the LCS Domain, and may be exported to a device outside the LCS Domain, including for example, a rewritable media, a viewer, player, or other receiver.

In FIG. 6, content is shown leaving the LCS Domain. This communication path is identified as Path 6 on FIG. 1. This path is similar to Path 5, with a few

important differences. The output receiver is an SU, and because the receiver is an SU, the content may leave the LCS without being watermarked. Path 6 requires a secure protocol to determine that the receiver is in fact an SU. Once the path is verified, the content can be exported without a watermark. The LCS may optionally transmit the content together with a hash value which will be uniquely associated with the content.

In FIG 7, content is shown leaving the SU, to a receiver other than the LCS. This communication path is identified as Path 7 on FIG. 1. Content is retrieved from the SU storage and then the content may be watermarked with a watermark that is unique to the SU (for example, one that is based upon the SU's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc., and may even include the hash which the LCS attached to the content. After watermarking, the content may be permitted to exit the SU, and may be exported to a device other than the LCS, including for example, a rewritable media, a viewer, player, or other receiver. The quality level of the content leaving the LCS is generally the same quality level as that of the content when stored internally to the LCS.

The system of the present invention is utilized to complete digital data transactions. A typical transaction would have the following steps:

- 1.) Using an LCS, a user connects to a SECD.
- 2.) The user reviews a collection of data sets which are available for license (which for purposes of this application, may be equated with a purchase). The user then selects a data set (e.g., a song or other content), and purchases (or otherwise obtains the right to receive) a copy of the data set. (The user may transmit purchase information, for example, credit card information, using digital security that is known in the art of electronic commerce.)
- 3.) The SECD transmits the secured content to the LCS. Before transmitting any digital content, the SECD embeds at least one watermark and may

also transmit (perhaps through cryptography) at least one hash value along with the data being transmitted. The at least one hash value may be embedded with the at least one watermark or may be attached to the beginning or end of the data being transmitted. Alternately, the hash output may be combined in ways that are known in the art.

4.) The LCS optionally may send its public key to the SECD, in which case the SECD may use the LCS public key to apply an additional security measure to the data to be transmitted, before the data is actually transmitted to the LCS.

5.) The LCS receives the secured content transmitted by the SECD. The LCS may optionally use its private key to remove the additional layer of security which was applied with the LCS's public key.

6.) The LCS may authenticate the secure content that was received from the SECD by checking the watermark(s) and/or hash values. Optionally, the LCS may unpack the secured content from its security wrapper and/or remove any other layers of security. If the content can be authenticated, the content may be accepted into the LCS domain. Otherwise, it may be rejected.

Fragile Watermark Structure

A fragile watermark—one that is encoded in the LSB of each 16 bit sample—can actually hold all of the data that would typically comprise the information being transmitted in the SecureChannel™. At a typical sampling rate of 44.1 kHz, there is 88,200 16 bit samples for each second of data in the time domain (44,100 × 2 stereo channels). This provides 88,200 bits per second which may be used for storing a fragile watermark. A typical 3 minute stereo song could therefore accommodate 1.89 MB of data for a fragile watermark. (The watermark is called fragile, because it is easily removed without greatly sacrificing the quality of the audio data.) 1.89 MB represents an immense capacity relative to the expected size of the typical data to be transmitted in a SecureChannel (100 - 200 K).

Preferably, the fragile watermark is bound to a specific copy of a specific song, so that "information pirates" (i.e., would-be thieves) cannot detect a watermark and then copy it onto another song in an effort to feign authorization when none exists. A fragile watermark may also contain information which can be utilized by various receivers which might receive the signal being packaged. For

instance, a fragile watermark may contain information to optimize the playback of a particular song on a particular machine. A particular example could include data which differentiates an MP3 encoded version of a song and an AAC encoded version of the same song.

5 One way to bind a fragile watermark to a specific data set is through the use of hash functions. An example is demonstrated by the following sequence of steps:

1.) A digital data set (e.g., a song) is created by known means (e.g., sampling music at 44.1 kHz, to create a plurality of 16 bit data sets). The digital data set comprises a plurality of sample sets (e.g., a plurality of 16 bit data sets).

10 2) Information relative to the digital data set (e.g., information about the version of the song) is transformed into digital data (which we will call the SecureChannel data), and the SecureChannel data is then divided into a plurality of SecureChannel data blocks, each of which blocks may then be separately encoded.

15 3) A first block of the SecureChannel data is then is encoded into a first block of sample sets (the first block of sample sets comprising—at a minimum—a sufficient number of sample sets to accommodate the size of the first block of Secure Channel Data), for example by overwriting the LSB of each sample in the first block of sample sets.

20 4) A hash pool is created comprising the first block of encoded sample sets.

5) A first hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data;

25 6) The first hash value is then encoded into a second block of sample sets, the second block of sample sets being sufficient in size to accommodate the size of the first hash value.

7.) The second block of sample sets is then added to the hash pool

8) A second block of the SecureChannel data is then is encoded into a third block of sample sets.

30 9) The third block of encoded sample sets is added to the hash pool.

10) A second hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data;

11) The second hash value is then encoded into a fourth block of sample sets.

Steps 7-11 are then repeated for successive blocks of SecureChannel data until all of the SecureChannel data is encoded. Understand that for each block of SecureChannel data, two blocks of content data are utilized. Moreover, for efficiency, one could use a predetermined subset of the samples in the hash pool, instead of the whole block.

Each SecureChannel block may, for example, have the following structure:

```

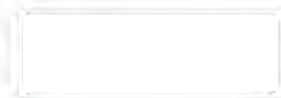
{
  long  BlockIdentifier,      //A code for the type of block
  long  BlockLength;        //The length of the block
  ...
  15  ...                    //Block data of a length matching BlockLength
  char  IdentityHash[hashSize];
  char  InsertionHash[hashSize];
}

```

In theory, each SecureChannel block may be of a different type of block (i.e., may begin with a different BlockIdentifier). In operation, a software application (or even an ASIC) may read the BlockIdentifier and determine whether it is a recognized block type for the particular application. If the application does not recognize the block type, the application may use the BlockLength to skip this block of SecureChannel.

Certain block types will be required to be present if the SecureChannel is going to be accepted. These might include an identity block and a SecureChannel hash block. The SecureChannel data may or may not be encrypted, depending on whether the data is transfer-restricted (a type of value-adding component, that is, VAC) or simply informative. For instance, user-added SecureChannel data need not be encrypted. A BlockIdentifier may also be used to indicate whether a SecureChannel data block is encrypted or not.

Robust Open Watermark (ROW)



A Robust-Open Watermark may be used to divide content into three categories. (The term "open watermark" is used merely to indicate that the watermark relies on a secret which is shared by an entire class of devices, as opposed to a secure watermark—which is readable only by a single member of a class of devices.) A binary setting may be used, whereby one state (e.g., "1") may be used to identify secure protected content—such as content that is distributed in a secured manner. When the LCS detects a secured status (e.g., by determining that the ROW is "1"), the content must be accompanied by an authenticatable SecureChannel before the content is permitted to enter the LCS Domain (e.g., electronic music distribution or EMD content). The other binary state (e.g., "0") may be used to identify unsecured content, for example, non-legacy media that is distributed in a pre-packaged form (e.g. CD's). When the binary setting is "0", the content may or may not have a SecureChannel. Such "0 content" shall only be admitted from a read-only medium in its original file format (e.g., a CD shall only be admitted if it is present on a Redbook CD medium). On the other hand, if the ROW is absent, then the LCS will understand that the content is "legacy". Legacy content may be admitted, or optionally, may be checked for a fragile watermark—and then admitted only if the fragile watermark is present. It would be possible to permit unfettered usage of legacy content—though again, it is the prerogative of the user who sets up the LCS.

Robust Forensic Watermark

Preferably, a robust forensic watermark is not accessible in any way to the consumer—or to "information pirates." A forensic watermark may be secured by a symmetric key held only by the seller. A transaction ID may be embedded at the time of purchase with a hash matching the symmetric key. The watermark is then embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of such a watermark is not limited by real-time/low cost constraints. The recovery will typically only be attempted on known pirated material, or material which is suspected of piracy. A recovery time of 2 hours on a 400 MHz PC may, therefore, be reasonable.

Sample Embodiment - Renewability

The system of the present invention contemplates the need for updating and replacing previously-embedded watermarks (which may be thought of generally as "renewing" a watermark). If someone is able to obtain the algorithms used to embed a watermark—or is otherwise able to crack the security, it would be desirable to be able to embed a new watermark using a secure algorithm. New watermarks, however, cannot be implemented with complete success over night, and thus, there inevitably will be transition periods where older SPCS are operating without updated software. In such a transition period, the content must continue to be recognizable to both the old SPCSs and the upgraded SPCSs. A solution is to embed both the original and the upgraded watermarks into content during the transition periods. Preferably, it is the decision of the content owner to use both techniques or only the upgraded technique.

The operation of the system of the present invention is complicated, however, by the presence of "legacy" digital content which is already in the hands of consumer (that is, digital content that was commercially distributed before the advent of watermarking systems) because legacy content will continue to be present in the future. Moreover, pirates who distribute unauthorized content will also complicate matters because such unauthorized copies are likely to be distributed in the same formats as legacy content. As it is unlikely that such unwatermarked content can ever be completely removed, the present system must try to accommodate such content.

Hardware can be configured to read old ROW content and extract the old ROW and insert in the content a new ROW.

Sample Embodiment – SPCS Audio Server

Tables 1, 2 and 3 depict a sample embodiment for an SPCS Audio Server, and in particular show how secured content packages are created as downloadable units (Table 1), how the LCS works on the input side for an SPCS Audio Server (Table 2), and how the LCS works on the output side (Table 3).

While the invention has been particularly shown and described by the foregoing detailed description, it will be understood by those skilled in the art that various other changes in form and detail may be made without departing from the spirit and scope of the invention.

Table 1

SAMPLE EMBODIMENT- SPCS Audio Server Stage

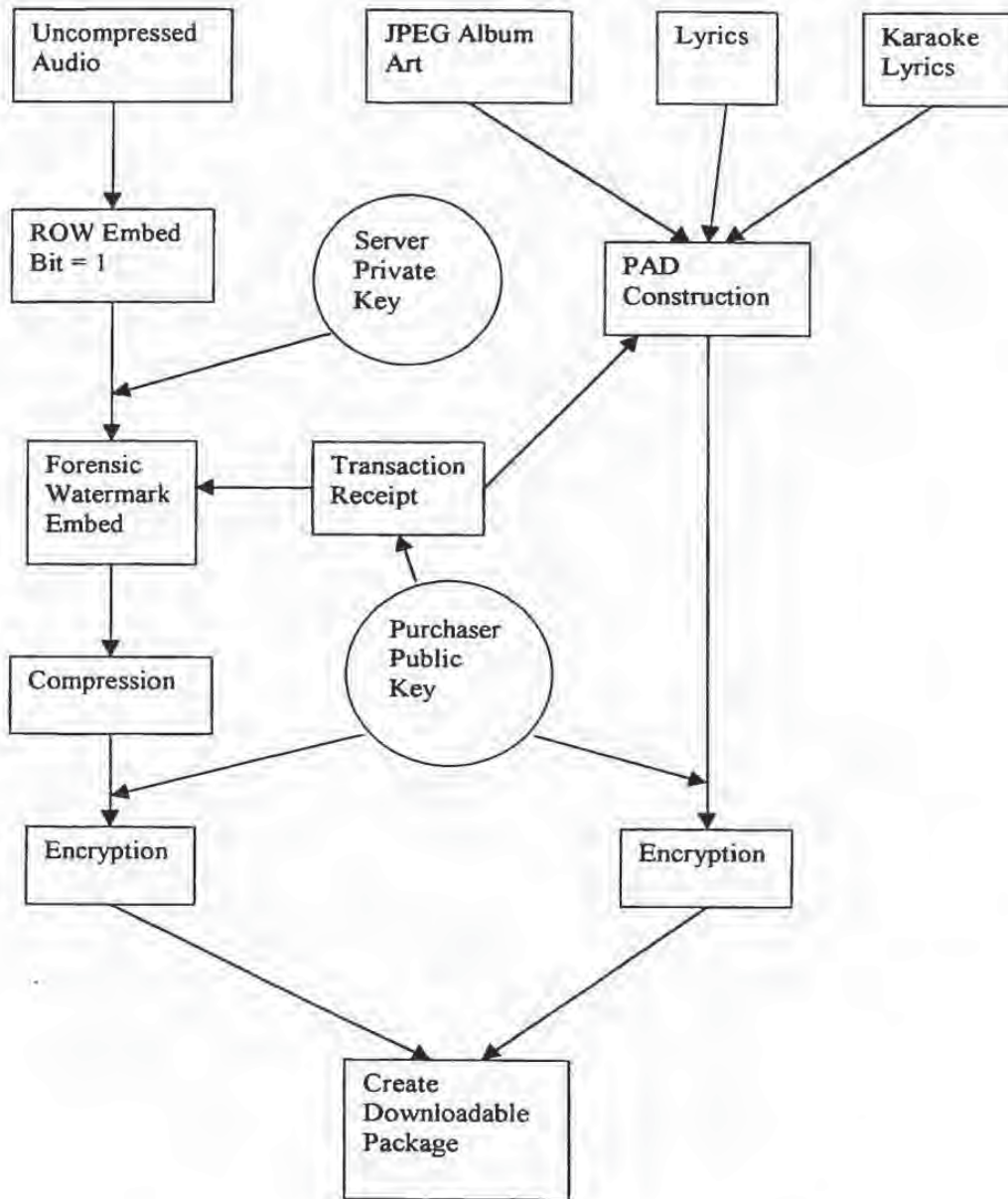


Table 2
SPCS Audio Player Input Stage

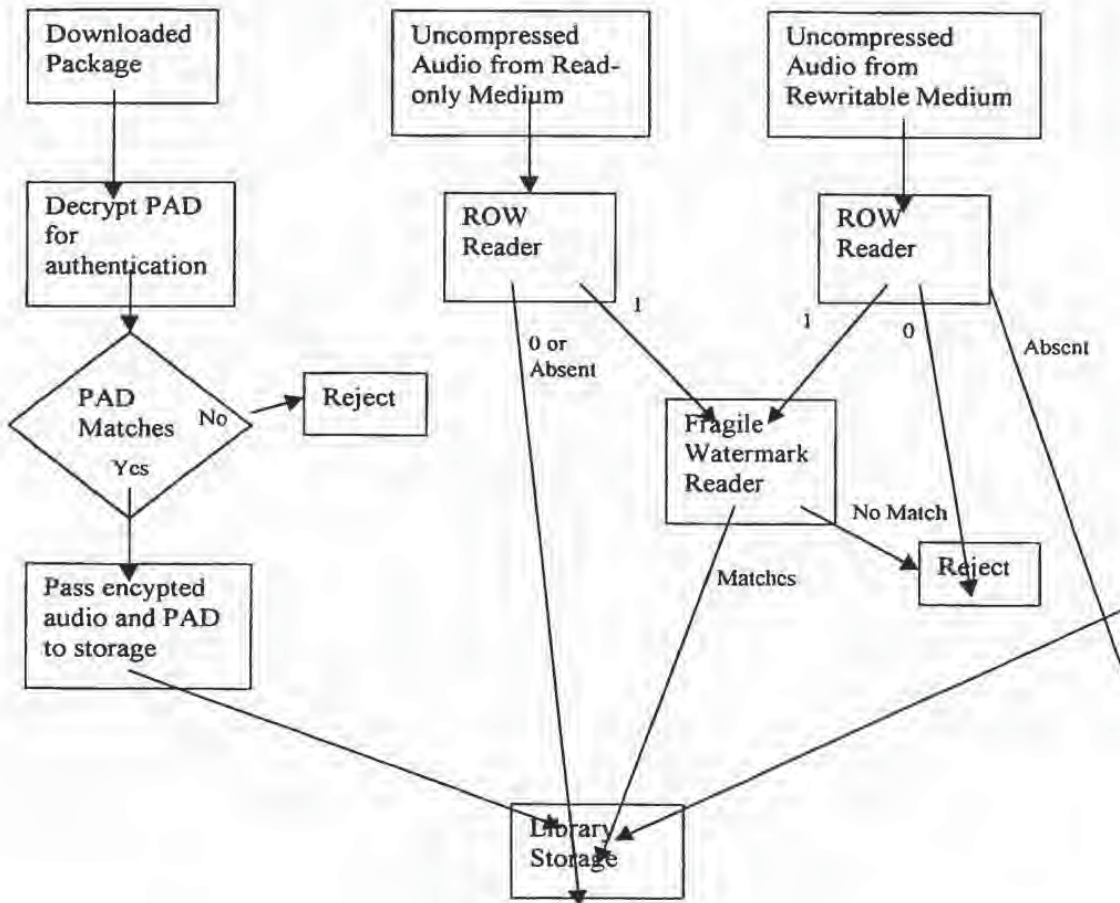
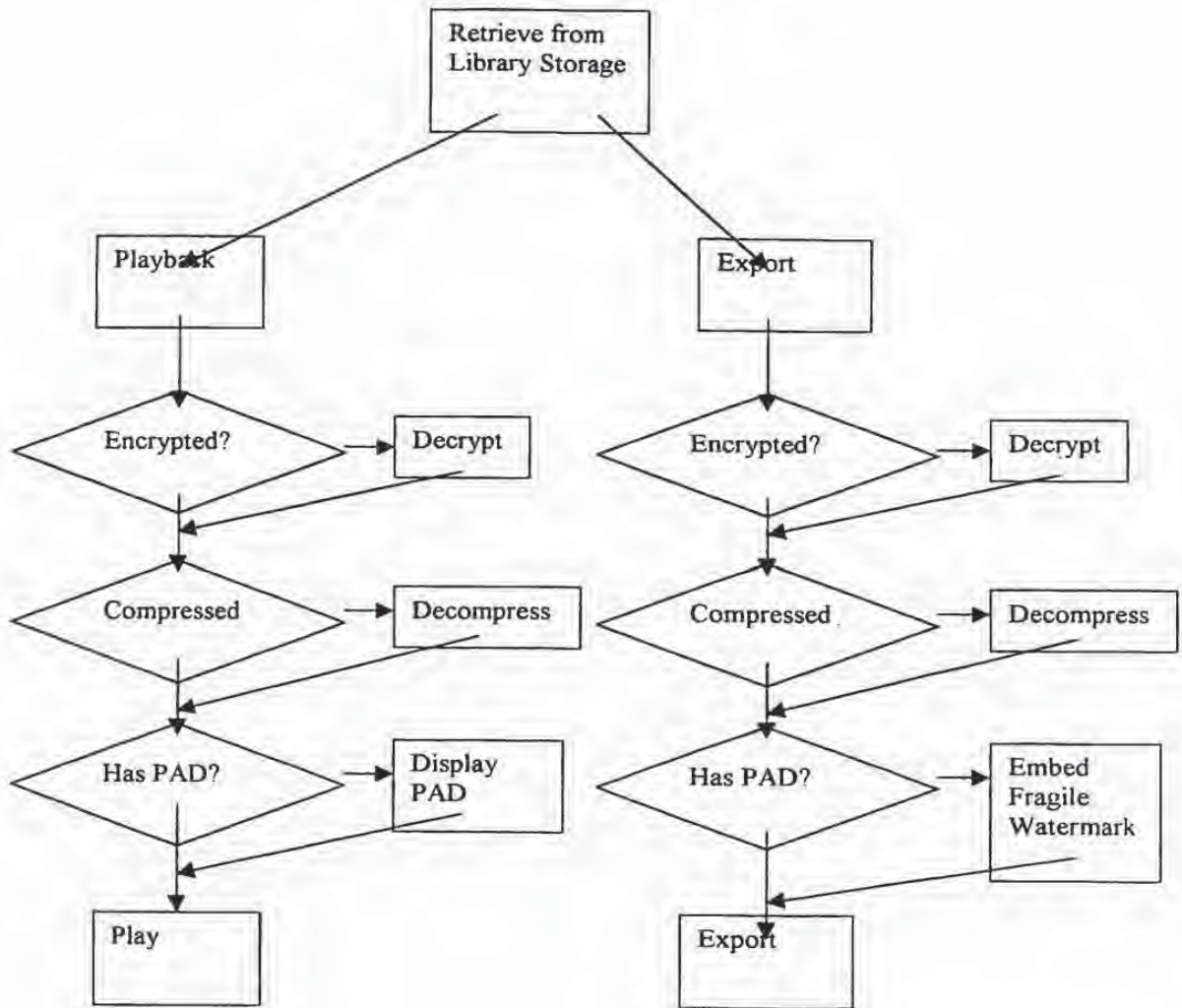


Table 3

SPCS Audio Player Output Stage



Claims:

- 1 A local content server system (LCS) for creating a secure environment for digital content, comprising:
- 5 a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;
- 10 b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved,
- c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS, and
- d) a programmable address module which can be programmed with an
- 15 identification code uniquely associated with the LCS, and
- said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS.
2. The LCS of claim 1 further comprising
- 20 e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content;
- and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided
- 25 the LCS first determines that digital content being received is authorized for use by the LCS,
- and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.

3. A local content server system (LCS) for creating a secure environment for digital content, comprising:
- a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;
 - b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and
 - c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved;
 - d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU; and
 - e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS;
- said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS,
- and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS.
4. The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred.
5. The system of claim 3, wherein said domain processor comprises:
- means for obtaining an identification code from an SU connected to the LCS's interface;

an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS;

means for analyzing digital content received from an SU;

5 said system permitting the digital content to be stored in the LCS if i) an analysis of the digital content received from the SU concludes that the content is authenticated, or ii) an analysis of the digital content received from the SU concludes that the content cannot be authenticated because no authentication data is embedded in the content, and

10 said system preventing the digital content from being stored on the LCS if i) an analysis of the digital content received from the SU concludes that the content is unauthenticated.

6. The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code of the LCS.

7. The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated because there is no authentication data embedded in the content.

8. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.

9. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to retrieve a copy of the requested content data set;

30 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

5 10. The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11. The system of claim 10,

10 wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve a copy of the requested content data set;

15 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

20 means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

wherein the LCS comprises:

25 means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

30 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

5 means to deliver the watermarked content data set to the SU for its use.

12. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

10 means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means receive a copy of the content data set,

15 means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated;

20 means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such the data contains no additional information to permit authentication.

14. The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated,

30 means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS; and

means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

15. The system of claim 5, wherein the LCS further comprises:

5 means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium.

16. A system for creating a secure environment for digital content, comprising:
a Secure Electronic Content Distributor (SECD);
a Local Content Server (LCS);

10 a communications network interconnecting the SECD to the LCS; and
a Satellite Unit (SU) capable of interfacing with the LCS,

said SECD comprising: a storage device for storing a plurality of data sets;
an input for receiving a request from the LCS to purchase a selection of at least one
of said plurality of data sets; a transaction processor for validating the request to
15 purchase and for processing payment for the request; a security module for
encrypting or otherwise securitizing the selected at least one data set; and an output
for transmitting the selected at least one data set that has been encrypted or
otherwise secured for transmission over the communications network to the LCS;

said LCS comprising: a domain processor; a first interface for connecting to
20 a communications network; a second interface for communicating with the SU; a
memory device for storing a plurality of data sets; and a programmable address
module which can be programmed with an identification code uniquely associated
with the LCS; and

said SU being a portable module comprising: a memory for accepting secure
25 digital content from a LCS; an interface for communicating with the LCS; and a
programmable address module which can be programmed with an identification
code uniquely associated with the SU.

17. A Method for creating a secure environment for digital content for a
consumer, comprising the following steps:

30 sending a message indicating that a user is requesting a copy of a content
data set;

retrieving a copy of the requested content data set;

embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;

transmitting the watermarked content data set to the requesting consumer via an electronic network;

receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user,

extracting at least one watermark from the transmitted watermarked content data set, and

permitting use of the content data set if the LCS determines that use is authorized.

18. The Method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user, and

permitting the storage of the content data set in a storage unit for the LCS.

19. The Method of claim 17, further comprising,

connecting a Satellite Unit (SU) to an LCS,

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user, and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering the content data set to the SU for its use.

20. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to an local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU,

5 analyzing the message to confirm that the SU is authorized to use the LCS;
and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

10 if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS, and

delivering the content data set to the SU for its use.

21. The Method of claim 20, further comprising:

embedding an open watermark into the content data to permit enhanced usage of the content data by the user.

15 22. The Method of claim 21, further comprising:

20 embedding at least one additional watermark into the content data, said at least one additional watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis to provide information on the history of the content data's use

23. The method of claim 20, wherein the content data can be stored at a level of quality which is selected by a user.

24. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

25 connecting a Satellite Unit (SU) to an local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

30 analyzing the message to confirm that the SU is authorized to use the LCS;
and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the watermarked content data set to the SU for its use.

5 25. The method of claim 24, further comprising:

embedding at least one robust open watermark into the copy of the requested content data set before the requested content data is delivered to the SU, said watermark indicating that the copy is authenticated.

10 26. The method of claim 25, wherein the robust watermark is embedded using any one of a plurality of embedding algorithms.

26. The method of claim 24, further comprising:

embedding a watermark which includes a hash value from a one-way hash function generated using the content data.

15 27. The method of claim 25, wherein the robust watermark can be periodically replaced with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.

28. The method of claim 24, further comprising the step of:

20 embedding additional robust open watermarks into the copy of the requested content data set before the requested content data is delivered to the SU, using a new algorithm; and

re-saving the newly watermarked copy to the LCS.

29. The method of claim 24, further comprising the step of:

25 saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

30. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) to an local content server (LCS),

30 sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS;
and
receiving a copy of the content data set;
assessing whether the content data set is authenticated;
5 if the content data is unauthenticated, denying access to the LCS storage unit;
and
if the content data is not capable of authentication, accepting the data at a
predetermined quality level, said predetermined quality level having been set for
legacy content.

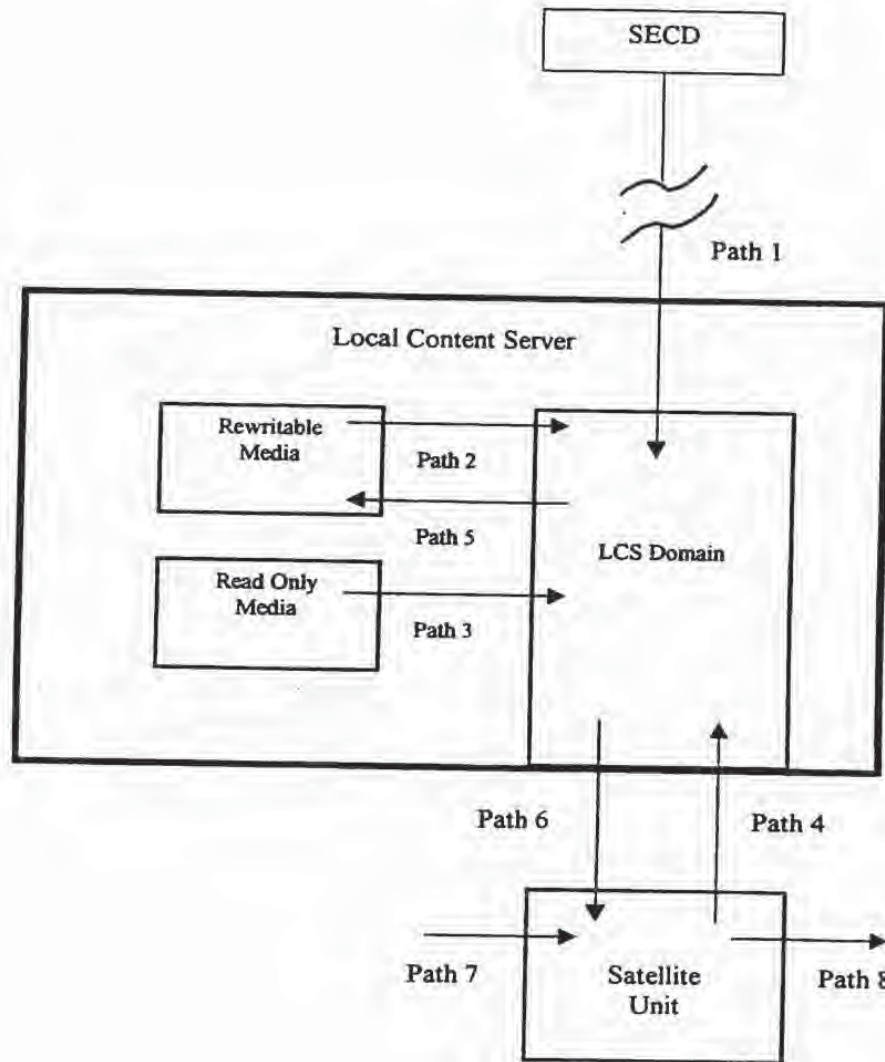


FIG. 1

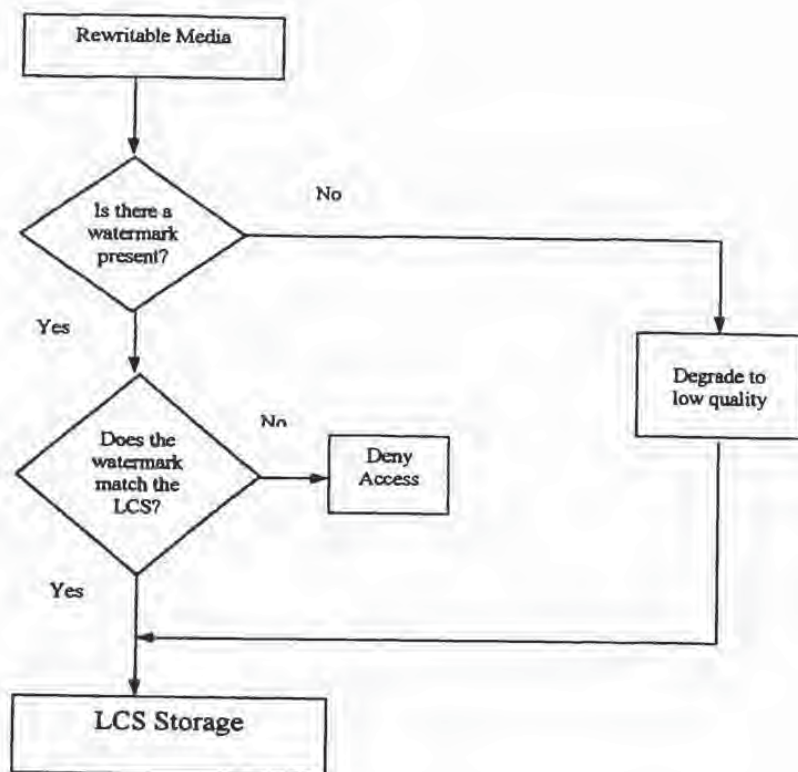


FIG. 2

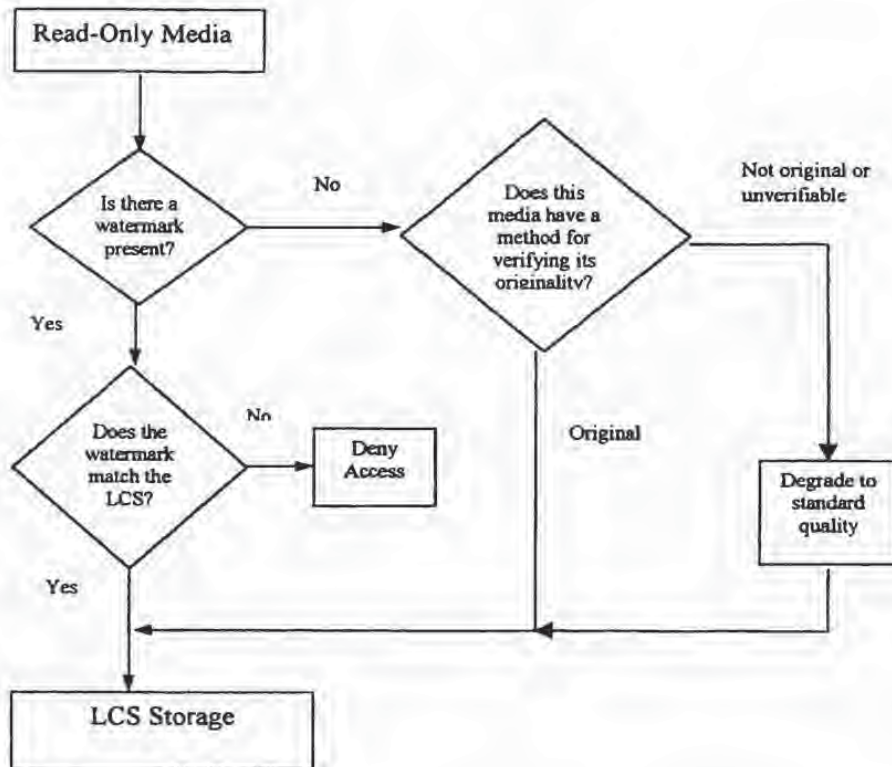


FIG. 3

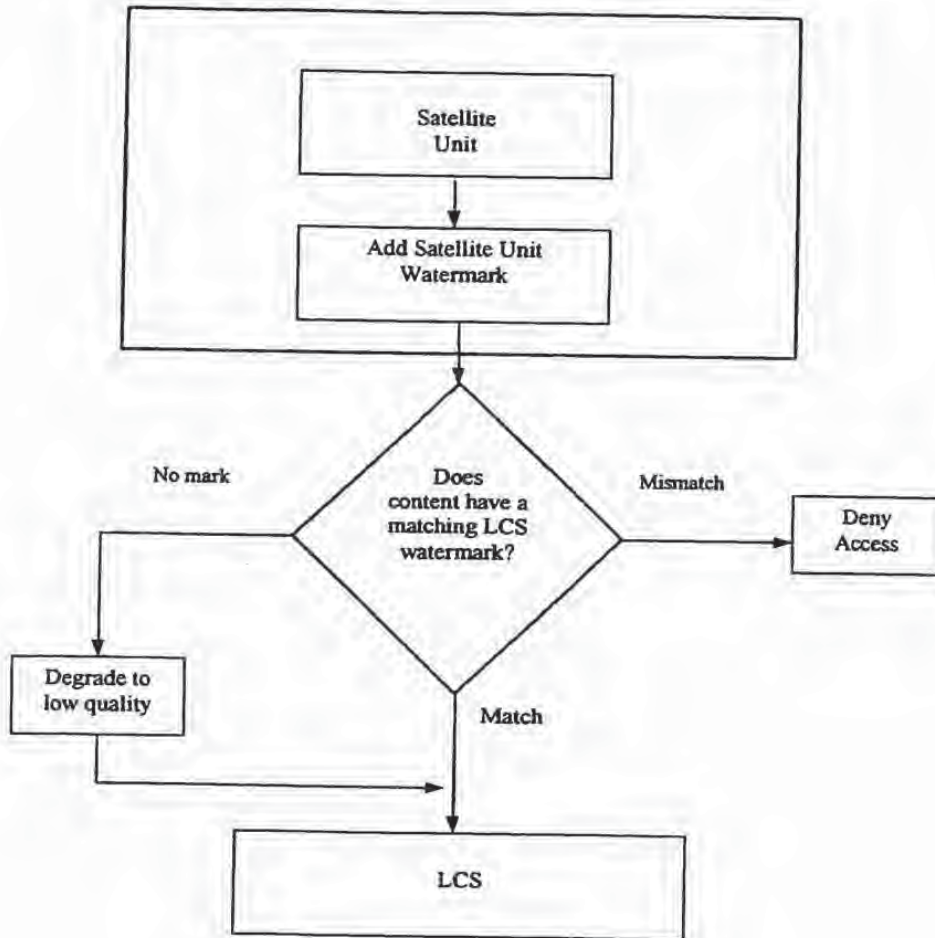


FIG. 4

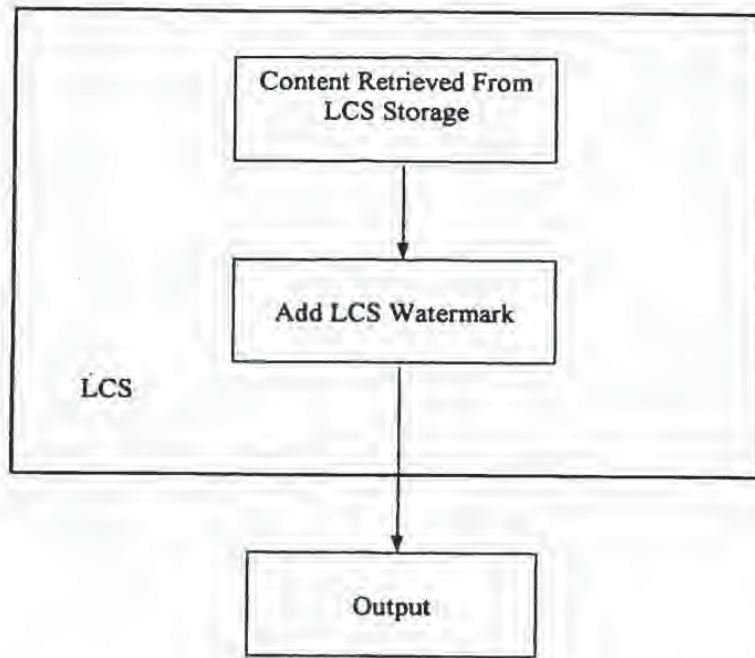


FIG. 5

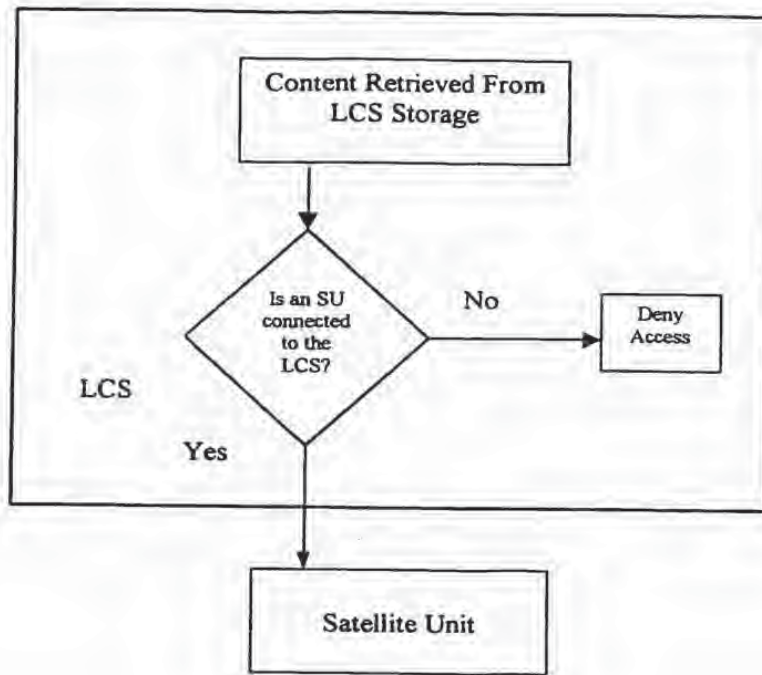


FIG. 6

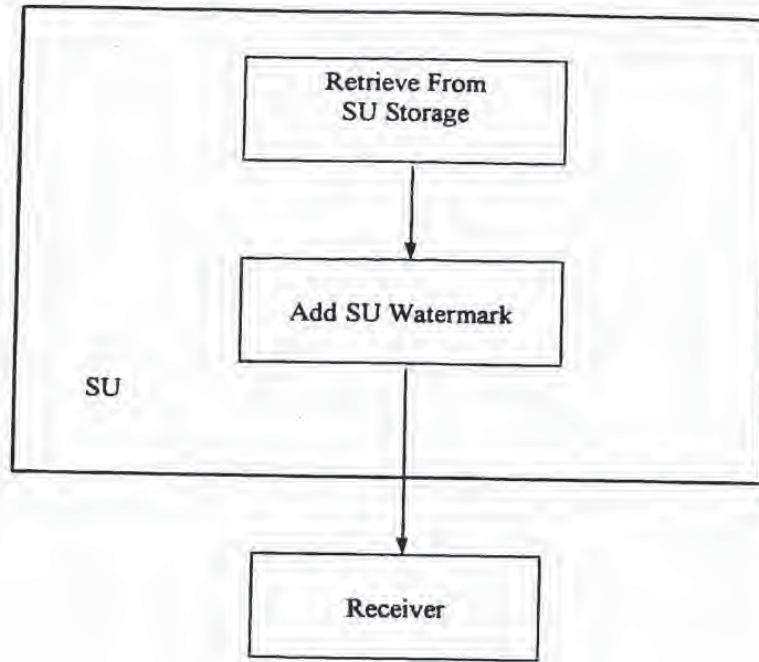


FIG. 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
15 March 2001 (15.03.2001)

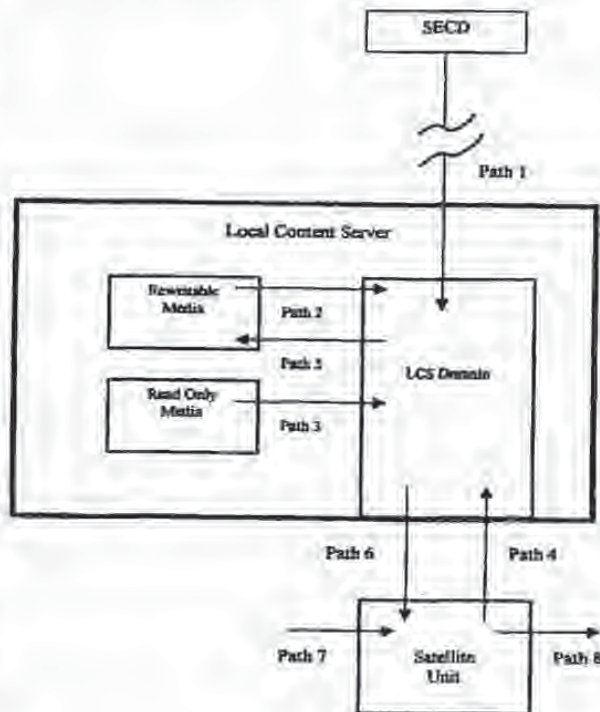
PCT

(10) International Publication Number
WO 01/18628 A3

- (51) International Patent Classification⁷: H04L 9/32, H04N 7/167
- (21) International Application Number: PCT/US00/21 (89)
- (22) International Filing Date: 4 August 2000 (04.08.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: *4 of Feb 82/30*
60/147,134 August 1999 (04.08.1999) US
60/213,489 23 June 2000 (23.06.2000) US
- (71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): MOSKOWITZ,
- Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).
- (74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, LLP, The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).
- (81) Designated States (national): JP, US.
- (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- Published:
— with international search report
- (88) Date of publication of the international search report:
22 November 2001

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



(57) Abstract: A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication (Path 1) for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium (Rewritable Media) whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU).

WO 01/18628 A3



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

| | | |
|---|--|---|
| Applicant's or agent's file reference 0661120139 | FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 3 below | |
| International application No. PCT/US00/21189 | International filing date (day/month/year) 04 AUGUST 2000 | (Earliest) Priority Date (day/month/year) 04 AUGUST 1999 |
| Applicant BLUE SPIKE, INC. | | |

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

I. Basis of the report

a. With regard to the language, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
 the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23 f(b)).

b. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international search was carried out on the basis of the sequence listing:

- contained in the international application in written form
- filed together with the international application in computer readable form
- furnished subsequently to this Authority in written form
- furnished subsequently to this Authority in computer readable form
- the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished
- the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. Certain claims were found unsearchable (See Box I)

3. Unity of invention is lacking (See Box I)

4. With regard to the title:

- the text is approved as submitted by the applicant
- the text has been established by this Authority to read as follows:

5. With regard to the abstract:

- the text is approved as submitted by the applicant
- the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the drawings to be published with the abstract is Figure No. 1

- as suggested by the applicant
- because the applicant failed to suggest a figure
- because this figure better characterizes the invention

None of the figures

Box III TEXT OF THE ABSTRACT (Continuation of item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d)).

The abstract is too long (PCT Rule 8.1(b)). The abstract must be less than 150 words, or 200 words when no Figure is to be published.

NEW ABSTRACT

A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication (Path 1) for connecting the LCS via a network to at least Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium (Rewritable Media) whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU).

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/21189

| A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : H04L 9/32; H04N 7/167 US CL : 713/176; 705/51, 52, 57; 380/203, 231 According to International Patent Classification (IPC) or to both national classification and IPC | | |
|---|--|-----------------------|
| B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/153; 705/51, 52, 57; 380/203, 231 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) APS EAST/BRS text search terms; watermark, audio, copy protect, distribution | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| Y | US 5,636,292 A (RHOADS) 03 JUNE 1997, col. 33, line 42-col. 34, line 8. | 4, 6-15 and 17-29 |
| Y | US 5,629,980 A (STEFIK et al) 13 MAY 1997, col. 26, line 37-col. 27, line 26. | 1-30 |
| Y, P | US 5,943,422 A (VAN WIE et al) 24 AUGUST 1999, col. 6, line 53-62 and col. 10, line 18-56. | 4, 6-15 and 17-29. |
| Y | US 5,636,276 A (BRUGGER) 03 JUNE 1997, col. 5, line 53-col. 6, line 8. | 1-30. |
| Y | US 5,341,429 A (STRINGER et al) 23 AUGUST 1994, col. 4, lines 1-22. | 30 |
| <input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex | | |
| * Special categories of cited documents: | | |
| *A* document defining the general state of the art which is not considered to be of particular relevance | *T* later document published after the international filing date in priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention | |
| *B* earlier document published on or after the international filing date | *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone. | |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art | |
| *O* document referring to an oral disclosure, use, exhibition or other means | *Z* document member of the same patent family | |
| *P* document published prior to the international filing date but later than the priority date claimed | | |
| Date of the actual completion of the international search 26 JANUARY 2001 | Date of mailing of the international search report 23 MAR 2001 | |
| Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230 | Authorized officer GILBERTO BARRÓN <i>Peggy Hanood</i> Telephone No. (703) 305-3900 | |

Form PCT/ISA/210 (second sheet) (July 1998)*

10/049101

JC13 Rec'd PGT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
 Applicable through 10/31/2002. CMB 0604-0032
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2002

Patent fees are subject to annual revision.

Complete if Known

| | |
|-----------------------|------------------------|
| Application Number: | PCT/US00/21189 |
| Filing Date: | 02/08/2002 |
| First Named Inventor: | Scott Moskowitz et al. |
| Examiner Name: | |
| Group Art Unit: | |
| Attorney Docket No.: | 80408.0011 |

TOTAL AMOUNT OF PAYMENT (\$)

| METHOD OF PAYMENT | | FEE CALCULATION (continued) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---------------------------|--|------------------------|--|---------------------------|-----------------------|-----------------|----------|--------|----------|--------------------|--------|---|--------------------|----------|-------------------|------|--|--|--------------|------------------|--------------|-----------------|-----|---------------------------|--------------------|-----|--------------------------|-----|----------|---|----|-----------------------------------|-----|-----|-------------|--|---------------------------------------|-----|-------|-----|-------|---|-----|-----|-----|-----|--|--|--|-----|-------------|-----|-----|---|--|-----|-----|-----|-----|--|--|-----|-------|-----|-----|---|--|-----|-------|-----|-----|--|--|-----|-----|-----|-----|------------------|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--------------------------|--|-----|-------|-----|-------|---|--|-----|-----|-----|----|----------------------------------|--|-----|-------|-----|-----|------------------------------------|--|-----|-------|-----|-----|--------------------------------|--|-----|-----|-----|-----|--------------------|--|-----|-----|-----|-----|-----------------|--|-----|-----|-----|-----|---------------------------|--|-----|----|-----|----|-------------------------------------|--|-----|-----|-----|-----|--|--|-----|----|-----|----|--|--|-----|-----|-----|-----|---|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|---|--|-----|-----|-----|-----|---|--|----------------------|--|--|--|--|------------------------------------|--|--|--|--|--------------|--|--|------|--------|
| <p>1. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:</p> <p>Deposit Account Number: 50-1120</p> <p>Deposit Account Name: Wiley Rein & Fielding, LLP Floyd Chapman</p> <p><input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR 1.17 and 1.177</p> <p><input type="checkbox"/> Applicant claims priority date: See 37 CFR 1.27</p> | | <p>3. ADDITIONAL FEES</p> <table border="1"> <thead> <tr> <th>Fee Code</th> <th>Large Entity Fee (\$)</th> <th>Small Entity Fee (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>105</td> <td>130</td> <td>205</td> <td>00</td> <td>Stouffage - late filing fee on priority</td> <td></td> </tr> <tr> <td>107</td> <td>50</td> <td>227</td> <td>25</td> <td>Surcharge - late provisional filing fee on power sheet</td> <td></td> </tr> <tr> <td>139</td> <td>130</td> <td>129</td> <td>130</td> <td>Non-English specification</td> <td></td> </tr> <tr> <td>147</td> <td>2,520</td> <td>147</td> <td>2,520</td> <td>Fee filing a request for ex parte reexamination</td> <td></td> </tr> <tr> <td>172</td> <td>920</td> <td>112</td> <td>920</td> <td>Requesting publication of SIR prior to Examiner action</td> <td></td> </tr> <tr> <td>173</td> <td>1,840</td> <td>119</td> <td>1,840</td> <td>Requesting publication of SIR after Examiner action</td> <td></td> </tr> <tr> <td>115</td> <td>110</td> <td>215</td> <td>05</td> <td>Extension for reply within first month</td> <td></td> </tr> <tr> <td>116</td> <td>400</td> <td>218</td> <td>200</td> <td>Extension for reply within second month</td> <td></td> </tr> <tr> <td>117</td> <td>920</td> <td>217</td> <td>400</td> <td>Extension for reply within third month</td> <td></td> </tr> <tr> <td>118</td> <td>1,440</td> <td>218</td> <td>720</td> <td>Extension for reply within fourth month</td> <td></td> </tr> <tr> <td>128</td> <td>1,980</td> <td>228</td> <td>980</td> <td>Extension for reply within fifth month</td> <td></td> </tr> <tr> <td>119</td> <td>320</td> <td>210</td> <td>180</td> <td>Notice of Appeal</td> <td></td> </tr> <tr> <td>120</td> <td>320</td> <td>220</td> <td>180</td> <td>Filing a brief in support of an appeal</td> <td></td> </tr> <tr> <td>121</td> <td>280</td> <td>224</td> <td>140</td> <td>Request for oral hearing</td> <td></td> </tr> <tr> <td>138</td> <td>1,510</td> <td>138</td> <td>1,510</td> <td>Petition to institute a public use proceeding</td> <td></td> </tr> <tr> <td>140</td> <td>110</td> <td>240</td> <td>55</td> <td>Petition to revive - unavoidable</td> <td></td> </tr> <tr> <td>141</td> <td>1,250</td> <td>240</td> <td>640</td> <td>Petition to revive - unintentional</td> <td></td> </tr> <tr> <td>142</td> <td>1,280</td> <td>242</td> <td>640</td> <td>Utility surcharge (or rescuer)</td> <td></td> </tr> <tr> <td>143</td> <td>400</td> <td>242</td> <td>230</td> <td>Division issue fee</td> <td></td> </tr> <tr> <td>144</td> <td>620</td> <td>244</td> <td>310</td> <td>Plant issue fee</td> <td></td> </tr> <tr> <td>122</td> <td>150</td> <td>122</td> <td>150</td> <td>Patents in Fee Commission</td> <td></td> </tr> <tr> <td>123</td> <td>50</td> <td>123</td> <td>50</td> <td>Processing fee under 37 CFR 1.17(g)</td> <td></td> </tr> <tr> <td>125</td> <td>180</td> <td>125</td> <td>180</td> <td>Submission of Information Disclosure Sheet</td> <td></td> </tr> <tr> <td>551</td> <td>40</td> <td>551</td> <td>40</td> <td>Financing each patent assignment per property (times number of properties)</td> <td></td> </tr> <tr> <td>145</td> <td>780</td> <td>246</td> <td>370</td> <td>Filing a submission after final rejection (37 CFR § 1.129(p))</td> <td></td> </tr> <tr> <td>146</td> <td>780</td> <td>249</td> <td>370</td> <td>For each additional invention to be examined (37 CFR § 1.129(b))</td> <td></td> </tr> <tr> <td>179</td> <td>740</td> <td>378</td> <td>370</td> <td>Request for Continued Examination (RCE)</td> <td></td> </tr> <tr> <td>169</td> <td>300</td> <td>169</td> <td>300</td> <td>Request for expedited examination of a design application</td> <td></td> </tr> <tr> <td colspan="4">Other fee (specify):</td> <td></td> </tr> <tr> <td colspan="4">*Recorded by Basic Filing Fee Paid</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (3)</td> <td>(\$)</td> <td>637.00</td> </tr> </tbody> </table> | | Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | 105 | 130 | 205 | 00 | Stouffage - late filing fee on priority | | 107 | 50 | 227 | 25 | Surcharge - late provisional filing fee on power sheet | | 139 | 130 | 129 | 130 | Non-English specification | | 147 | 2,520 | 147 | 2,520 | Fee filing a request for ex parte reexamination | | 172 | 920 | 112 | 920 | Requesting publication of SIR prior to Examiner action | | 173 | 1,840 | 119 | 1,840 | Requesting publication of SIR after Examiner action | | 115 | 110 | 215 | 05 | Extension for reply within first month | | 116 | 400 | 218 | 200 | Extension for reply within second month | | 117 | 920 | 217 | 400 | Extension for reply within third month | | 118 | 1,440 | 218 | 720 | Extension for reply within fourth month | | 128 | 1,980 | 228 | 980 | Extension for reply within fifth month | | 119 | 320 | 210 | 180 | Notice of Appeal | | 120 | 320 | 220 | 180 | Filing a brief in support of an appeal | | 121 | 280 | 224 | 140 | Request for oral hearing | | 138 | 1,510 | 138 | 1,510 | Petition to institute a public use proceeding | | 140 | 110 | 240 | 55 | Petition to revive - unavoidable | | 141 | 1,250 | 240 | 640 | Petition to revive - unintentional | | 142 | 1,280 | 242 | 640 | Utility surcharge (or rescuer) | | 143 | 400 | 242 | 230 | Division issue fee | | 144 | 620 | 244 | 310 | Plant issue fee | | 122 | 150 | 122 | 150 | Patents in Fee Commission | | 123 | 50 | 123 | 50 | Processing fee under 37 CFR 1.17(g) | | 125 | 180 | 125 | 180 | Submission of Information Disclosure Sheet | | 551 | 40 | 551 | 40 | Financing each patent assignment per property (times number of properties) | | 145 | 780 | 246 | 370 | Filing a submission after final rejection (37 CFR § 1.129(p)) | | 146 | 780 | 249 | 370 | For each additional invention to be examined (37 CFR § 1.129(b)) | | 179 | 740 | 378 | 370 | Request for Continued Examination (RCE) | | 169 | 300 | 169 | 300 | Request for expedited examination of a design application | | Other fee (specify): | | | | | *Recorded by Basic Filing Fee Paid | | | | | SUBTOTAL (3) | | | (\$) | 637.00 |
| Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 130 | 205 | 00 | Stouffage - late filing fee on priority | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 | 50 | 227 | 25 | Surcharge - late provisional filing fee on power sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 139 | 130 | 129 | 130 | Non-English specification | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 147 | 2,520 | 147 | 2,520 | Fee filing a request for ex parte reexamination | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 172 | 920 | 112 | 920 | Requesting publication of SIR prior to Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 173 | 1,840 | 119 | 1,840 | Requesting publication of SIR after Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 115 | 110 | 215 | 05 | Extension for reply within first month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 116 | 400 | 218 | 200 | Extension for reply within second month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 117 | 920 | 217 | 400 | Extension for reply within third month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 118 | 1,440 | 218 | 720 | Extension for reply within fourth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 128 | 1,980 | 228 | 980 | Extension for reply within fifth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 119 | 320 | 210 | 180 | Notice of Appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 120 | 320 | 220 | 180 | Filing a brief in support of an appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 121 | 280 | 224 | 140 | Request for oral hearing | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 138 | 1,510 | 138 | 1,510 | Petition to institute a public use proceeding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 140 | 110 | 240 | 55 | Petition to revive - unavoidable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 141 | 1,250 | 240 | 640 | Petition to revive - unintentional | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 142 | 1,280 | 242 | 640 | Utility surcharge (or rescuer) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 143 | 400 | 242 | 230 | Division issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 144 | 620 | 244 | 310 | Plant issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 122 | 150 | 122 | 150 | Patents in Fee Commission | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 123 | 50 | 123 | 50 | Processing fee under 37 CFR 1.17(g) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 125 | 180 | 125 | 180 | Submission of Information Disclosure Sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 551 | 40 | 551 | 40 | Financing each patent assignment per property (times number of properties) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 145 | 780 | 246 | 370 | Filing a submission after final rejection (37 CFR § 1.129(p)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 146 | 780 | 249 | 370 | For each additional invention to be examined (37 CFR § 1.129(b)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 179 | 740 | 378 | 370 | Request for Continued Examination (RCE) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169 | 300 | 169 | 300 | Request for expedited examination of a design application | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Other fee (specify): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| *Recorded by Basic Filing Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (3) | | | (\$) | 637.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. <input type="checkbox"/> Payment Enclosed:</p> <p><input type="checkbox"/> Check <input type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other</p> | | <p>1. BASIC FILING FEE</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (E)</th> <th>Small Entity Fee Code (E)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>101</td> <td>280</td> <td>0201 070</td> <td>Utility filing fee</td> <td>370.00</td> </tr> <tr> <td>106</td> <td>350</td> <td>0205 100</td> <td>Design filing fee</td> <td></td> </tr> <tr> <td>107</td> <td>350</td> <td>0207 050</td> <td>Plant filing fee</td> <td></td> </tr> <tr> <td>108</td> <td>740</td> <td>0208 170</td> <td>Rescuer filing fee</td> <td></td> </tr> <tr> <td>114</td> <td>100</td> <td>0214 000</td> <td>Provisional filing fee</td> <td></td> </tr> <tr> <td colspan="3">SUBTOTAL (1)</td> <td>(\$) 370.00</td> </tr> </tbody> </table> | | Large Entity Fee Code (E) | Small Entity Fee Code (E) | Fee Description | Fee Paid | 101 | 280 | 0201 070 | Utility filing fee | 370.00 | 106 | 350 | 0205 100 | Design filing fee | | 107 | 350 | 0207 050 | Plant filing fee | | 108 | 740 | 0208 170 | Rescuer filing fee | | 114 | 100 | 0214 000 | Provisional filing fee | | SUBTOTAL (1) | | | (\$) 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (E) | Small Entity Fee Code (E) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 101 | 280 | 0201 070 | Utility filing fee | 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 106 | 350 | 0205 100 | Design filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 | 350 | 0207 050 | Plant filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 108 | 740 | 0208 170 | Rescuer filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 114 | 100 | 0214 000 | Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (1) | | | (\$) 370.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. EXTRA CLAIM FEES</p> <table border="1"> <thead> <tr> <th>Total Claims</th> <th>Extra Claims</th> <th>Fee from below</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>47</td> <td>20*</td> <td>27</td> <td>188.00</td> </tr> <tr> <td>1</td> <td>3**</td> <td>4</td> <td>168.00</td> </tr> <tr> <td colspan="3">Multiple Dependent</td> <td>0.00</td> </tr> </tbody> </table> | | Total Claims | Extra Claims | Fee from below | Fee Paid | 47 | 20* | 27 | 188.00 | 1 | 3** | 4 | 168.00 | Multiple Dependent | | | 0.00 | <p>Large Entity Small Entity</p> <table border="1"> <thead> <tr> <th>Fee Code (E)</th> <th>Fee Code (E)</th> <th>Fee Code (E)</th> <th>Fee Description</th> </tr> </thead> <tbody> <tr> <td>103</td> <td>78</td> <td>203</td> <td>0</td> <td>Claim fee - excess of 20</td> </tr> <tr> <td>102</td> <td>84</td> <td>202</td> <td>42</td> <td>Independent claims in excess of 3</td> </tr> <tr> <td>104</td> <td>290</td> <td>204</td> <td>140</td> <td>Multiple dependent claim, if not paid</td> </tr> <tr> <td>105</td> <td>84</td> <td>205</td> <td>42</td> <td>Rescuer independent claims over original patent</td> </tr> <tr> <td>110</td> <td>18</td> <td>210</td> <td>9</td> <td>Remove claims in excess of 20 and over original patent</td> </tr> <tr> <td colspan="3">SUBTOTAL (2)</td> <td>(\$) 422.00</td> </tr> </tbody> </table> | | Fee Code (E) | Fee Code (E) | Fee Code (E) | Fee Description | 103 | 78 | 203 | 0 | Claim fee - excess of 20 | 102 | 84 | 202 | 42 | Independent claims in excess of 3 | 104 | 290 | 204 | 140 | Multiple dependent claim, if not paid | 105 | 84 | 205 | 42 | Rescuer independent claims over original patent | 110 | 18 | 210 | 9 | Remove claims in excess of 20 and over original patent | SUBTOTAL (2) | | | (\$) 422.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total Claims | Extra Claims | Fee from below | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 47 | 20* | 27 | 188.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 3** | 4 | 168.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Multiple Dependent | | | 0.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fee Code (E) | Fee Code (E) | Fee Code (E) | Fee Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 | 78 | 203 | 0 | Claim fee - excess of 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 102 | 84 | 202 | 42 | Independent claims in excess of 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 104 | 290 | 204 | 140 | Multiple dependent claim, if not paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 84 | 205 | 42 | Rescuer independent claims over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 110 | 18 | 210 | 9 | Remove claims in excess of 20 and over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SUBTOTAL (2) | | | (\$) 422.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| SUBMITTED BY | | Complete if applicable | |
|-------------------|-------------------------|---------------------------------|--------------|
| Name (Print/Type) | Floyd B. Chapman | Registration No. (Member/Agent) | 40,555 |
| Signature | <i>Floyd B. Chapman</i> | Telephone | 202/719-7000 |
| | | Date | 02/08/2002 |

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Duration: Your Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

10/049101
 JG13 Rec'd PCT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | | |
|--|--------------------------|--------------------------------|
| <h1>FEE TRANSMITTAL</h1> <h2>for FY 2002</h2> <p>Patent fees are subject to annual revision.</p> | Complete if Known | |
| | Application Number | PCT/US00/01189 |
| | Filing Date | 02/08/2002 |
| | First Named Inventor | Scott Moskowitz et al. |
| | Examiner Name | |
| | Group Art Unit | |
| TOTAL AMOUNT OF PAYMENT (\$) | | Attorney Docket No. 80408.0011 |

| METHOD OF PAYMENT | FEE CALCULATION (continued) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|----------------------------|-----------------------|---|-----------------|----------|-----|-----|--------------------|-----|-----|-----|----------------------------|----------------------------|-------------------|----------|-----|-----|-----|-----|------------------------|-----|-----|-----|-----|-------|-----------------------------------|-------|-----|-----|-----|------|--|------|-----|----|-----|--------|--|--------|-----|----|-----|-----|---|----|--|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-------|-----|-----|--|--|-----|-------|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-------|-----|-------|--|--|-----|-----|-----|----|--|--|-----|-------|-----|-----|--|--------|-----|-------|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|----|-----|----|--|--|-----|----|-----|----|--|--|-----|-----|-----|-----|--|--|-----|----|-----|----|--|--|-----|-----|-----|-----|--|--|-----|----|-----|-----|--|--|-----|-----|-----|-----|--|--|-----|-----|-----|-----|--|--|
| <p>1. <input type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:</p> <p>Deposit Account Number: 50-1120</p> <p>Deposit Account Name: Wiley Rein & Fielding, LLP Floyd Chapman</p> <p><input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17</p> <p><input type="checkbox"/> Refund/credits (mail only state - See 37 CFR 1.27)</p> <p>2. <input checked="" type="checkbox"/> Payment Enclosed: <input type="checkbox"/> Check <input checked="" type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other</p> | <p>3. ADDITIONAL FEES</p> <table border="1"> <thead> <tr> <th>Fee Code</th> <th>Large Entity Fee (\$)</th> <th>Small Entity Fee (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>105</td><td>120</td><td>205</td><td>65</td><td>5</td><td>5</td></tr> <tr><td>127</td><td>50</td><td>227</td><td>25</td><td></td><td></td></tr> <tr><td>139</td><td>130</td><td>139</td><td>130</td><td></td><td></td></tr> <tr><td>147</td><td>2,520</td><td>147</td><td>2,520</td><td></td><td></td></tr> <tr><td>112</td><td>920*</td><td>112</td><td>920*</td><td></td><td></td></tr> <tr><td>113</td><td>1,840*</td><td>113</td><td>1,840*</td><td></td><td></td></tr> <tr><td>115</td><td>110</td><td>215</td><td>55</td><td></td><td></td></tr> <tr><td>116</td><td>400</td><td>216</td><td>200</td><td></td><td></td></tr> <tr><td>117</td><td>920</td><td>217</td><td>360</td><td></td><td></td></tr> <tr><td>118</td><td>1,440</td><td>218</td><td>720</td><td></td><td></td></tr> <tr><td>125</td><td>1,060</td><td>225</td><td>980</td><td></td><td></td></tr> <tr><td>119</td><td>320</td><td>219</td><td>160</td><td></td><td></td></tr> <tr><td>120</td><td>320</td><td>220</td><td>160</td><td></td><td></td></tr> <tr><td>121</td><td>280</td><td>221</td><td>140</td><td></td><td></td></tr> <tr><td>128</td><td>1,510</td><td>128</td><td>1,510</td><td></td><td></td></tr> <tr><td>140</td><td>110</td><td>240</td><td>55</td><td></td><td></td></tr> <tr><td>141</td><td>1,280</td><td>241</td><td>640</td><td></td><td>640.00</td></tr> <tr><td>142</td><td>1,280</td><td>242</td><td>640</td><td></td><td></td></tr> <tr><td>143</td><td>480</td><td>243</td><td>200</td><td></td><td></td></tr> <tr><td>144</td><td>620</td><td>244</td><td>310</td><td></td><td></td></tr> <tr><td>122</td><td>50</td><td>122</td><td>50</td><td></td><td></td></tr> <tr><td>123</td><td>50</td><td>123</td><td>50</td><td></td><td></td></tr> <tr><td>126</td><td>180</td><td>126</td><td>180</td><td></td><td></td></tr> <tr><td>581</td><td>40</td><td>581</td><td>40</td><td></td><td></td></tr> <tr><td>148</td><td>140</td><td>248</td><td>370</td><td></td><td></td></tr> <tr><td>149</td><td>70</td><td>249</td><td>170</td><td></td><td></td></tr> <tr><td>170</td><td>140</td><td>270</td><td>370</td><td></td><td></td></tr> <tr><td>169</td><td>300</td><td>169</td><td>600</td><td></td><td></td></tr> </tbody> </table> <p>Other fee (specify):</p> <p>*Reduced by Basic Filing Fee Paid</p> <p>SUBTOTAL (3) (\$) 640.00</p> | Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | 105 | 120 | 205 | 65 | 5 | 5 | 127 | 50 | 227 | 25 | | | 139 | 130 | 139 | 130 | | | 147 | 2,520 | 147 | 2,520 | | | 112 | 920* | 112 | 920* | | | 113 | 1,840* | 113 | 1,840* | | | 115 | 110 | 215 | 55 | | | 116 | 400 | 216 | 200 | | | 117 | 920 | 217 | 360 | | | 118 | 1,440 | 218 | 720 | | | 125 | 1,060 | 225 | 980 | | | 119 | 320 | 219 | 160 | | | 120 | 320 | 220 | 160 | | | 121 | 280 | 221 | 140 | | | 128 | 1,510 | 128 | 1,510 | | | 140 | 110 | 240 | 55 | | | 141 | 1,280 | 241 | 640 | | 640.00 | 142 | 1,280 | 242 | 640 | | | 143 | 480 | 243 | 200 | | | 144 | 620 | 244 | 310 | | | 122 | 50 | 122 | 50 | | | 123 | 50 | 123 | 50 | | | 126 | 180 | 126 | 180 | | | 581 | 40 | 581 | 40 | | | 148 | 140 | 248 | 370 | | | 149 | 70 | 249 | 170 | | | 170 | 140 | 270 | 370 | | | 169 | 300 | 169 | 600 | | |
| Fee Code | Large Entity Fee (\$) | Small Entity Fee (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 120 | 205 | 65 | 5 | 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 127 | 50 | 227 | 25 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 139 | 130 | 139 | 130 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 147 | 2,520 | 147 | 2,520 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 112 | 920* | 112 | 920* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 113 | 1,840* | 113 | 1,840* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 115 | 110 | 215 | 55 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 116 | 400 | 216 | 200 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 117 | 920 | 217 | 360 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 118 | 1,440 | 218 | 720 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 125 | 1,060 | 225 | 980 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 119 | 320 | 219 | 160 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 120 | 320 | 220 | 160 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 121 | 280 | 221 | 140 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 128 | 1,510 | 128 | 1,510 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 140 | 110 | 240 | 55 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 141 | 1,280 | 241 | 640 | | 640.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 142 | 1,280 | 242 | 640 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 143 | 480 | 243 | 200 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 144 | 620 | 244 | 310 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 122 | 50 | 122 | 50 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 123 | 50 | 123 | 50 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 126 | 180 | 126 | 180 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 581 | 40 | 581 | 40 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 148 | 140 | 248 | 370 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 149 | 70 | 249 | 170 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 170 | 140 | 270 | 370 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169 | 300 | 169 | 600 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>1. BASIC FILING FEE</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>101</td><td>140</td><td>201</td><td>370</td><td>Utility filing fee</td><td></td></tr> <tr><td>106</td><td>330</td><td>206</td><td>165</td><td>Design filing fee</td><td></td></tr> <tr><td>107</td><td>510</td><td>207</td><td>255</td><td>Plant filing fee</td><td></td></tr> <tr><td>108</td><td>740</td><td>208</td><td>370</td><td>Reissuance fee</td><td></td></tr> <tr><td>114</td><td>160</td><td>214</td><td>80</td><td>Provisional filing fee</td><td></td></tr> </tbody> </table> <p>SUBTOTAL (1) (\$)</p> | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 101 | 140 | 201 | 370 | Utility filing fee | | 106 | 330 | 206 | 165 | Design filing fee | | 107 | 510 | 207 | 255 | Plant filing fee | | 108 | 740 | 208 | 370 | Reissuance fee | | 114 | 160 | 214 | 80 | Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 101 | 140 | 201 | 370 | Utility filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 106 | 330 | 206 | 165 | Design filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 107 | 510 | 207 | 255 | Plant filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 108 | 740 | 208 | 370 | Reissuance fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 114 | 160 | 214 | 80 | Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. EXTRA CLAIM FEES</p> <table border="1"> <thead> <tr> <th>Total Claims</th> <th>Extra Claims</th> <th>Fee from Law</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>70**</td><td>3**</td><td></td><td></td></tr> <tr><td>70**</td><td>3**</td><td></td><td></td></tr> </tbody> </table> <p>Multiple dependent:</p> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>103</td><td>18</td><td>203</td><td>9</td><td>Claims in excess of 20</td><td></td></tr> <tr><td>102</td><td>84</td><td>202</td><td>42</td><td>Independent claims in excess of 3</td><td></td></tr> <tr><td>104</td><td>280</td><td>204</td><td>140</td><td>Multiple dependent claims, if not paid</td><td></td></tr> <tr><td>109</td><td>84</td><td>209</td><td>42</td><td>** Reissue independent claims over original patent</td><td></td></tr> <tr><td>110</td><td>18</td><td>210</td><td>9</td><td>* Reissue claims in excess of 20 over original patent</td><td></td></tr> </tbody> </table> <p>SUBTOTAL (2) (\$)</p> | Total Claims | Extra Claims | Fee from Law | Fee Paid | 70** | 3** | | | 70** | 3** | | | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 103 | 18 | 203 | 9 | Claims in excess of 20 | | 102 | 84 | 202 | 42 | Independent claims in excess of 3 | | 104 | 280 | 204 | 140 | Multiple dependent claims, if not paid | | 109 | 84 | 209 | 42 | ** Reissue independent claims over original patent | | 110 | 18 | 210 | 9 | * Reissue claims in excess of 20 over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total Claims | Extra Claims | Fee from Law | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70** | 3** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70** | 3** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 | 18 | 203 | 9 | Claims in excess of 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 102 | 84 | 202 | 42 | Independent claims in excess of 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 104 | 280 | 204 | 140 | Multiple dependent claims, if not paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 109 | 84 | 209 | 42 | ** Reissue independent claims over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 110 | 18 | 210 | 9 | * Reissue claims in excess of 20 over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|---------------------|-------------------------|-----------------------------------|--------------|
| SUBMITTED BY | | Complete if applicable | |
| Name (Print/Type) | Floyd B. Chapman | Registration No. (Attorney/Agent) | 40,555 |
| Signature | <i>Floyd B. Chapman</i> | Telephone | 202/719-7000 |
| | | Date | 02/08/2002 |

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2838.

Best-in-Class Statement: This form is estimated to take 3-7 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



MAY 16 2002

UNITED STATES PATENT AND TRADEMARK OFFICE

#3

Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231
www.uspto.gov

WILEY REIN & FIELDING, LLP
1776 k Street, N.W
Washington, D.C. 20006

In re Application of
MOSKOWITZ et al
Application No. : 10/049,101
PCT No. : PCT/US00/21189
Int. Filing Date: 04 August 2000
Priority Date: 04 August 1999
Attorney's Docket No. : 80408.0011
For: A SECURE PERSONAL CONTENT
SERVER

DECISION ON
PETITION UNDER
37 CFR 1.137(b)

This is in response to the "Petition For Revival Of An International Application For Patent Designating The U.S. Abandoned Unintentionally Under 37 C.F.R. § 1.137(b)" filed on 08 February 2002.

BACKGROUND

On 04 August 2000, this international application was filed, claiming an earliest priority date of 04 August 1999.

No Demand electing the United States was filed in this international application Accordingly, the deadline for paying the basic national fee in the United States under 35 U.S.C. 371 and 37 CFR 1.494 was 04 April 2001. This international application became abandoned with respect to the United States at midnight on 04 April 2001 for failure pay the basic national fee.

On 08 February 2002, applicant filed in the United States Patent and Trademark Office (PTO) the instant petition, and a transmittal letter for entry into the national stage in the U.S. under 35 U.S.C. 371, which was accompanied by, *inter alia*, the U.S. basic national fee, and an executed declaration.

DISCUSSION

A grantable petition to revive an abandoned application under 37 CFR 1.137(b) must be accompanied by (1) the required reply, unless previously filed. In a nonprovisional application abandoned for failure to prosecute, the required reply may be met by the filing of a continuing application; (2) the petition fee as set forth in § 1.17(m), and (3) a statement that the entire delay in filing the required reply from the due date for the reply until the filing of a grantable petition pursuant to this paragraph was unintentional. The Commissioner may require additional information where there is a question whether the delay was unintentional; and (4) any terminal



disclaimer (and fee as set forth in § 1.20 (d)) required pursuant to paragraph (c) of this section.


Petitioner has provided: (1) the proper reply by submitting the basic national filing fee, (2) the petition fee set forth in §1.17(m) and (3) the proper statement under 137(b)(3). In this application, no terminal disclaimer is required.

Accordingly, the petition is deemed to satisfy requirements (1), (2), (3) and, (4) under 37 CFR 1.137(b).

DECISION

The petition under 37 CFR 1.137(b) is **GRANTED**.

This application is being returned to the United States Designated/Elected Office (DO/EO/US) for continued processing.


Rafael Bacares
PCT Legal Examiner
PCT Legal Office
Tel: (703) 308-6312
Fax: (703) 308-6459





UNITED STATES PATENT AND TRADEMARK OFFICE

 Commissioner for Patents, Box PCT
 United States Patent and Trademark Office
 Washington, D.C. 20211
 www.uspto.gov

| | | |
|----------------------------|-----------------------|------------------|
| U.S. APPLICATION NUMBER NO | FIRST NAMED APPLICANT | ATTY. DOCKET NO. |
| 10/049,101 | Scott A. Moskowitz | 80408.0011 |

| |
|-------------------------------|
| INTERNATIONAL APPLICATION NO. |
|-------------------------------|

PCT/US00/21189

| | |
|------------------|---------------|
| I.A. FILING DATE | PRIORITY DATE |
|------------------|---------------|

08/04/2000

08/04/1999

 Wiley Rein & Fielding
 1776 K Street NW
 Washington, DC 20006

CONFIRMATION NO. 8028

371 FORMALITIES LETTER



OC00000008153082

Date Mailed: 05/23/2002

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated Office (37 CFR 1.494):

- U.S. Basic National Fees
- Indication of Small Entity Status
- Priority Document
- Copy of the International Application
- Copy of the International Search Report
- Request for Immediate Examination
- Small Entity Statement

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date.
- \$65 Surcharge for providing the oath or declaration later than the appropriate 20 months months from the priority date (37 CFR 1.492(e)) is required.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTH FROM THE DATE OF THIS NOTICE OR BY 22 or 32 MONTHS (where 37 CFR 1.495 applies) FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

SUMMARY OF FEES DUE:

| |
|--|
| |
|--|

Total additional fees required for this application is \$65 for a Small Entity:

- \$65 Late oath or declaration Surcharge.

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

*A copy of this notice **MUST** be returned with the response.*

CHARITTA A BURT

Telephone: (703) 305-3734

PART 2 - OFFICE COPY

| U.S. APPLICATION NUMBER NO. | INTERNATIONAL APPLICATION NO. | ATTY. DOCKET NO. |
|-----------------------------|-------------------------------|------------------|
| 10/049,101 | PCT/US00/21189 | 80408.0011 |

FORM PCT/DO/EO/905 (371 Formalities Notice)

#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Scott Moskowitz et al.

U.S. Serial No.: 10/049,101

International Application No.: PCT/US00/21189

Filing Date: February 4, 2002

International Filing Date: 04 August 2000

For: A SECURE PERSONAL CONTENT SERVER

RECEIVED
01 JUL 2002
Legal Unit
International Division

**REQUEST TO "CORRECT" THE RECORD IN CONNECTION
WITH THE DECISION ON PETITION UNDER 37 CFR 1.137(B)**

Commissioner for Patents
Washington, DC 20231
Attn BOX PCT - Rafael Bacares - PCT Legal Examiner, PCT Legal Office

Dear Commissioner:

Applicants wish to thank the Examiner for the favorable Decision dated May 16, 2002, in connection with the above-identified application. Applicants submits that there were two factual inaccuracies in the text of the Decision, and accordingly, Applicants feel compelled to bring them to the Examiner's attention. Applicants do not believe, however, that the inaccuracies are material, and therefore, does not expect any change in the outcome of Applicants' petition.

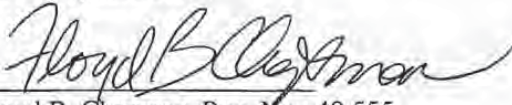
The Decision dated May 16, 2002, recites that "No Demand electing the United States was filed in this international application." This statement is incorrect. Applicants filed a Demand in the international application on March 2, 2001. A copy of this Demand is attached hereto.

The Decision further recites that an executed Declaration was submitted with the petition. This is also incorrect. Applicants did not file an executed Declaration at the time of filing the 371 application, but has since received a Notice of Missing Requirements, to which an executed declaration will be submitted in response.

Applicants do not believe the factual inaccuracies affect the substantive analysis of the prior petition, or the outcome of the decision. Accordingly, it is respectfully requested that this correction be noted in the record. If any additional information is required, I invite the Examiner to contact me at 202.719.7308 to obtain an expedited response on behalf of Applicants.

Dated: June 24, 2002

Respectfully submitted,


By 
Floyd B. Chapman, Reg. No.: 40,555
Agent for Applicants

Wiley Rein & Fielding LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Tel: 202-719-7000
Fax: 202-719-7049

WRFMAIN 1132413.2

| | | |
|---|---|--|
| (FORM PCT/2001) (REV. 9-2001) U.S. DEPARTMENT OF COMMERCE (INTERNATIONAL TRADEMARK OFFICE) | | ATTORNEY'S DOCKET NUMBER: B0408.0011 |
| TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371 | | U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 10/049101 |
| INTERNATIONAL APPLICATION NO. PCT/US00/21189 | INTERNATIONAL FILING DATE August 4, 2000 | PRIORITY DATE CLAIMED August 4, 1999 |
| TITLE OF INVENTION A SECURE PERSONAL CONTENT SERVER | | |
| APPLICANT(S) FOR DO/EO/US Scott A. MOSKOWITZ et al | | |
| Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information: | | |
| 1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. 3. <input checked="" type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)). This submission must include items (5), (6), (9) and (21) indicated below. 4. <input type="checkbox"/> The US has been elected by the expiration of 19 months from the priority date (Article 31). 5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2)) a. <input checked="" type="checkbox"/> is attached hereto (required only if not communicated by the International Bureau). b. <input checked="" type="checkbox"/> has been communicated by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US). 6. <input checked="" type="checkbox"/> An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)) a. <input checked="" type="checkbox"/> is attached hereto. b. <input type="checkbox"/> has been previously submitted under 35 U.S.C. 154(d)(4). 7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(e)(3)) a. <input type="checkbox"/> are attached hereto (required only if not communicated by the International Bureau). b. <input type="checkbox"/> have been communicated by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input checked="" type="checkbox"/> have not been made and will not be made. 8. <input type="checkbox"/> An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(e)(3)). 9. <input type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(e)(4)). 10. <input type="checkbox"/> An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(e)(5)). | | |
| Items 11 to 20 below concern document(s) or information included: | | |
| 11. <input type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 12. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. 13. <input type="checkbox"/> A FIRST preliminary amendment. 14. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. 15. <input type="checkbox"/> A substitute specification. 16. <input type="checkbox"/> A change of power of attorney and/or address letter. 17. <input type="checkbox"/> A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825. 18. <input type="checkbox"/> A second copy of the published international application under 35 U.S.C. 154(i)(4). 19. <input type="checkbox"/> A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4). 20. <input checked="" type="checkbox"/> Other items or information: PCT/IB/308 Copy of Published Application (WG 01/08628) International Search Report | | |

Form PCT/01.1

| | | | |
|---|--------------|--|--|
| U.S. APPLICATION NO. 10/049101 | | INTERNATIONAL APPLICATION NO. PCT/US00/21489 | ATTORNEY'S/CASE NO. NUMBER 80408.0011 |
| 21. <input checked="" type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO | | | \$1040.00 |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO | | | \$890.00 |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO | | | \$740.00 |
| International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) | | | \$710.00 |
| International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) | | | \$100.00 |
| ENTER APPROPRIATE BASIC FEE AMOUNT = | | | \$ 340.00 |
| Surcharge of \$120.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(c)). | | | |
| CLAIMS | NUMBER FILED | NUMBER EXTRA | RATE |
| Total claims | 51 - 20 = | 11 | x \$18.00 |
| Independent claims | 7 - 3 = | 4 | x \$84.00 |
| MULTIPLE DEPENDENT CLAIM(S) (if applicable) | | | x \$280.00 |
| TOTAL OF ABOVE CALCULATIONS = | | | \$ 1,274.00 |
| <input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. | | | \$ 637.00 |
| SUBTOTAL = | | | \$ 637.00 |
| Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)). | | | |
| TOTAL NATIONAL FEE = | | | \$ 637.00 |
| Fee for recording the enclosed assignment (37 CFR 1.21(f)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) \$40.00 per property + | | | |
| TOTAL FEES ENCLOSED = | | | \$ 637.00 |
| | | | Amount to be refunded: \$ |
| | | | charged: \$ |
| a. <input type="checkbox"/> A check in the amount of \$ _____ to cover the above fees is enclosed. | | | |
| b. <input checked="" type="checkbox"/> Please charge my Deposit Account No. <u>50-1129</u> in the amount of \$ <u>637.00</u> to cover the above fees. A duplicate copy of this sheet is enclosed. | | | |
| c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>50-1129</u> . A duplicate copy of this sheet is enclosed. | | | |
| d. <input type="checkbox"/> Fees are to be charged to a credit card. WARNING: Information on this form may become public. Credit card information should not be included in this form. Provide credit card information and authorization on PTO-2038. | | | |
| NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status. | | | |
| SEND ALL CORRESPONDENCE TO: Intellectual Property Department WILEY REIN & FIELDING, LLP 1776 K Street, N.W. Washington, D.C. 20006 Tel: 202/719-7000 Fax: 202/719-7049 | |  SIGNATURE Floyd B. Chapman NAME 40.555 REGISTRATION NUMBER | |

FORM PTO-100 (REV. 6-2001) 1001-1017

7/pt

A SECURE PERSONAL CONTENT SERVERField of Invention

The present invention relates to the secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to
5 make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security.

Authentication, verification and authorization are all handled with a combination of cryptographic and steganographic protocols to achieve efficient, trusted, secure exchange of digital information.

Cross-Reference To Related Application

This application is based on and claims the benefit of pending U.S. Patent Application Serial No. 60/147,134, filed 08/04/99, entitled, "A Secure Personal Content Server" and pending U.S. Patent Application Serial No. 60/213,489, filed
10 06/23/2000, entitled "A Secure Personal Content Server."

This application also incorporates by reference the following applications:
15 pending U.S. Patent Application Serial No. 08/999,766, filed 7/23/97, entitled "Steganographic Method and Device"; pending U.S. Patent Application Serial No. 08/772,222, filed 12/20/96, entitled "Z-Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 09/456,319, filed
20 12/08/99, entitled "Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 08/674,726, filed 7/2/96, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management"; pending U.S. Patent Application Serial No. 09/545,589, filed 04/07/2000, entitled "Method and System
25 for Digital Watermarking"; pending U.S. Patent Application Serial No. 09/046,627, filed 3/24/98, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed 04/02/98, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No.
30 09/281,279, filed 3/30/99, entitled "Optimization Methods for the Insertion, Protection, and Detection.", U.S. Patent Application Serial No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and

Cryptographic Systems" (which is a continuation-in-part of PCT application No PCT/US00/06522, filed 14 March 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed 24 March 1999); and pending U.S. Application No 60/169,274, filed 12/7/99, entitled "Systems, Methods And
5 Devices For Trusted Transactions." All of the patent applications previously identified in this paragraph are hereby incorporated by reference, in their entireties.

Background of the Invention

The music industry is at a critical inflection point. Digital technology enables anyone to make perfect replica copies of musical recordings from the
10 comfort of their home, or as in some circumstances, in an offshore factory. Internet technology enables anyone to distribute these copies to their friends, or the entire world. Indeed, virtually any popular recording is already likely available in the MP3 format, for free if you know where to look.

How the industry will respond to these challenges and protect the rights and
15 livelihoods of copyright owners and managers and has been a matter of increasing discussion, both in private industry forums and the public media. Security disasters like the cracking of DVD-Video's CSS security system have increased doubt about the potential for effective robust security implementations. Meanwhile, the success of non-secure initiatives such as portable MP3 players lead many to believe that
20 these decisions may have already been made.

Music consumers have grown accustomed to copying their music for their own personal use. This fact of life was written into law in the United States via the Audio Home Recording Act of 1992. Millions of consumers have CD players and purchase music in the Compact Disc format. It is expected to take years for a format
25 transition away from Red Book CD Audio to reach significant market penetration.

Hence, a need exists for a new and improved system for protecting digital content against unauthorized copying and distribution.

Summary of the Invention

A local content server system (LCS) for creating a secure environment for
30 digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a

plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, which SUs are capable of receiving and transmitting digital content, at least one SU, and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit.

A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably be embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.

Another embodiment of the method of the present invention comprises connecting a Satellite Unit to an local content server (LCS), sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, analyzing the message to confirm that the SU is authorized to use the LCS, retrieving a copy of the

requested content data set; assessing whether a secured connection exists between the LCS and the SU; if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS, and delivering the content data set to the SU for its use.

The SU may also request information that is located not on the LCS, but on an SECD, in which case, the LCS will request and obtain a copy from the SECD, provided the requesting SU is authorized to access the information.

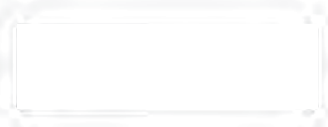
Digital technology offers economies of scale to value-added data not possible with physical or tangible media distribution. The ability to digitize information both reduces the cost of copying and enables perfect copies. This is an advantage and a disadvantage to commercial publishers who must weigh the cost reduction against the real threat of unauthorized duplication of their value-added data content. Because cost reduction is an important business consideration, securing payment and authenticating individual copies of digital information (such as media content) presents unique opportunities to information service and media content providers. The present invention seeks to leverage the benefits of digital distribution to consumers and publishers alike, while ensuring the development and persistence of trust between all parties, as well as with any third parties involved, directly or indirectly, in a given transaction.

In another approach that is related to this goal, there are instances where transactions must be allowed to happen after perceptually-based digital information can be authenticated. (Perceptually based information is information whose value is in large part, based upon its ability to be perceived by a human, and includes for example, acoustic, psychoacoustic, visual and psychovisual information.) The process of authenticating before distributing will become increasingly important for areas where the distributed material is related to a trust-requiring transaction event. A number of examples exist. These include virtual retailers (for example, an on-line music store selling CDs and electronic versions of songs); service providers (for example, an on-line bank or broker who performs transactions on behalf of a consumer); and transaction providers (for example, wholesalers or auction houses). These parties have different authentication interests and requirements. By using the

teachings of this application, these interests and requirements may be separated and then independently quantified by market participants in shorter periods of time.

5 All parties in a transaction must authenticate information that is perceptually observable before trust between the parties can be established. In today's world, information (including perceptually rich information) is typically digitized, and as a result, can easily be copied and redistributed, negatively impacting buyers, sellers and other market participants. Unauthorized redistribution confuses authenticity, non-repudiation, limit of ability and other important "transaction events." In a networked environment, transactions and interactions occur over a transmission line or a network, with buyer and seller at different points on the line or network. While such electronic transactions have the potential to add value to the underlying information being bought and sold (and the potential to reduce the cost of the transaction), instantaneous piracy can significantly reduce the value of the underlying data, if not wholly destroy it. Even the threat of piracy tends to undermine the value of the data that might otherwise exist for such an electronic transaction.

Related situations range from the ability to provably establish the "existence" of a virtual financial institution to determining the reliability of an "electronic stamp." The present invention seeks to improve on the prior art by describing optimal combinations of cryptographic and steganographic protocols for "trusted" verification, confidence and non-repudiation of digitized representations of perceptually rich information of the actual seller, vendor or other associated institutions which may not be commercial in nature (confidence building with logos such as the SEC, FDIC, Federal Reserve, FBI, etc. apply). To the extent that an entity plays a role in purchase decisions made by a consumer of goods and services relating to data, the present invention has a wide range of beneficial applications. One is enabling independent trust based on real world representations that are not physically available to a consumer or user. A second is the ability to match informational needs between buyers and sellers that may not be universally appealing or cost effective in given market situations. These include auction models based on recognition of the interests or demand of consumers and market participants—which make trading profitable by focusing specialized buyers and



sellers. Another use for the information matching is to establish limits on the liability of such institutions and profit-seeking entities, such as insurance providers or credit companies. These vendors lack appropriate tools for determining intangible asset risk or even the value of the information being exchanged. By encouraging separate and distinct "trust" arrangements over an electronic network, profitable market-based relationships can result.

The present invention can make possible efficient and openly accessible markets for tradable information. Existing transaction security (including on-line credit cards, electronic cash or its equivalents, electronic wallets, electronic tokens, etc.) which primarily use cryptographic techniques to secure a transmission channel--but are not directly associated or dependent on the information being sold--fails to meet this valuable need. The present invention proposes a departure from the prior art by separating transactions from authentication in the sale of digitized data. Such data may include videos, songs, images, electronic stamps, electronic trademarks, and electronic logos used to ensure membership in some institutional body whose purpose is to assist in a dispute, limit liability and provide indirect guidance to consumers and market participants, alike.

With an increasingly anonymous marketplace, the present invention offers invaluable embodiments to accomplish "trusted" transactions in a more flexible, transparent manner while enabling market participants to negotiate terms and conditions. Negotiation may be driven by predetermined usage rules or parameters, especially as the information economy offers potentially many competitive marketplaces in which to transact, trade or exchange among businesses and consumers. As information grows exponentially, flexibility becomes an advantage to market participants, in that they need to screen, filter and verify information before making a transaction decision. Moreover, the accuracy and speed at which decisions can be made reliably enables confidence to grow with an aggregate of "trusted transactions". "Trusted transactions" beget further "trusted transactions" through experience. The present invention also provides for improvements over the prior art in the ability to utilize different independently important "modules" to enable a "trusted transaction" using competitive cryptographic and steganographic elements, as well as being able to support a wide variety of perceptually-based

media and information formats. The envisioned system is not bound by a proprietary means of creating recognition for a good or service, such as that embodied in existing closed system. Instead, the flexibility of the present invention will enable a greater and more diverse information marketplace.

5 The present invention is not a "trusted system", *per se*, but "trusted transactions" are enabled, since the same value-added information that is sought may still be in the clear, not in a protected storage area or closed, rule-based "inaccessible virtual environment"

10 A related additional set of embodiments regards the further separation of the transaction and the consumer's identification versus the identification of the transaction only. This is accomplished through separated "trusted transactions" bound by authentication, verification and authorization in a transparent manner. With these embodiments, consumer and vendor privacy could be incorporated. More sophisticated relationships are anticipated between parties, who can mix information
15 about their physical goods and services with a transparent means for consumers, who may not be known to the seller, who choose not to confide in an inherently closed "trusted system" or provide additional personal information or purchasing information (in the form of a credit card or other electronic payment system), in
20 advance of an actual purchase decision or ability to observe (audibly or visibly) the content in the clear. This dynamic is inconsistent with the prior art's emphasis on access control, not transparent access to value-added information (in the form of goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

25 These embodiments may include decisions about availability of a particular good or service through electronic means, such as the Internet, or means that can be modularized to conduct a transaction based on interconnection of various users (such as WebTV, a Nintendo or Sony game console with network abilities, cellular phone, PalmPilot, etc.). These embodiments may additionally be implemented in traditional
30 auction types (including Dutch auctions). Consumers may view their anonymous marketplace transactions very differently because of a lack of physical human interactions, but the present invention can enable realistic transactions to occur by maintaining open access and offering strict authentication and verification of the

information being traded. This has the effect of allowing legacy relationships, legacy information, and legacy business models to be offered in a manner which more closely reflects many observable transactions in the physical world. The tremendous benefits to sellers and consumers is obvious; existing transactions need not reduce their expectations of security. As well, the ability to isolate and quantify aspects of a transaction by module potentially allows for better price determinations of intangible asset insurance, transaction costs, advertising costs, liability, etc. which have physical world precedent.

It is contemplated that the publisher and/or owner of the copyrights will want to dictate restrictions on the ability of the purchaser to use the data being sold. Such restrictions can be implemented through the present invention, which presents a significant advantage over the prior art (which attempts to effect security through access control and attempted tight reigns over distribution). See US Pat. No. 5,428,606 for a discussion on democratizing digital information exchange between publishers and subscribers of said information.

A goal for providers of value-added content is to maximize profits for the sale of their content. Marketing and promotion of the informational content cannot be eliminated, considering the ever increasing amount of information vying for consumers and other market participant's attention. Nonetheless, in a market where the goods are speculatively valued, marketing budgets are inherently constrained, as you are trying to create demand for a product with little inherent value. Where such markets have participants, both buyers and sellers and their respective agents, with access to the same information in real time, market mechanisms efficiently price the market goods or services. These markets are characterized by "price commoditization" so buyers and sellers are limited to differentiating their offerings by selection and service. If the markets are about information itself, it has proven more difficult to accurately forecast the target price where sellers can maximize their profits. Quality and quantity provide different evaluation criteria of selection and service relating to the information being traded. The present invention regards a particular set of implementations of value-added content security in markets which may include unsecured and secure versions of the same value-added data (such as

songs, video, research, pictures, electronic logos, electronic trademarks, value-added information, etc.).

Transactions for value-added information can occur without any physical location. So, there is a need for a secure personal content server for which the value
5 added information can be offered for transactions in a manner similar to real world transactions. One feature is to offer seemingly similar value added information in differing quality settings. These settings have logical relationships with fidelity and discreteness and are determined by market participants. Another issue is that because purchasers may be anonymous to sellers, it is more important to have a
10 particular value-added information object available so that market participants can fulfill their role as consumers.

One fundamental weakness of current information markets is the lack of mechanisms to ensure that buyers and sellers can reach pricing equilibrium. This deficit is related to the "speculative", "fashion", and "vanity" aspects of perceptual
15 content (such as music, video, and art or some future recognition to purchasers). For other goods and services being marketed to an anonymous marketplace, market participants may never see (and indeed, may choose to never see, an actual location where the transaction may physically occur. A physical location may simply not exist. There are a number of such virtual operations in business today, which would
20 benefit from the improvements offered under the present system.

The present invention also seeks to provide improvements to the art in enabling a realistic model for building trust between parties (or their agents) not in a "system", per se. Because prior art systems lack any inherent ability to allow for information to flow freely to enable buyers and sellers to react to changing market
25 conditions. The present invention can co-exist with these "trusted systems" to the extent that all market participants in a given industry have relatively similar information with which to price value-added data. The improvement over such systems, however, addresses a core features in most data-added value markets: predictions, forecasts, and speculation over the value of information is largely an
30 unsuccessful activity for buyers and sellers alike. The additional improvement is the ability to maintain security even with unsecured or legacy versions of value-added information available to those who seek choices that fit less quantitative criteria--

"aesthetic quality" of the information versus "commercial price". Purchase or transaction decisions can be made first by authenticating an electronic version of a song, image, video, trademark, stamp, currency, etc.

5 Additional anticipated improvements include the ability to support varying pricing models such as auctions that are difficult or impossible to accomplish under existing prior art that leaves all access and pricing control with the seller alone, and the separation of the transaction from the exchange of the value-added information, which gives more control to buyers over their identities and purchasing habits, (both sensitive and separately distinct forms of "unrelated" value-added information)

10 Essentially, no system known in the art allows for realistic protocols to establish trust between buyers and sellers in a manner more closely reflecting actual purchasing behavior of consumers and changing selling behavior of sellers. The goal in such transactions is the creation of trust between parties as well as "trusted relationships" with those parties. The present invention is an example of one such

15 system for media content where the "aesthetic" or "gestalt" of the underlying content and its characteristics is a component of buying habits. Without an ability to open distribution systems to varying buyers and sellers, media content may be priced at less than maximum economic value and buyers may be deprived of a competitive, vigorous marketplace for exciting media content from many different creative

20 participants.

To the extent that recognition plays such a key role in an information economy, value-added data should be as accessible as possible to the highest number of market participants in the interests of furthering creativity and building a competitive marketplace for related goods and services. This is to the benefit of

25 both buyers and sellers as well as the other participants in such an economic ecosystem. The Internet and other transmission-based transactions with unknown parties presents a number of challenges to information vendors who wish to develop customer relations, trust and profitable sales. The information economy is largely an anonymous marketplace, thus, making it much more difficult to identify consumers

30 and sellers. The present invention provides remedies to help overcome these weaknesses.

The present invention is concerned with methods and systems which enable secure, paid exchange of value-added information, while separating transaction protocols. The present invention improves on existing means for distribution control by relying on authentication, verification and authorization that may be flexibly determined by both buyers and sellers. These determinations may not need to be predetermined, although pricing matrix and variable access to the information opens additional advantages over the prior art. The present invention offers methods and protocols for ensuring value-added information distribution can be used to facilitate trust in a large or relatively anonymous marketplace (such as the Internet's World Wide Web).

We now define components of the preferred embodiments for methods, systems, and devices.

Definitions:

Local Content Server (LCS): A device or software application which can securely store a collection of value-added digital content. The LCS has a unique ID.

Secure Electronic Content Distributor (SECD): An entity, device or software application which can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. In cryptographic terms, the SECD acts as a "certification authority" or its equivalent. SECDs may have differing arrangements with consumers and providers of value-added information. (The term "content" is used to refer generally to digital data, and may comprise video, audio, or any other data that is stored in a digital format).

Satellite Unit (SU): A portable medium or device which can accept secure digital content from a LCS through a physical, local connection and which can either play or make playable the digital content. The SU may have other functionality as it relates to manipulating the content, such as recording. The SU has a unique ID. An SU may be a CD player, a video camera, a backup drive, or other electronic device which has a storage unit for digital data.

LCS Domain: A secure medium or area where digital content can be stored, with an accompanying rule system for transfer of digital content in and out of the LCS Domain. The domain may be a single device or multiple devices—all of which have some common ownership or control. Preferably, a LCS domain is linked to a

single purchasing account. Inside the domain, one can enjoy music or other digital data without substantial limitations—as typically a license extends to all personal use.

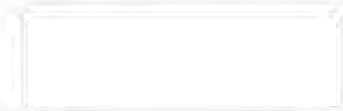
SecureChannel™: A secure channel to pass individualized content to differentiate authentic content from legacy or unauthorized, pirated content. For example, the Secure Channel may be used as an auxiliary channel through which members of the production and distribution chain may communicate directly with individual consumers. Preferably, the Secure Channel is never exposed and can only be accessed through legitimate methods. SecureChannel may carry a value-adding component (VAC). The ability to provide consumers with value adding features will serve to give consumers an incentive to purchase new, secure hardware and software that can provide the additional enhanced services. The SecureChannel may also include protected associated data—data which is associated with a user and/or a particular set of content.

Standard Quality: A transfer path into the LCS Domain which maintains the digital content at a predetermined reference level or degrades the content if it is at a higher quality level. In an audio implementation, this might be defined as Red Book CD Quality (44100 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of a subset of VAC's or a quality level associated with particular VAC's. If a VAC is not in the subset, it is not passed. If a VAC is above the defined quality level, it is degraded.

Low Quality: A transfer path into the LCS Domain which degrades the digital content to a sub-reference level. In an audio implementation, this might be defined as below CD Quality (for instance, 32000 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of an absence of VAC's or a degraded quality level associated with particular VAC's.

High Quality: A transfer path into the LCS Domain which allows digital content of any quality level to pass unaltered. This transfer path can alternately be defined in terms of a complete set of VAC's or the highest quality level available associated with particular VAC's.

Rewritable Media: An mass storage device which can be rewritten (e.g. hard drive, CD-RW, Zip cartridge, M-D drive, etc.)



Read-Only Media: A mass storage device which can only be written once (e.g. CD-ROM, CD-R, DVD, DVD-R, etc.) Note: pre-recorded music, video, software, or images, etc. are all "read only" media.

Unique ID: A Unique ID is created for a particular transaction and is unique to that transaction (roughly analogous to a human fingerprint). One way to generate a Unique ID is with a one-way hash function. Another way is by incorporating the hash result with a message into a signing algorithm will create a signature scheme. For example, the hash result may be concatenated to the digitized, value added information which is the subject of a transaction. Additional uniqueness may be observed in a hardware device so as to differentiate that device, which may be used in a plurality of transactions, from other similar devices.

Value-added: Value-added information is differentiated from non-commoditized information in terms of its marketability or demand, which can vary, obviously, from each market that is created for the information. By way of example, information in the abstract has no value until a market is created for the information (i.e., the information becomes a commodity). The same information can be packaged in many different forms, each of which may have different values. Because information is easily digitized, one way to package the "same" information differently is by different levels of fidelity and discreteness. Value is typically bounded by context and consideration.

Authentication: A receiver of a "message" (embedded or otherwise within the value-added information) should be able to ascertain the original of the message (or by effects, the origin of the carrier within which the message is stored). An intruder should not be able to successfully represent someone else. Additional functionality such as Message Authentication Codes (MAC) could be incorporated (a one-way hash function with a secret key) to ensure limited verification or subsequent processing of value-added data.

Verification: In cryptographic terms, "verification" serves the "integrity" function to prevent an intruder from substituting false messages for legitimate ones. In this sense, the receiver of the message (embedded or otherwise present within the value-added information) should be assured that the message was not modified or altered in transit.

One-way hash function One-way hash functions are known in the art. A hash function is a function which converts an input into an output, which is usually a fixed-sized output. For example, a simple hash function may be a function which accepts a digital stream of bytes and returns a byte consisting of the XOR function of all of the bytes in the digital stream of input data. Roughly speaking, the hash function may be used to generate a "fingerprint" for the input data. The hash function need not be chosen based on the characteristics of the input. Moreover, the output produced by the hash function (i.e., the "hash") need not be secret, because in most instances it is not computationally feasible to reconstruct the input which yielded the hash. This is especially true for a "one-way" hash function—one that can be used to generate a hash value for a given input string, but which hash cannot be used (at least, not without great effort) to create an input string that could generate the same hash value.

Authorization: A term which is used broadly to cover the acts of conveying official sanction, permitting access or granting legal power to an entity.

Encryption: For non digitally-sampled data, encryption is data scrambling using keys. For value-added or information rich data with content characteristics, encryption is typically slow or inefficient because content file sizes tend to be generally large. Encrypted data is called "ciphertext".

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the value-added or information rich data at the inherent granularity of the file format. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. Scrambling is efficient for larger media files and can be used to provide content in less than commercially viable or referenced quality levels. Scrambling is not as secure as encryption for these applications, but provides more fitting manipulation of media rich content in the context of secured distribution. Scrambled data is also called "ciphertext" for the purposes of this invention. Encryption generally acts on the data as a whole, whereas scrambling is applied often to a particular subset of the data concerned with the granularity of the data, for instance the file formatting. The result is that a smaller amount of data is "encoded" or "processed" versus strict encryption, where all of the data is "encoded" or "processed." By way of example, a cable TV signal

-15-

can be scrambled by altering the signal which provides for horizontal and vertical tracking, which would alter only a subset of the data, but not all of the data—which is why the audio signal is often untouched. Encryption, however, would generally so alter the data that no recognizable signal would be perceptually appreciated. Further, the scrambled data can be compared with the unscrambled data to yield the scrambling key. The difference with encryption is that the ciphertext is not completely random, that is, the scrambled data is still perceptible albeit in a lessened quality. Unlike watermarking, which maps a change to the data set, scrambling is a transfer function which does not alter or modify the data set.

10 **Detailed Discussion of Invention**

The LCS Domain is a logical area inside which a set of rules governing content use can be strictly enforced. The exact rules can vary between implementations, but in general, unrestricted access to the content inside the LCS Domain is disallowed. The LCS Domain has a set of paths which allow content to enter the domain under different circumstances. The LCS Domain also has paths which allow the content to exit the domain.

A simple example provides insight into the scope of an LCS domain. If an LCS is assigned to an individual, then all music, video, and other content data which has lawfully issued to the individual may be freely used on that person's LCS domain (though perhaps "freely" is misleading, as in theory, the individual has purchased a license). A LCS Domain may comprise multiple SUs, for example, a video player, a CD player, etc. An individual may be authorized to take a copy of a song and play it in another's car stereo, but only while the individual's device or media is present. Once the device is removed, the friend's LCS will no longer have a copy of the music to play.

The act of entering the LCS Domain includes a verification of the content (an authentication check). Depending upon the source of the content, such verification may be easier or harder. Unvalidateable content will be subjected to a quality degradation. Content that can be validated but which belongs to a different LCS Domain will be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between domains.

When content leaves the LCS Domain, the exiting content is embedded with information to uniquely identify the exiting content as belonging to the domain from which the content is leaving. It is allowed to leave at the quality level at which the content was originally stored in the LCS Domain (i.e. the quality level determined by the validation path). For example, the exiting content may include an embedded digital watermark and an attached hash or digital signature, the exiting content may also include a time stamp—which itself may be embedded or merely attached). Once it has exited, the content cannot return to the domain unless both the watermark and hash can be verified as belonging to this domain. The presence of one or the other may be sufficient to allow re-entry, or security can be set to require the presence of more than one identification signal.

This system is designed to allow a certifiable level of security for high-quality content while allowing a device to also be usable with unsecured content at a degraded quality level. The security measures are designed such that a removal of the watermark constitutes only a partial failure of the system. The altered content (i.e., the content from which the watermark has been removed or the content in which the watermark has been degraded) will be allowed back into the LCS Domain, but only at a degraded quality level, a result of the watermark destruction and subsequent obscurity to the system. Consumers will not be affected to the extent that the unauthorized content has only been degraded, but access has not been denied to the content. Only a complete forgery of a cryptographically-secure watermark will constitute a complete failure of the system. For a discussion on such implementations please see US Pat. No. 5,613,004, US Pat. No. 5,687,236, US Pat. No. 5,745,569, US Pat. No. 5,822,432, US Pat. No. 5,889,868, US Pat. No. 5,905,800, included by reference in their entirety and pending U.S. patent applications with Serial No. 09/046,627 "Method for Combining Transfer Function...", Serial No. 09/053,628 "Multiple Transform Utilization and Application for Secure Digital Watermarking", Serial No. 08/775,216 "Steganographic Method and Device", Serial No. 08/772,222 "Z-Transform Implementation...", Serial No. 60/125990 "Utilizing Data Reduction in Steganographic and Cryptographic Systems".

Provable security protocols can minimize this risk. Thus the embedding system used to place the watermark does not need to be optimized for robustness, only for imperceptibility (important to publishers and consumers alike) and security (more important to publishers than to consumers). Ideally, as previously disclosed, security should not obscure the content, or prevent market participants from accessing information, which in the long term, should help develop trust or create relationships.

The system can flexibly support one or more "robust" watermarks as a method for screening content to speed processing. Final validation, however, relies upon the fragile, secure watermark and its hash or digital signature (a secure time stamp may also be incorporated). Fragile watermarks, meaning that signal manipulations would affect the watermark, may be included as a means to affect the quality of the content or any additional attributes intended to be delivered to the consumer.

15 **LCS Functions**

The LCS provides storage for content, authentication of content, enforcement of export rules, and watermarking and hashing of exported content. Stored content may be on an accessible rewritable medium, but it must be stored as ciphertext (encrypted or scrambled), not plain text, to prevent system-level extraction of the content. This is in contrast to the prior art which affix or otherwise attach meta-data to the content for access control by the variously proposed systems.

Typically, an LCS receives secured data from one or more SECDs. The SECD transfers content only after it has been secured. For example, the SECD may use an individualized cryptographic container to protect music content while in transit. Such a container may use public/private key cryptography, ciphering and/or compression, if desired.

The LCS may be able to receive content from a SECD, and must be able to authenticate content received via any of the plurality of implemented paths. The LCS must monitor and enforce any rules that accompany received content, such as number of available copies. Finally, it is preferred for the LCS to watermark all exported material (with the exception of Path 6 - see below) and supply a hash made from the unique ID of the LCS and the content characteristics (so as to be



maintained perceptually within the information and increase the level of security of the watermark).

SU Functions

5 The SU enables the content to be usable away from the LCS. The SU is partially within the LCS Domain. A protocol must exist for the SU and LCS to authenticate any connection made between them. This connection can have various levels of confidence set by the level of security between the SU and LCS and determinable by a certification authority or its equivalent, an authorized site for the content, for example. The transfer of content from the SU to the LCS without
10 watermarking is allowed. However, all content leaving the SU must be watermarked. Preferably, the SU watermark contains a hash generated from the SU's Unique ID and the content characteristics of the content being transferred. If the content came from a LCS, the SU watermark must also be generated based, in part, upon the hash received from the LCS. The LCS and SU watermarking
15 procedures do not need to be the same. However, the LCS must be able to read the SU watermarks for all different types of SU's with which it can connect. The SU does not need to be able to read any LCS watermarks. Each LCS and SU must have separate Unique IDs.

Sample Embodiment

20 BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

25 FIG. 1 shows in block diagram form a system for one embodiment of an LCS, showing the possible paths for content to enter and exit the system.

FIG. 2 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the rewritable media.

FIG. 3 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the read-only media.

30 FIG. 4 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the satellite unit.

FIG. 5 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain.

FIG. 6 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain from the read-only media.

5 FIG. 7 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the SU to a receiver other than the LCS.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment of the present invention and its advantages are best understood by referring to FIGs. 1 through 7 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

10 FIG. 1 is a block diagram showing the components of a sample LCS system and showing the possible paths for content to enter and leave the LCS. In the embodiment of Figure 1, the LCS is a general purpose computing device such as a PC with software loaded to emulate the functions of a LCS. The LCS of Figure 1 has a Rewritable media (such as a hard drive), a Read-Only media (such as a CD-ROM drive), and software to control access (which software, in effect, defines the "LCS Domain"). The Secure Electronic Content Distributor (SECD) is connected via a network (such as the Internet, intranet, cable, satellite link, cellular communications network, or other commonly accepted network). The Satellite

15 Unite (SU) is a portable player which connects to the LCS and/or to other players where applicable (for example by way of a serial interface, USB, IEEE 1394, infrared, or other commonly used interface protocol). FIG. 1 also identifies seven (7) path ways.

20 Path 1 depicts a secure distribution of digital content from a SECD to a LCS. The content can be secured during the transmission using one or more 'security protocols' (e.g., encryption or scrambling). Moreover, a single LCS may have the capability to receive content transmissions from multiple SECDs, and each SECD may use the same security protocols or different security protocols. In the context of FIG. 1, however, only a single SECD is displayed. It is also contemplated that the same SECD may periodically or randomly use different security protocols. A typical security protocol uses an asymmetric cryptographic system, an example being a public key cryptography system where private and public key pairs allow the

25

30

LCS to authenticate and accept the received content. Another security protocol may involve the ability to authenticate the received content using a signature scheme.

In FIG. 2, content enters the LCS Domain from the rewritable media (such as a hard drive). This communication path is identified as Path 2 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the quality of the content is downgraded to Low Quality before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain. Optionally, if a watermark is present, the hash may be checked as further verification, and if the hash matches, the content is allowed in at High Quality. If it does not match, the content is rejected. If the extracted watermark does not match the expected watermark, then the content is denied access to the LCS Storage (i.e., the content is rejected).

In FIG. 3, content enters the LCS Domain from the Read-Only media. This communication path is identified as Path 3 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the LCS attempts to further analyze the content using other methods (i.e., other than watermarking) to try and verify the content for originality. If the content cannot be verified or is deemed to have been altered, then the content is downgraded to Standard Quality (or even Low Quality) before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, or in the event that the content is verified by means other than the watermark, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain (which is likely to be High Quality). For example, the Read-Only media may also contain a media-based identifier which verifies the content as an original, as opposed to a copy—and hence, a non-watermark method may be used to verify authenticity.

Optionally, even in the event of a watermark match, a hash may be checked as further verification; and if the hash matches, the content is allowed in at High

Quality, but if there is no match, the content is rejected. If the extracted watermark does not match the expected watermark, or if the LCS is unable to identify any other method for verifying the content's authenticity, then the content may be denied access to the LCS Storage (i.e., the content may be rejected), or if preferred by the user, the content may be permitted into the system at a degraded quality level. It is the user's prerogative to decide how the system will treat non-authenticated content, as well as legacy content.

In FIG. 4, content enters the LCS Domain from the satellite unit. This communication path is identified as Path 4 on FIG. 1. Content from an SU is marked with an SU watermark before exiting the SU. The LCS analyzes the content from the SU for watermarks, and in particular to determine if there is a watermark that matches that of the LCS. If the watermarks match, the content is permitted access to the LCS at the highest quality level. If there is a mismatch, then the content is denied access (i.e., the content is rejected). If the content does not contain a watermark, the quality is downgraded to Low Quality before permitting access to the LCS. Optionally, even in the event of a watermark match, a hash may be checked as further verification, and access at the highest quality level may depend upon both a match in watermarks and a match in hashes.

In FIG. 5, content is shown leaving the LCS Domain. This communication path is identified as Path 5 on FIG. 1. Content is retrieved from the LCS storage and then the content may be watermarked with a watermark that is unique to the LCS (for example, one that is based upon the LCS's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc. After watermarking, the content may be permitted to exit the LCS Domain, and may be exported to a device outside the LCS Domain, including for example, a rewritable media, a viewer, player, or other receiver.

In FIG. 6, content is shown leaving the LCS Domain. This communication path is identified as Path 6 on FIG. 1. This path is similar to Path 5, with a few

important differences. The output receiver is an SU, and because the receiver is an SU, the content may leave the LCS without being watermarked. Path 6 requires a secure protocol to determine that the receiver is in fact an SU. Once the path is verified, the content can be exported without a watermark. The LCS may optionally transmit the content together with a hash value which will be uniquely associated with the content.

In FIG. 7, content is shown leaving the SU, to a receiver other than the LCS. This communication path is identified as Path 7 on FIG. 1. Content is retrieved from the SU storage and then the content may be watermarked with a watermark that is unique to the SU (for example, one that is based upon the SU's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc., and may even include the hash which the LCS attached to the content. After watermarking, the content may be permitted to exit the SU, and may be exported to a device other than the LCS, including for example, a rewritable media, a viewer, player, or other receiver. The quality level of the content leaving the LCS is generally the same quality level as that of the content when stored internally to the LCS.

The system of the present invention is utilized to complete digital data transactions. A typical transaction would have the following steps:

- 1.) Using an LCS, a user connects to a SECD
- 2.) The user reviews a collection of data sets which are available for license (which for purposes of this application, may be equated with a purchase). The user then selects a data set (e.g., a song or other content), and purchases (or otherwise obtains the right to receive) a copy of the data set. (The user may transmit purchase information, for example, credit card information, using digital security that is known in the art of electronic commerce.)
- 3.) The SECD transmits the secured content to the LCS. Before transmitting any digital content, the SECD embeds at least one watermark and may

also transmit (perhaps through cryptography) at least one hash value along with the data being transmitted. The at least one hash value may be embedded with the at least one watermark or may be attached to the beginning or end of the data being transmitted. Alternately, the hash output may be combined in ways that are known in the art.

4.) The LCS optionally may send its public key to the SECD, in which case the SECD may use the LCS public key to apply an additional security measure to the data to be transmitted, before the data is actually transmitted to the LCS.

5.) The LCS receives the secured content transmitted by the SECD. The LCS may optionally use its private key to remove the additional layer of security which was applied with the LCS's public key.

6.) The LCS may authenticate the secure content that was received from the SECD by checking the watermark(s) and/or hash values. Optionally, the LCS may unpack the secured content from its security wrapper and/or remove any other layers of security. If the content can be authenticated, the content may be accepted into the LCS domain. Otherwise, it may be rejected.

Fragile Watermark Structure

A fragile watermark—one that is encoded in the LSB of each 16 bit sample—can actually hold all of the data that would typically comprise the information being transmitted in the SecureChannel™. At a typical sampling rate of 44.1 kHz, there is 88,200 16 bit samples for each second of data in the time domain (44,100 x 2 stereo channels). This provides 88,200 bits per second which may be used for storing a fragile watermark. A typical 3 minute stereo song could therefore accommodate 1.89 MB of data for a fragile watermark. (The watermark is called fragile, because it is easily removed without greatly sacrificing the quality of the audio data.) 1.89 MB represents an immense capacity relative to the expected size of the typical data to be transmitted in a SecureChannel (100 - 200 K).

Preferably, the fragile watermark is bound to a specific copy of a specific song, so that "information pirates" (i.e., would-be thieves) cannot detect a watermark and then copy it onto another song in an effort to feign authorization when none exists. A fragile watermark may also contain information which can be utilized by various receivers which might receive the signal being packaged. For

instance, a fragile watermark may contain information to optimize the playback of a particular song on a particular machine. A particular example could include data which differentiates an MP3 encoded version of a song and an AAC encoded version of the same song.

- 5 One way to bind a fragile watermark to a specific data set is through the use of hash functions. An example is demonstrated by the following sequence of steps
- 1) A digital data set (e.g., a song) is created by known means (e.g., sampling music at 44.1 kHz, to create a plurality of 16 bit data sets). The digital data set comprises a plurality of sample sets (e.g., a plurality of 16 bit data sets).
 - 10 2) Information relative to the digital data set (e.g., information about the version of the song) is transformed into digital data (which we will call the SecureChannel data), and the SecureChannel data is then divided into a plurality of SecureChannel data blocks, each of which blocks may then be separately encoded.
 - 15 3) A first block of the SecureChannel data is then is encoded into a first block of sample sets (the first block of sample sets comprising—at a minimum—a sufficient number of sample sets to accommodate the size of the first block of Secure Channel Data), for example by overwriting the LSB of each sample in the first block of sample sets.
 - 20 4) A hash pool is created comprising the first block of encoded sample sets.
 - 5) A first hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data.
 - 25 6) The first hash value is then encoded into a second block of sample sets, the second block of sample sets being sufficient in size to accommodate the size of the first hash value.
 - 7) The second block of sample sets is then added to the hash pool
 - 8) A second block of the SecureChannel data is then is encoded into a third block of sample sets.
 - 30 9) The third block of encoded sample sets is added to the hash pool

10) A second hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data,

11) The second hash value is then encoded into a fourth block of sample sets.

Steps 7-11 are then repeated for successive blocks of SecureChannel data until all of the SecureChannel data is encoded. Understand that for each block of SecureChannel data, two blocks of content data are utilized. Moreover, for efficiency, one could use a predetermined subset of the samples in the hash pool, instead of the whole block.

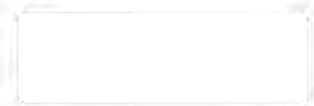
Each SecureChannel block may, for example, have the following structure

```
{
    long   BlockIdentifier;    //A code for the type of block
    long   BlockLength;      //The length of the block
    ..     ..                //Block data of a length matching BlockLength
    char   IdentityHash[hashSize],
    char   InsertionHash[hashSize];
}
```

In theory, each SecureChannel block may be of a different type of block (i.e., may begin with a different BlockIdentifier). In operation, a software application (or even an ASIC) may read the BlockIdentifier and determine whether it is a recognized block type for the particular application. If the application does not recognize the block type, the application may use the BlockLength to skip this block of SecureChannel.

Certain block types will be required to be present if the SecureChannel is going to be accepted. These might include an identity block and a SecureChannel hash block. The SecureChannel data may or may not be encrypted, depending on whether the data is transfer-restricted (a type of value-adding component, that is, VAC) or simply informative. For instance, user-added SecureChannel data need not be encrypted. A BlockIdentifier may also be used to indicate whether a SecureChannel data block is encrypted or not.

Robust Open Watermark (ROW)



A Robust-Open Watermark may be used to divide content into three categories. (The term "open watermark" is used merely to indicate that the watermark relies on a secret which is shared by an entire class of devices, as opposed to a secure watermark—which is readable only by a single member of a class of devices.) A binary setting may be used, whereby one state (e.g., "1") may be used to identify secure protected content—such as content that is distributed in a secured manner. When the LCS detects a secured status (e.g., by determining that the ROW is "1"), the content must be accompanied by an authenticatable SecureChannel before the content is permitted to enter the LCS Domain (e.g., electronic music distribution or EMD content). The other binary state (e.g., "0") may be used to identify unsecured content, for example, non-legacy media that is distributed in a pre-packaged form (e.g. CD's). When the binary setting is "0", the content may or may not have a SecureChannel. Such "0 content" shall only be admitted from a read-only medium in its original file format (e.g., a 0 CD shall only be admitted if it is present on a Redbook CD medium). On the other hand, if the ROW is absent, then the LCS will understand that the content is "legacy". Legacy content may be admitted, or optionally, may be checked for a fragile watermark—and then admitted only if the fragile watermark is present. It would be possible to permit unfettered usage of legacy content—though again, it is the prerogative of the user who sets up the LCS.

Robust Forensic Watermark

Preferably, a robust forensic watermark is not accessible in any way to the consumer—or to "information pirates." A forensic watermark may be secured by a symmetric key held only by the seller. A transaction ID may be embedded at the time of purchase with a hash matching the symmetric key. The watermark is then embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of such a watermark is not limited by real-time/low cost constraints. The recovery will typically only be attempted on known pirated material, or material which is suspected of piracy. A recovery time of 2 hours on a 400 MHz PC may, therefore, be reasonable.

Sample Embodiment - Renewability

The system of the present invention contemplates the need for updating and replacing previously-embedded watermarks (which may be thought of generally as "renewing" a watermark). If someone is able to obtain the algorithms used to embed a watermark—or is otherwise able to crack the security, it would be desirable to be able to embed a new watermark using a secure algorithm. New watermarks, however, cannot be implemented with complete success over night, and thus, there inevitably will be transition periods where older SPCS are operating without updated software. In such a transition period, the content must continue to be recognizable to both the old SPCSs and the upgraded SPCSs. A solution is to embed both the original and the upgraded watermarks into content during the transition periods. Preferably, it is the decision of the content owner to use both techniques or only the upgraded technique.

The operation of the system of the present invention is complicated, however, by the presence of "legacy" digital content which is already in the hands of consumer (that is, digital content that was commercially distributed before the advent of watermarking systems) because legacy content will continue to be present in the future. Moreover, pirates who distribute unauthorized content will also complicate matters because such unauthorized copies are likely to be distributed in the same formats as legacy content. As it is unlikely that such unwatermarked content can ever be completely removed, the present system must try to accommodate such content.

Hardware can be configured to read old ROW content and extract the old ROW and insert in the content a new ROW

Sample Embodiment – SPCS Audio Server

Tables 1, 2 and 3 depict a sample embodiment for an SPCS Audio Server, and in particular show how secured content packages are created as downloadable units (Table 1), how the LCS works on the input side for an SPCS Audio Server (Table 2), and how the LCS works on the output side (Table 3).

While the invention has been particularly shown and described by the foregoing detailed description, it will be understood by those skilled in the art that various other changes in form and detail may be made without departing from the spirit and scope of the invention.

Table 1

SAMPLE EMBODIMENT- SPCS Audio Server Stage

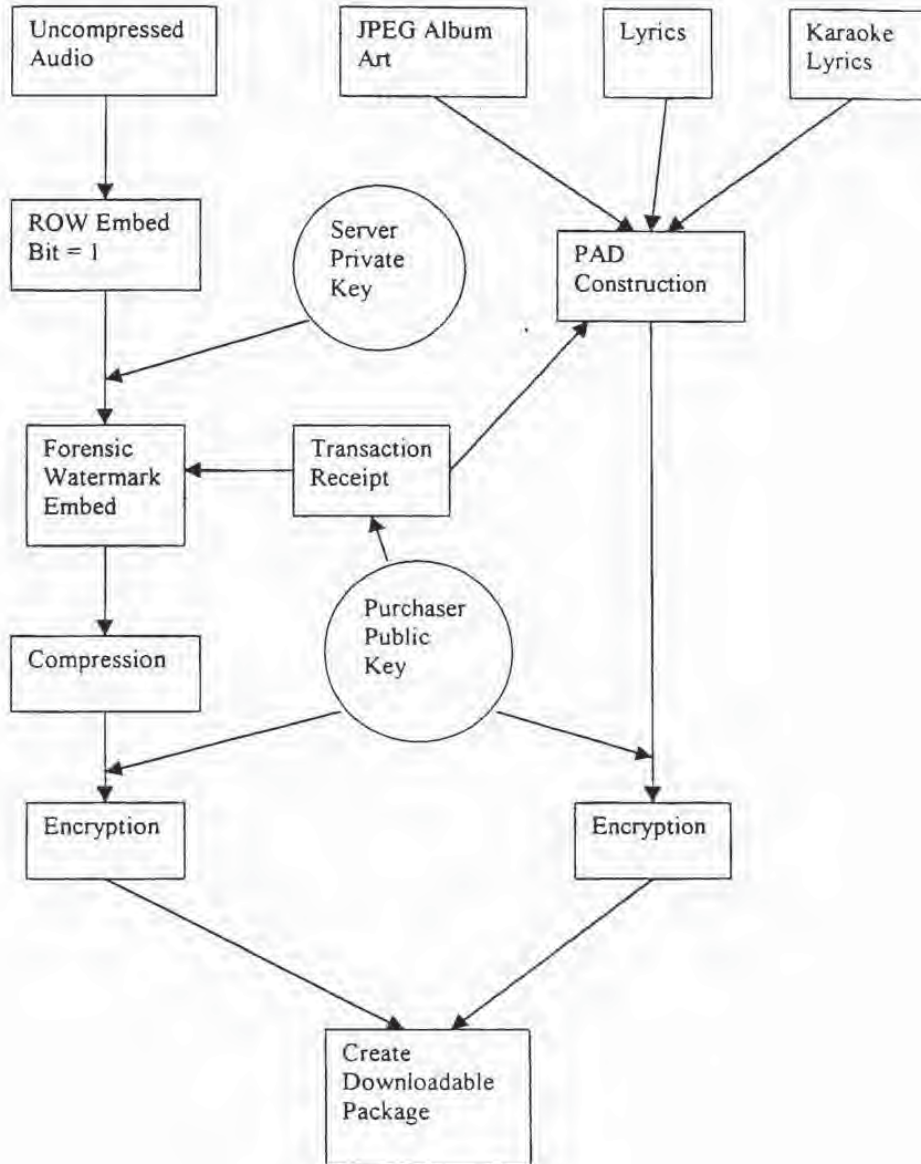


Table 2
SPCS Audio Player Input Stage

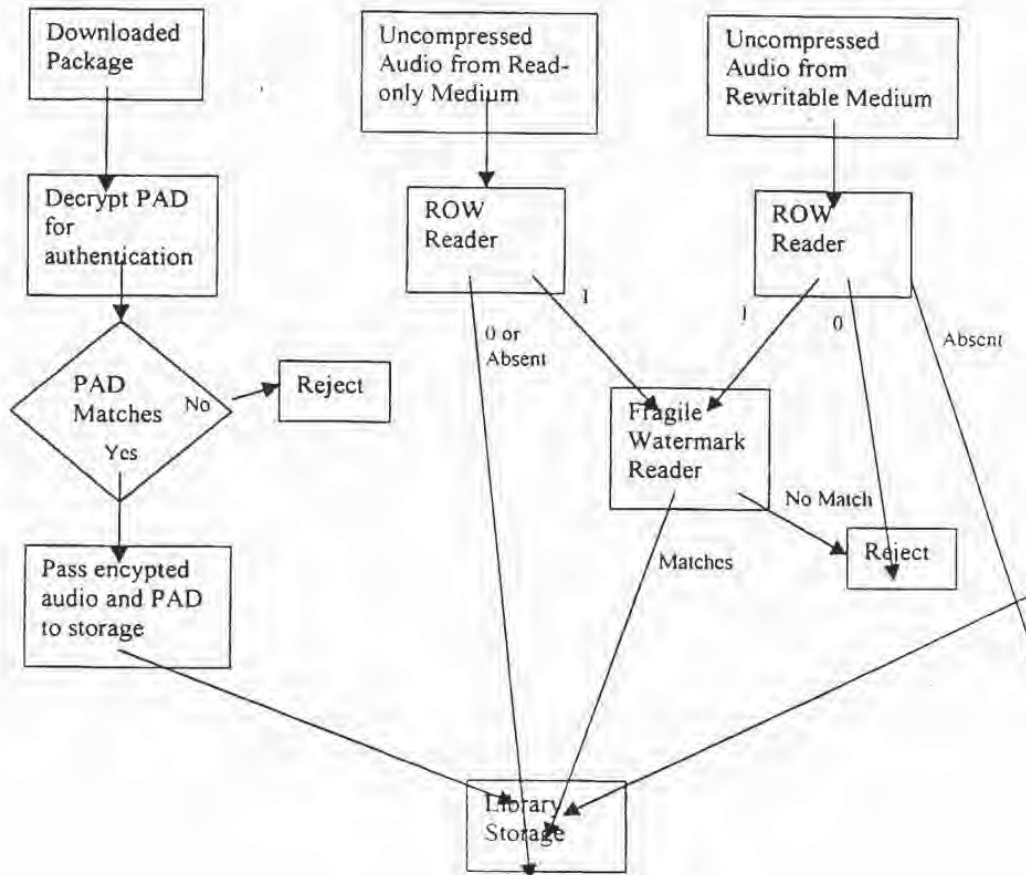
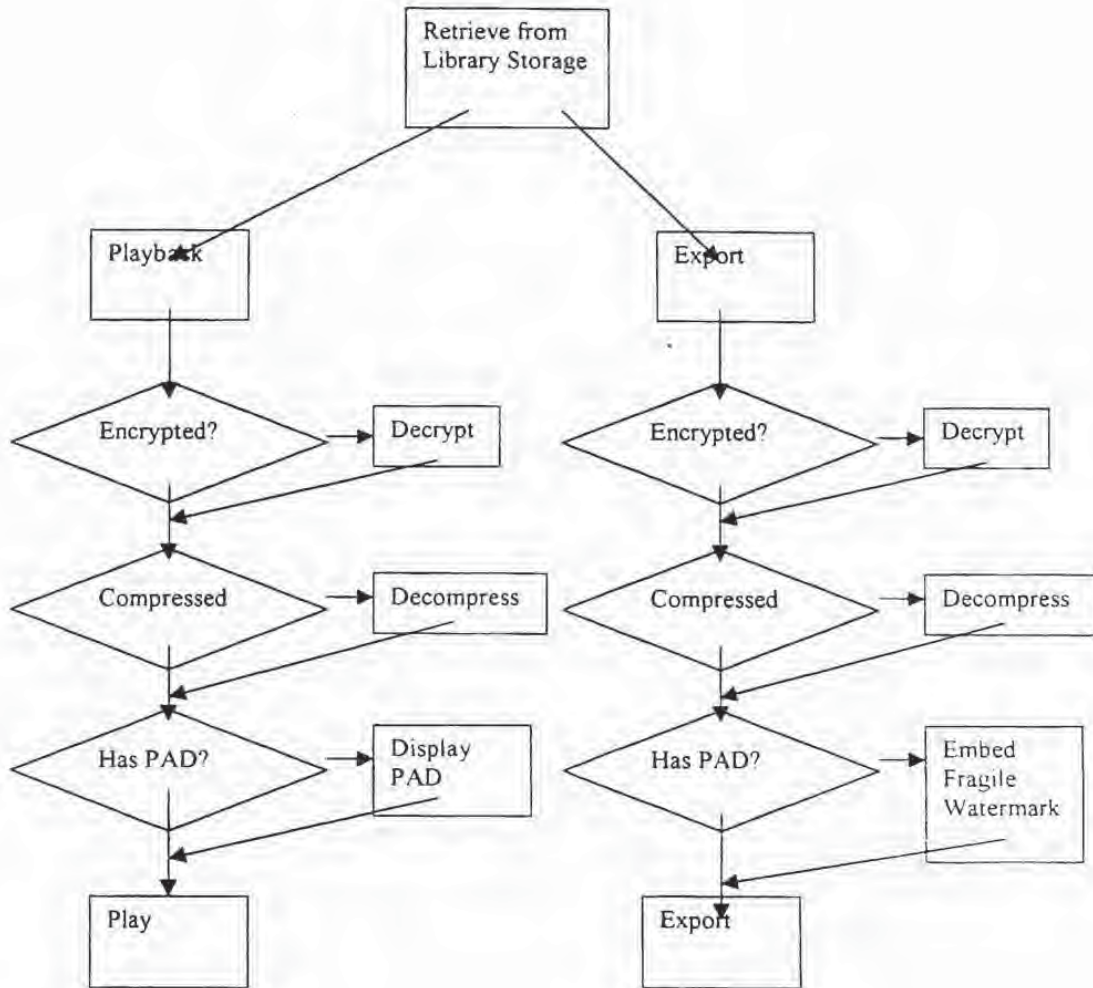


Table 3
SPCS Audio Player Output Stage



Claims:

1. A local content server system (LCS) for creating a secure environment for digital content, comprising:
- 5 a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission,
- 10 b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved,
- c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS, and
- d) a programmable address module which can be programmed with an
- 15 identification code uniquely associated with the LCS, and
- said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS.
2. The LCS of claim 1 further comprising
- 20 e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content;
- and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided
- 25 the LCS first determines that digital content being received is authorized for use by the LCS,
- and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU

-32-

3 A local content server system (LCS) for creating a secure environment for digital content, comprising

5 a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission,

10 b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content, and

c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved,

d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU

15 and

e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS,

said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS,

20 and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS

4 The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred

5 The system of claim 3, wherein said domain processor comprises

30 means for obtaining an identification code from an SU connected to the LCS's interface,

an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS,

means for analyzing digital content received from an SU,

said system permitting the digital content to be stored in the LCS if i) an
5 analysis of the digital content received from the SU concludes that the content is authenticated, or ii) an analysis of the digital content received from the SU concludes that the content cannot be authenticated because no authentication data is embedded in the content, and

said system preventing the digital content from being stored on the LCS if i)
10 an analysis of the digital content received from the SU concludes that the content is unauthenticated.

6. The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the
15 digital content has been previously marked with the unique identification code of the LCS.

7. The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot
20 be authenticated because there is no authentication data embedded in the content.

8. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.

9. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is
25 stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS,

means to retrieve a copy of the requested content data set;

30 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated,

-34-

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

5 10. The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11 The system of claim 10,

10 wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises

means to retrieve a copy of the requested content data set;

15 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

20 means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

wherein the LCS comprises

25 means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

30 means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

5 means to deliver the watermarked content data set to the SU for its use.

12. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

10 means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means receive a copy of the content data set;

15 means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated,

20 means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such the data contains no additional information to permit authentication.

25 14. The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated;

30 means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS, and

means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs

15 The system of claim 5, wherein the LCS further comprises

5 means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium

16 A system for creating a secure environment for digital content, comprising a Secure Electronic Content Distributor (SECD);

a Local Content Server (LCS);

10 a communications network interconnecting the SECD to the LCS, and

a Satellite Unit (SU) capable of interfacing with the LCS;

said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise securitizing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network to the LCS.

15 said LCS comprising: a domain processor; a first interface for connecting to a communications network; a second interface for communicating with the SU; a memory device for storing a plurality of data sets; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS, and

20 said SU being a portable module comprising: a memory for accepting secure digital content from a LCS; an interface for communicating with the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the SU.

17 A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

30 sending a message indicating that a user is requesting a copy of a content data set;

retrieving a copy of the requested content data set.

-37-

embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated,

embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user,

transmitting the watermarked content data set to the requesting consumer via an electronic network,

receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;

extracting at least one watermark from the transmitted watermarked content data set, and

permitting use of the content data set if the LCS determines that use is authorized.

18. The Method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user, and

permitting the storage of the content data set in a storage unit for the LCS

19. The Method of claim 17, further comprising:

connecting a Satellite Unit (SU) to an LCS,

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user, and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU,

delivering the content data set to the SU for its use.

20. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to an local content server (LCS),

- 5 sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;
 analyzing the message to confirm that the SU is authorized to use the LCS,
5 and
 retrieving a copy of the requested content data set;
 assessing whether a secured connection exists between the LCS and the SU;
 if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information
10 transmitted by the SU and information about the LCS, and
 delivering the content data set to the SU for its use.
21. The Method of claim 20, further comprising:
 embedding an open watermark into the content data to permit enhanced usage of the content data by the user.
- 15 22. The Method of claim 21, further comprising:
 embedding at least one additional watermark into the content data, said at least one additional watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis to provide information on the history of the content data's
20 use
23. The method of claim 20, wherein the content data can be stored at a level of quality which is selected by a user
24. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:
25 connecting a Satellite Unit (SU) to an local content server (LCS),
 sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;
 analyzing the message to confirm that the SU is authorized to use the LCS,
30 and
 retrieving a copy of the requested content data set;
 assessing whether a secured connection exists between the LCS and the SU,

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the watermarked content data set to the SU for its use.

5 25. The method of claim 24, further comprising:

embedding at least one robust open watermark into the copy of the requested content data set before the requested content data is delivered to the SU, said watermark indicating that the copy is authenticated.

10 26. The method of claim 25, wherein the robust watermark is embedded using any one of a plurality of embedding algorithms.

26. The method of claim 24, further comprising:

embedding a watermark which includes a hash value from a one-way hash function generated using the content data.

15 27. The method of claim 25, wherein the robust watermark can be periodically replaced with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.

28. The method of claim 24, further comprising the step of:

20 embedding additional robust open watermarks into the copy of the requested content data set before the requested content data is delivered to the SU, using a new algorithm; and

re-saving the newly watermarked copy to the LCS.

29. The method of claim 24, further comprising the step of:

25 saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

30 A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) to an local content server (LCS),

30 sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS,

and

receiving a copy of the content data set,

assessing whether the content data set is authenticated;

5 if the content data is unauthenticated, denying access to the LCS storage unit,

and

if the content data is not capable of authentication, accepting the data at a predetermined quality level, said predetermined quality level having been set for legacy content.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
15 March 2001 (15.03.2001)

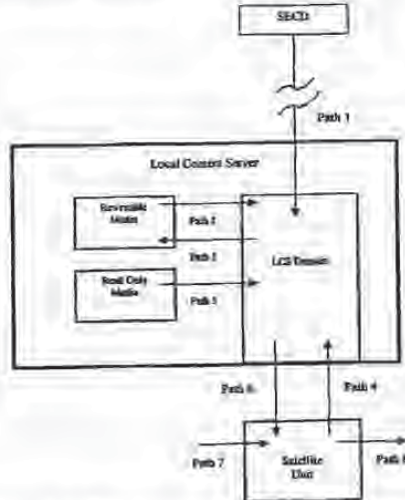
PCT

(10) International Publication Number
WO 01/18628 A2

- (51) International Patent Classification: G06F (72) Inventors; and
(75) Inventors/Applicants (for US only): MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).
- (21) International Application Number: PCT/US00/21189
- (22) International Filing Date: 4 August 2000 (04.08.2000)
- (25) Filing Language: English (74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, LLP; The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).
- (26) Publication Language: English (81) Designated States (national): JP, US.
- (30) Priority Data: 04 Apr 01
60/147,134 4 August 1999 (04.08.1999) US (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
60/213,489 23 June 2000 (23.06.2000) US
- (71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US). Published:
— Without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



(57) Abstract: A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS, and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected

[Continued on next page]

WO 01/18628 A2

WO 01/18628 A2



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

to the system through the interface, which SUs are capable of receiving and transmitting digital content; at least one SU; and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit. A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.

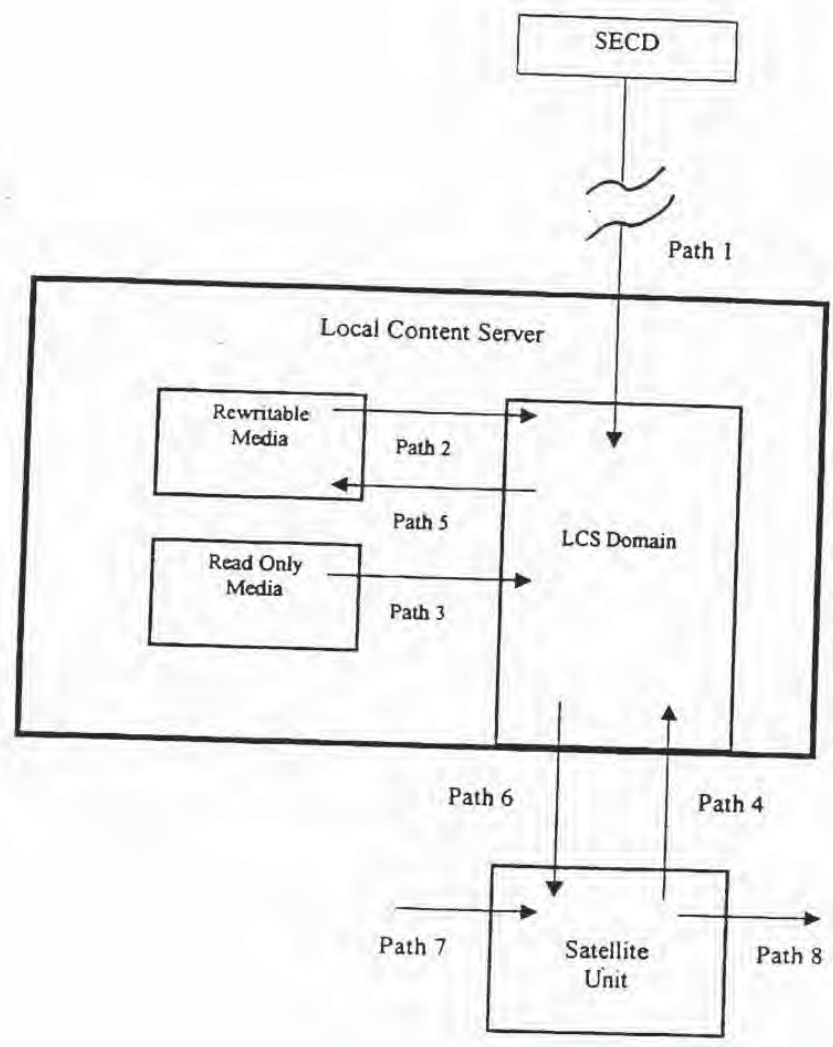


FIG. 1

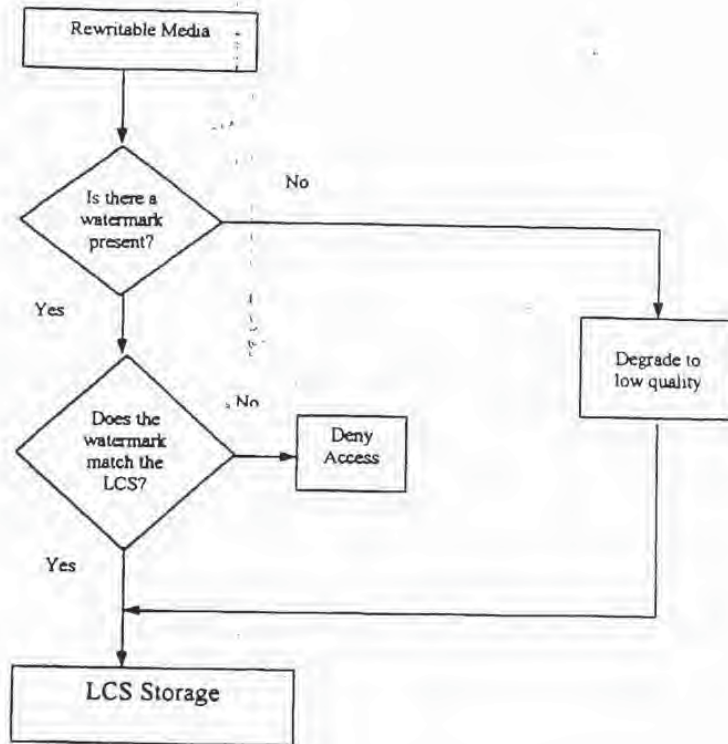


FIG. 2

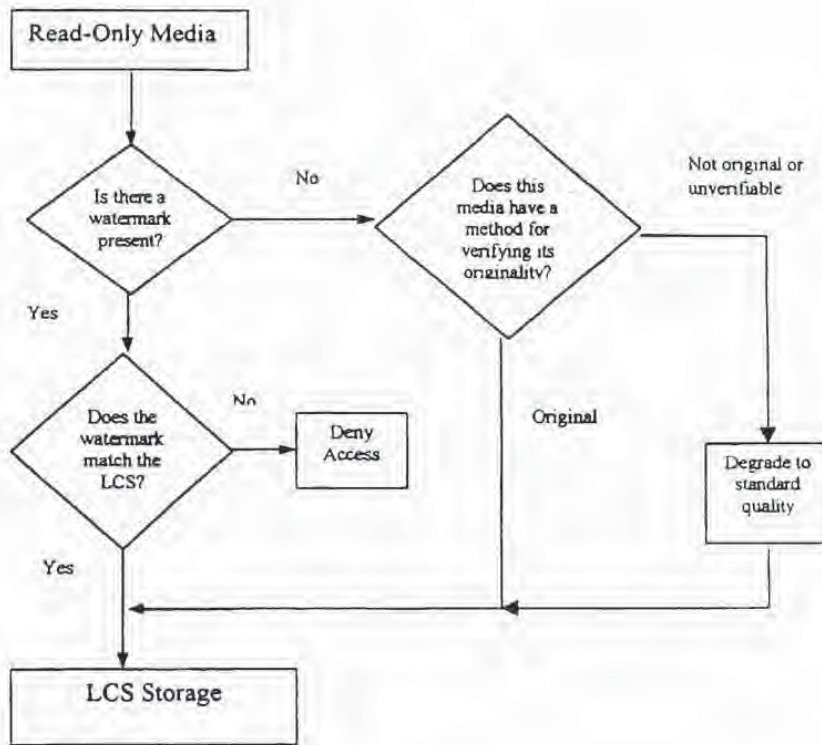


FIG. 3

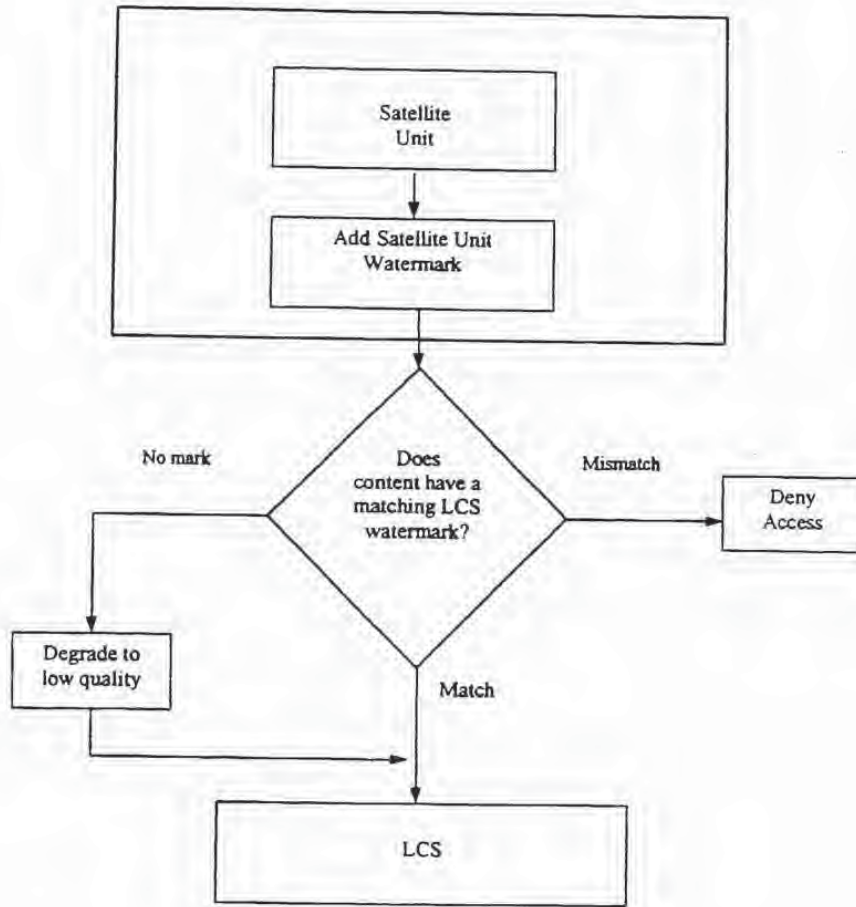


FIG. 4

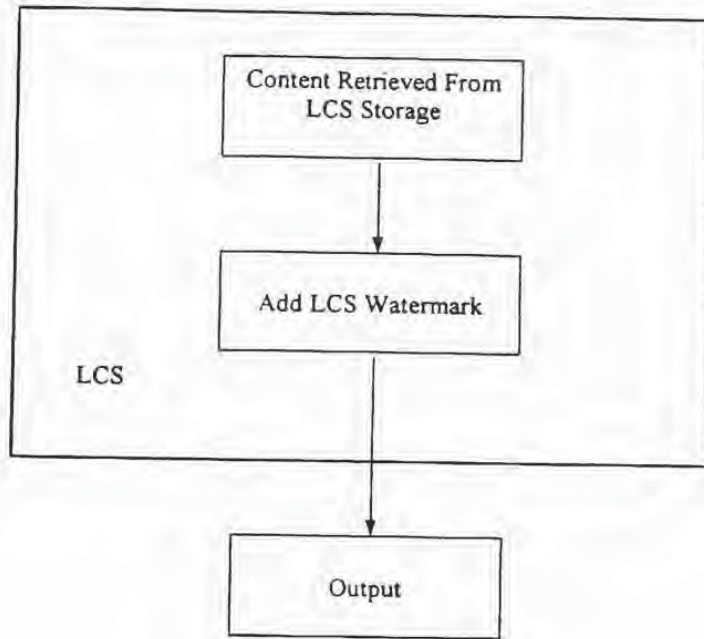


FIG. 5

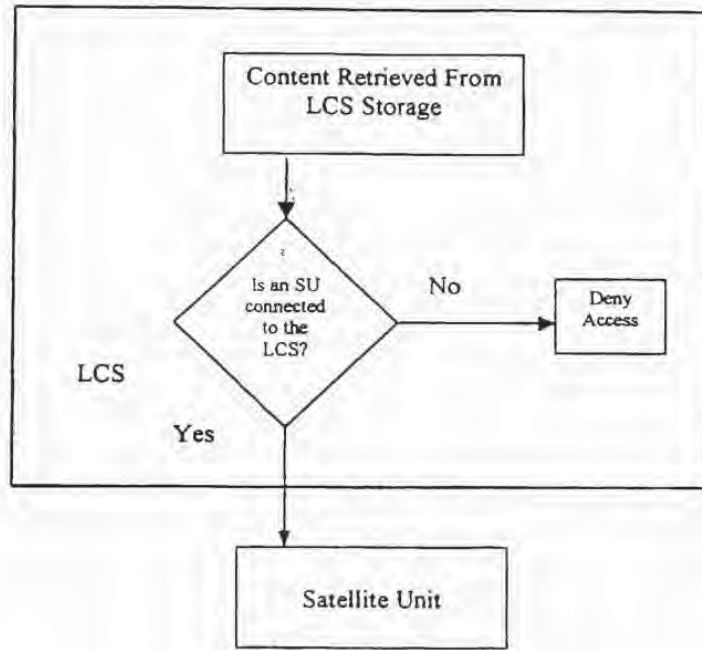


FIG. 6

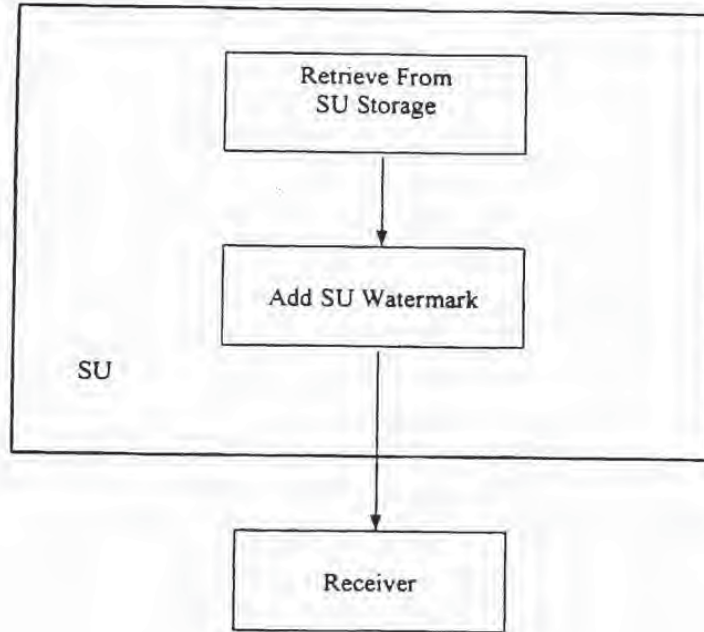


FIG. 7

Signature _____ Date _____

Full Name of First Inventor: MOSKOWITZ Scott A.
(Family Name) (First Given Name) (Second Given Name)

1-0

Citizenship: U.S.A.

Residence: Miami, Florida 33160

FL

Post Office Address: 16711 Collins Avenue, No. 2505, Miami, FL 33160, USA

Signature _____ Date 6/29/02

Full Name of Second Inventor: BERRY MICHAEL
(Family Name) (First Given Name) (Second Given Name)

20

Citizenship: U.S.A.

Residence: Albuquerque, New Mexico 87112

NM

Post Office Address: 12401 Princess Jeanne, Albuquerque, New Mexico 87112, USA

WRFMAIN 1142437.1



Prior Provisional Application(s)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

| Application Number | Date of Filing (day, month, year) |
|--------------------|-----------------------------------|
| 60/147,134 | 04/08/1999 |
| 60/213,489 | 23/06/2000 |

Prior United States Application(s)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| Application Number | Date of Filing (day, month, year) | Status - Patented, Pending, Abandoned |
|--------------------|-----------------------------------|---------------------------------------|
| | | |
| | | |

All correspondence and telephone communications should be addressed to:

Floyd B. Chapman, Esq.
 Wiley Rein & Fielding LLP
 Intellectual Property Department
 1776 K Street, N.W.
 Washington, D.C. 20006
 Telephone Number: 202.719.7000
 Facsimile Number: 202.719.7049

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and imprisonment, or both, under 18 U.S.C. § 1001, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

DECLARATION FOR PATENT APPLICATION

As one of the below named inventors, WE hereby declare that:

My residence, post office address and citizenship is as stated below next to my name:

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A SECURE PERSONAL CONTENT SERVER

the specification of which: is attached hereto.
 was filed on: February 4, 2002
as Application No.: 10/049,101
and was amended on: _____

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56.

And I hereby authorize and request my agents, Wiley Rein & Fielding LLP, whose address is set forth below, to insert above, the filing date and application number of said application when known.

Prior Foreign Application(s)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

| Country | Application Number | Date of Filing (day, month, year) | Date of Issue (day, month, year) | Priority Claimed | |
|---------|--------------------|-----------------------------------|----------------------------------|---|-----------------------------|
| PCT | PCT/US00/21189 | 04/08/2000 | | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> |
| | | | | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

WILEY REIN & FIELDING LLP
1776 K STREET, N.W.
WASHINGTON, D.C. 20006
202.719.3000 (TELEPHONE) 202.719.7049 (FACSIMILE)



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Scott A. Moskowitz et al.

Appl. No.: 10/049,101

Filed: February 4, 2002

For: A SECURE PERSONAL
CONTENT SERVER

Art Unit: Unassigned

Examiner: Unassigned

**POWER OF ATTORNEY FROM ASSIGNEE UNDER § 3.71
and CERTIFICATION UNDER § 3.73**

Commissioner of Patent
Washington, D.C. 20231

Sir:

The undersigned ASSIGNEE having the entire right, title and interest in the above-identified application for letters patent hereby appoints:

Floyd B. Chapman, Registration No. 40,555; David J. Kulik, Registration No. 36,576; Gregory R. Lyons, Registration No. 37,666; James H. Wallace, Jr., Registration No. 25,541; James T. Bruce, III, Registration No. 31,491; Christopher Mills, Registration No. 46,934; Mark Pacella, Registration No. 46,974; Kevin Anderson, Registration No. 43,471; and Christopher Hale, Registration No. 48,940, of the firm

Wiley Rein & Fielding LLP 1776 K Street, N.W. Washington, D.C., 20006,
associated with **Customer Number 29693**,

to prosecute this application, and any continuations or divisionals, reissues and reexaminations thereof, and all foreign and international applications corresponding thereto, and to transact all business in the United States Patent and Trademark Office in connection therewith and hereby revokes all prior powers of attorney; said appointment to be the exclusion of the inventors and the inventors' attorneys.

PATENT

Serial No. 10/049,101

Attorney Docket No.: 80408.0011

All correspondence and telephone communications should be addressed to:

Floyd B. Chapman, Esq.
Wiley Rein & Fielding LLP
Intellectual Property Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone Number: 202.719.7000
Facsimile Number: 202.719.7049

CERTIFICATE UNDER 37 C.F.R. § 3.73(b)

The following evidentiary documents establish a chain of title from the original owner(s) or inventor(s) to the ASSIGNEE as required under 37 C.F.R. § 3.73(b):

 X a copy of an Assignment(s) is attached hereto, which Assignment(s) has been (or is herewith) forwarded to the Patent and Trademark Office for recording; or
 the Assignment has been recorded on _____ at reel _____, frame(s) _____.

Pursuant to 37 C.F.R. § 3.73(b), the undersigned ASSIGNEE hereby states that the evidentiary documents have been reviewed and hereby certifies that, to the best of ASSIGNEE's knowledge and belief, title is in the identified ASSIGNEE.

Date: 7/19/02

BLUE SPIKE, INC.

By: [Signature]
[SIGNATURE]

Name: Scott Moskowitz
(TYPED)

Title: CEO

WRFM/AIN 1142767.1



DECLARATION FOR PATENT APPLICATION

As one of the below named inventors, WE hereby declare that:

My residence, post office address and citizenship is as stated below next to my name:

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A SECURE PERSONAL CONTENT SERVER

the specification of which: is attached hereto.
 was filed on: February 4, 2002
 as Application No.: 10/049,101
 and was amended on: _____

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56.

And I hereby authorize and request my agents, Wiley Rein & Fielding LLP, whose address is set forth below, to insert above, the filing date and application number of said application when known.

Prior Foreign Application(s)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

| Country | Application Number | Date of Filing (day, month, year) | Date of Issue (day, month, year) | Priority Claimed | |
|---------|--------------------|--------------------------------------|-------------------------------------|---|-----------------------------|
| PCT | PCT/US00/21189 | 04/08/2000 | | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> |
| | | | | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

WILEY REIN & FIELDING LLP
 1776 K STREET, N.W.
 WASHINGTON, D.C. 20006
 202.719.7000 (TELEPHONE) 202.719.7049 (FACSIMILE)

PAGE 1 of 3

Prior Provisional Application(s)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

| Application Number | Date of Filing (day, month, year) |
|--------------------|-----------------------------------|
| 60/147,134 | 04/08/1999 |
| 60/213,489 | 23/06/2000 |

Prior United States Application(s)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| Application Number | Date of Filing (day, month, year) | Status - Patented, Pending, Abandoned |
|--------------------|-----------------------------------|---------------------------------------|
| | | |
| | | |

All correspondence and telephone communications should be addressed to:

Floyd B. Chapman, Esq.
Wiley Rein & Fielding LLP
Intellectual Property Department
1776 K Street, N.W.
Washington, D.C. 20006

Telephone Number: 202.719.7000
 Facsimile Number: 202.719.7049

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and imprisonment, or both, under 18 U.S.C. § 1001, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.



Signature Scott A. Moskowitz Date 7/19/02
 Full Name of First Inventor: MOSKOWITZ Scott A.
 (Family Name) (First Given Name) (Second Given Name)
 Citizenship: U.S.A.
 Residence: Miami, Florida 33160 FL
 Post Office Address: 16711 Collins Avenue, No. 2505, Miami, FL 33160, USA

Signature _____ Date _____
 Full Name of Second Inventor: BERRY MICHAEL
 (Family Name) (First Given Name) (Second Given Name)
 Citizenship: U.S.A.
 Residence: Albuquerque, New Mexico 87112
 Post Office Address: 12401 Princess Jeanne, Albuquerque, New Mexico 87112, USA

WRFMAIN 1142437.1

10/00101

PTO/SB/11/03
 #7
 Mar 03

Under the Paperwork Reduction Act of 1995, no answers are required in response to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2002

Federal fees are subject to annual revision.

Complete if Known

| | |
|----------------------|--------------------------|
| Application Number | 10/049,101 |
| Filing Date | 02/04/2002 |
| First Named Inventor | Scott A. Moskowitz et al |
| Examiner Name | Unassigned |
| Group Art Unit | N/A |
| Attorney Docket No. | 80408.0011 US |

TOTAL AMOUNT OF PAYMENT (\$) 65.00

| METHOD OF PAYMENT | | FEE CALCULATION (continued) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|----------------------------|--|--|----------------------------|----------------------------|--------------------|-----------------|----------|-----|----------------------------|--------|-------------------------------------|-------|----------------------------|----------------------------|-----------------|--|--------------------------|-----|------------------------------|-----|----------------------------|----|--|-------|-------------------------------|---|---|-----|-----|-----|--|--|-----|-------|--|---|--|-----|-----|-----|---|--|-----|-----|-----|---|--|-----|-----|-----|--|--|-----|-------|-----|---|--|-----|-------|-----|--|--|-----|-----|-----|----------------------|--|-----|-----|-----|--|--|-----|-----|-----|------------------------------|--|-----|-------|-----|---|--|-----|-----|-----|-------------------------------------|--|-----|-------|-----|--|--|-----|-------|-----|------------------------------------|--|-----|-----|-----|----------------------|--|-----|-----|-----|---------------------|--|-----|-----|-----|--------------------------------|--|-----|----|-----|---|--|-----|-----|-----|--|--|-----|----|-----|--|--|-----|-----|-----|---|--|-----|-----|-----|--|--|-----|-----|-----|---|--|-----|-----|-----|---|--|
| 1. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to: Deposit Account Number: 50-1129 Deposit Account Name: Wiley Rein & Fielding, LLP <input type="checkbox"/> Charge Any Additional Fee Reserved Under 37 CFR 1.16 and 1.17 <input checked="" type="checkbox"/> Applicant claims small entity status See 37 CFR 1.212 | | 3. ADDITIONAL FEES <table border="1"> <thead> <tr> <th>Fee Code (\$)</th> <th>Large Entity (\$)</th> <th>Small Entity (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>105</td><td>130</td><td>85</td><td>Surcharge - late filing fee or oath</td><td>65.00</td></tr> <tr><td>127</td><td>50</td><td>25</td><td>Surcharge - late provisional filing fee or cover sheet</td><td></td></tr> <tr><td>138</td><td>130</td><td>130</td><td>Non-English specification</td><td></td></tr> <tr><td>147</td><td>2,520</td><td>147</td><td>2,520 For filing a request for ex parte reexamination</td><td></td></tr> <tr><td>112</td><td>620</td><td>112</td><td>620 Requesting publication of SAR prior to Examiner action</td><td></td></tr> <tr><td>113</td><td>1,640</td><td>113</td><td>1,640 Requesting publication of RFR after Examiner action</td><td></td></tr> <tr><td>115</td><td>110</td><td>215</td><td>55 Extension for reply within first month</td><td></td></tr> <tr><td>116</td><td>400</td><td>215</td><td>300 Extension for reply within second month</td><td></td></tr> <tr><td>117</td><td>920</td><td>217</td><td>400 Extension for reply within third month</td><td></td></tr> <tr><td>118</td><td>1,440</td><td>218</td><td>720 Extension for reply within fourth month</td><td></td></tr> <tr><td>125</td><td>1,980</td><td>228</td><td>800 Extension for reply within fifth month</td><td></td></tr> <tr><td>119</td><td>320</td><td>219</td><td>100 Notice of Appeal</td><td></td></tr> <tr><td>120</td><td>320</td><td>220</td><td>100 Filing a brief in support of an appeal</td><td></td></tr> <tr><td>121</td><td>280</td><td>221</td><td>140 Request for oral hearing</td><td></td></tr> <tr><td>139</td><td>1,510</td><td>139</td><td>1,510 Petition to institute a public use proceeding</td><td></td></tr> <tr><td>140</td><td>110</td><td>240</td><td>55 Petition to revive - unavoidable</td><td></td></tr> <tr><td>141</td><td>1,380</td><td>241</td><td>640 Petition to revive - unintentional</td><td></td></tr> <tr><td>142</td><td>1,380</td><td>242</td><td>640 Utility issue fee (or revival)</td><td></td></tr> <tr><td>143</td><td>400</td><td>243</td><td>250 Design issue fee</td><td></td></tr> <tr><td>144</td><td>520</td><td>244</td><td>310 Plant issue fee</td><td></td></tr> <tr><td>192</td><td>130</td><td>130</td><td>130 Refund to the Commissioner</td><td></td></tr> <tr><td>123</td><td>50</td><td>123</td><td>50 Processing fee under 37 CFR 1.137(d)</td><td></td></tr> <tr><td>136</td><td>180</td><td>136</td><td>180 Submission of Information Disclosure Sheet</td><td></td></tr> <tr><td>081</td><td>40</td><td>581</td><td>50 Recording each claim assignment per priority (three number of priorities)</td><td></td></tr> <tr><td>146</td><td>740</td><td>246</td><td>370 Filing a submission after final rejection (37 CFR § 1.122(e))</td><td></td></tr> <tr><td>148</td><td>740</td><td>248</td><td>370 For each additional invention to be examined (37 CFR § 1.120(b))</td><td></td></tr> <tr><td>179</td><td>740</td><td>279</td><td>370 Request for Continued Examination (RCE)</td><td></td></tr> <tr><td>169</td><td>800</td><td>169</td><td>900 Request for expedited examination of a design application</td><td></td></tr> </tbody> </table> | | Fee Code (\$) | Large Entity (\$) | Small Entity (\$) | Fee Description | Fee Paid | 105 | 130 | 85 | Surcharge - late filing fee or oath | 65.00 | 127 | 50 | 25 | Surcharge - late provisional filing fee or cover sheet | | 138 | 130 | 130 | Non-English specification | | 147 | 2,520 | 147 | 2,520 For filing a request for ex parte reexamination | | 112 | 620 | 112 | 620 Requesting publication of SAR prior to Examiner action | | 113 | 1,640 | 113 | 1,640 Requesting publication of RFR after Examiner action | | 115 | 110 | 215 | 55 Extension for reply within first month | | 116 | 400 | 215 | 300 Extension for reply within second month | | 117 | 920 | 217 | 400 Extension for reply within third month | | 118 | 1,440 | 218 | 720 Extension for reply within fourth month | | 125 | 1,980 | 228 | 800 Extension for reply within fifth month | | 119 | 320 | 219 | 100 Notice of Appeal | | 120 | 320 | 220 | 100 Filing a brief in support of an appeal | | 121 | 280 | 221 | 140 Request for oral hearing | | 139 | 1,510 | 139 | 1,510 Petition to institute a public use proceeding | | 140 | 110 | 240 | 55 Petition to revive - unavoidable | | 141 | 1,380 | 241 | 640 Petition to revive - unintentional | | 142 | 1,380 | 242 | 640 Utility issue fee (or revival) | | 143 | 400 | 243 | 250 Design issue fee | | 144 | 520 | 244 | 310 Plant issue fee | | 192 | 130 | 130 | 130 Refund to the Commissioner | | 123 | 50 | 123 | 50 Processing fee under 37 CFR 1.137(d) | | 136 | 180 | 136 | 180 Submission of Information Disclosure Sheet | | 081 | 40 | 581 | 50 Recording each claim assignment per priority (three number of priorities) | | 146 | 740 | 246 | 370 Filing a submission after final rejection (37 CFR § 1.122(e)) | | 148 | 740 | 248 | 370 For each additional invention to be examined (37 CFR § 1.120(b)) | | 179 | 740 | 279 | 370 Request for Continued Examination (RCE) | | 169 | 800 | 169 | 900 Request for expedited examination of a design application | |
| Fee Code (\$) | Large Entity (\$) | Small Entity (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 105 | 130 | 85 | Surcharge - late filing fee or oath | 65.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 127 | 50 | 25 | Surcharge - late provisional filing fee or cover sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 138 | 130 | 130 | Non-English specification | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 147 | 2,520 | 147 | 2,520 For filing a request for ex parte reexamination | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 112 | 620 | 112 | 620 Requesting publication of SAR prior to Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 113 | 1,640 | 113 | 1,640 Requesting publication of RFR after Examiner action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 115 | 110 | 215 | 55 Extension for reply within first month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 116 | 400 | 215 | 300 Extension for reply within second month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 117 | 920 | 217 | 400 Extension for reply within third month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 118 | 1,440 | 218 | 720 Extension for reply within fourth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 125 | 1,980 | 228 | 800 Extension for reply within fifth month | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 119 | 320 | 219 | 100 Notice of Appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 120 | 320 | 220 | 100 Filing a brief in support of an appeal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 121 | 280 | 221 | 140 Request for oral hearing | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 139 | 1,510 | 139 | 1,510 Petition to institute a public use proceeding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 140 | 110 | 240 | 55 Petition to revive - unavoidable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 141 | 1,380 | 241 | 640 Petition to revive - unintentional | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 142 | 1,380 | 242 | 640 Utility issue fee (or revival) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 143 | 400 | 243 | 250 Design issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 144 | 520 | 244 | 310 Plant issue fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 192 | 130 | 130 | 130 Refund to the Commissioner | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 123 | 50 | 123 | 50 Processing fee under 37 CFR 1.137(d) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 136 | 180 | 136 | 180 Submission of Information Disclosure Sheet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 081 | 40 | 581 | 50 Recording each claim assignment per priority (three number of priorities) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 146 | 740 | 246 | 370 Filing a submission after final rejection (37 CFR § 1.122(e)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 148 | 740 | 248 | 370 For each additional invention to be examined (37 CFR § 1.120(b)) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 179 | 740 | 279 | 370 Request for Continued Examination (RCE) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169 | 800 | 169 | 900 Request for expedited examination of a design application | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. <input type="checkbox"/> Payment Enclosed: <input type="checkbox"/> Check <input type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other | | FEE CALCULATION 1. BASIC FILING FEE <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>101</td><td>740</td><td>301 370 Utility filing fee</td><td></td></tr> <tr><td>106</td><td>830</td><td>306 165 Design filing fee</td><td></td></tr> <tr><td>103</td><td>510</td><td>303 225 Plant filing fee</td><td></td></tr> <tr><td>108</td><td>740</td><td>208 370 Reissue filing fee</td><td></td></tr> <tr><td>114</td><td>150</td><td>214 50 Provisional filing fee</td><td></td></tr> </tbody> </table> SUBTOTAL (1) (\$) 0.00 | | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 101 | 740 | 301 370 Utility filing fee | | 106 | 830 | 306 165 Design filing fee | | 103 | 510 | 303 225 Plant filing fee | | 108 | 740 | 208 370 Reissue filing fee | | 114 | 150 | 214 50 Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 101 | 740 | 301 370 Utility filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 106 | 830 | 306 165 Design filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 | 510 | 303 225 Plant filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 108 | 740 | 208 370 Reissue filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 114 | 150 | 214 50 Provisional filing fee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. EXTRA CLAIM FEES <table border="1"> <thead> <tr> <th>Total Claims</th> <th>Extra Claims</th> <th>Fee from below</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr> <td>Independent Claims</td> <td>-30** =</td> <td>X</td> <td></td> </tr> <tr> <td>Multiple Dependent</td> <td>-3** =</td> <td>X</td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Large Entity Fee Code (\$)</th> <th>Small Entity Fee Code (\$)</th> <th>Fee Description</th> <th>Fee Paid</th> </tr> </thead> <tbody> <tr><td>103</td><td>18</td><td>203 9 Claims in excess of 20</td><td></td></tr> <tr><td>100</td><td>74</td><td>200 42 Independent claims in excess of 3</td><td></td></tr> <tr><td>104</td><td>260</td><td>204 140 Multiple dependent claim, if not paid</td><td></td></tr> <tr><td>109</td><td>84</td><td>209 42 ** Release independent claims over original patent</td><td></td></tr> <tr><td>110</td><td>18</td><td>210 9 ** Release claims in excess of 20 and over original patent</td><td></td></tr> </tbody> </table> SUBTOTAL (2) (\$) 0.00 | | Total Claims | Extra Claims | Fee from below | Fee Paid | Independent Claims | -30** = | X | | Multiple Dependent | -3** = | X | | Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | 103 | 18 | 203 9 Claims in excess of 20 | | 100 | 74 | 200 42 Independent claims in excess of 3 | | 104 | 260 | 204 140 Multiple dependent claim, if not paid | | 109 | 84 | 209 42 ** Release independent claims over original patent | | 110 | 18 | 210 9 ** Release claims in excess of 20 and over original patent | | Other fee (specify) _____ **For number previously paid, if greater. For Reissues, see above *Reduced by Basic Filing Fee Paid SUBTOTAL (3) (\$) 65.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total Claims | Extra Claims | Fee from below | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Independent Claims | -30** = | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Multiple Dependent | -3** = | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Large Entity Fee Code (\$) | Small Entity Fee Code (\$) | Fee Description | Fee Paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 103 | 18 | 203 9 Claims in excess of 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 100 | 74 | 200 42 Independent claims in excess of 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 104 | 260 | 204 140 Multiple dependent claim, if not paid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 109 | 84 | 209 42 ** Release independent claims over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 110 | 18 | 210 9 ** Release claims in excess of 20 and over original patent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|-------------------|-------------------------|---------------------------------|--------------|
| SUBMITTED BY: | | Complete if applicable | |
| Name (Print/Type) | Floyd B. Chapman | Registration No. (Assign/Agent) | 40,565 |
| Signature | <i>Floyd B. Chapman</i> | Telephone | 202-719-7000 |
| | | Date | 07/23/2002 |

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burdorff Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



Commissioner for Patents
Washington, DC 20231
www.uspto.gov



CONFIRMATION NO. 8028

Bib Data Sheet

| | | | | | |
|---|---|-------------------------------|---|--|--------------------------------|
| SERIAL NUMBER 10/049,101 | FILING DATE 07/23/2002 RULE | CLASS 713 | GROUP ART UNIT 2182 | ATTORNEY DOCKET NO. 80408.0011 | |
| APPLICANTS Scott A. Moskowitz, Miami, FL; * CONTINUING DATA ***** This application is a 371 of PCT/US00/21189 08/04/2000 which claims benefit of 60/147,134 08/04/1999 and claims benefit of 60/213,489 06/23/2000 ** FOREIGN APPLICATIONS ***** ** SMALL ENTITY ** | | | | | |
| Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no 35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after Allowance | | STATE OR COUNTRY FL | SHEETS DRAWING 7 | TOTAL CLAIMS 30 | INDEPENDENT CLAIMS 7 |
| Verified and Acknowledged _____ Examiner's Signature _____ Initials _____ | | | | | |
| ADDRESS Wiley Rein & Fielding Intellectual Property Department 1776 K Street NW Washington, DC 20006 | | | | | |
| TITLE Secure personal content server | | | | | |
| FILING FEE RECEIVED 702 | FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following: | | <input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit | | |



10/049101

DTB Rec'd PCT/PTO 23 JUL 2002 #7
PATENT
Atty Docket No.: 80408.001
JF Mar 03

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE

Application of:

Scott A. MOSKOWITZ et al.
Application No: 10/049,101
Filing Date: 02/04/2002
I.A. Filing Date: 08/04/2000
For: A SECURE PERSONAL CONTENT
SERVER

Art Unit: Unassigned
Examiner: Unassigned

Box PCT (Missing Parts)
Commissioner for Patents
Washington DC 20231

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS
UNDER 35 U.S.C. 371 IN THE UNITED STATES (DO/EO/US)

In response to the Notification of Missing Requirements Under 35 U.S.C. § 371 In the United States Designated/Elected Office (DO/EO/US) mailed May 23, 2002, Applicants submit the documents and fees indicated below. All required documents and fees are now being submitted. Applicants respectfully request examination of the application.

Applicants hereby submit the following:

- Copy of Notice of Missing Parts;
- Two Original Executed Declarations (Total 6 pages);
- Authorization to charge Deposit Account for surcharge under 37 C.F.R. § 1.16(e) for the late filing of the executed Declaration \$65.00;
- Original Executed Power of Attorney By Assignee (2 pages) with copies of Assignment documents not for recordation.

USPTO 02 07 02 00000120 501129 10749101
85.00 01

Applicants hereby authorize the Commissioner of Patents to charge Deposit Account No. 50-1129 for the \$65.00 surcharge for the late filing of Declaration. Applicants believe no



additional extension of time fees, requests for extension of time, petitions, extra claim fees, or additional fees are necessary to enter and consider this paper or any accompanying paper. If, however, any petitions, requests for extensions of time, or any fees are required in order to enter or consider this paper, or to keep this application pending, Applicants hereby authorize the Commissioner to charge our Deposit Account No. 50-1129.

Respectfully submitted,
Wiley Rein & Fielding LLP

Date: July 23, 2002

By:


Floyd B. Chapman, Reg. No. 40,555

Wiley Rein & Fielding LLP
Patent Administration
1776 K Street N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049

WRFMAIN 1151702.1

17 MAR 2003



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

WILEY REIN & FIELDING, LLP
1776 k Street, N.W.
Washington, D.C. 20006

In re Application of
MOSKOWITZ et al
Application No.: 10/049,101
PCT No.: PCT/US00/21189
Int. Filing Date: 04 August 2000
Priority Date: 04 August 1999
Attorney's Docket No.: 80408.0011
For: A SECURE PERSONAL CONTENT
SERVER

COMMUNICATION

This is in response to the "REQUEST TO "CORRECT" THE RECORD IN CONNECTION WITH THE DECISION ON PETITION UNDER 37 CFR 1.137(B)" filed on 24 June 2002.

BACKGROUND

In a decision from this Office on 16 May 2002, the petition under 37 CFR 1.137(b) filed for revival of U.S. application 10/049,101 abandoned unintentionally was granted. The decision indicated, inter alia, that no Demand electing the United States was filed in this international application and that an executed declaration was filed.

On 24 June 2002, applicants filed the instant correction in connection with the decision on petition under 37 CFR 1.137(b). The applicants indicate that a Demand was filed for international application PCT/US00/21189 on March 2, 2001 and no executed Declaration was filed at that time.

DISCUSSION

A review of PCT/US00/21189 indicates that there is no record of a Demand being filed for this application. Applicants may want to file a petition for PCT/US00/21189 under 37 CFR 1.181 to correct the record. Accordingly, the statement in the decision that no demand was filed is correct.

In addition, applicants statement that no executed declaration was filed at that time is correct. The phrase "an executed declaration" was inadvertently added in the decision. However, because no declaration was filed a 35 U.S.C. 371 date was not given to the application at that time.

Application No. 10/049,101

-2-

This application is being returned to the United States Designated/Elected Office (DO/EO/US) for continued processing.



Rafael Bacares
PCT Legal Examiner
PCT Legal Office

Tel: (703) 308-6312

Fax: (703) 308-6459



Leonard Smith
PCT Legal Examiner
PCT Legal Office



UNITED STATES PATENT AND TRADEMARK OFFICE

 Commissioner for Patents, Box PCT
 United States Patent and Trademark Office
 Washington, D.C. 20231
 www.uspto.gov

| | | |
|-----------------------------|-----------------------|------------------|
| U.S. APPLICATION NUMBER NO. | FIRST NAMED APPLICANT | ATTY. DOCKET NO. |
| 10/049,101 | Scott A. Moskowitz | 80408,0011 |

| |
|-------------------------------|
| INTERNATIONAL APPLICATION NO. |
| PCT/US00/21189 |

| | |
|------------------|---------------|
| I.A. FILING DATE | PRIORITY DATE |
| 08/04/2000 | 08/04/1999 |

Wiley Rein & Fielding
 Intellectual Property Department
 1776 K Street NW
 Washington, DC 20006

CONFIRMATION NO. 8028

371 ACCEPTANCE LETTER



OC000000009682230

Date Mailed: 03/24/2003

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

| | |
|---|--|
| <u>07/23/2002</u> | <u>07/23/2002</u> |
| DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS | DATE OF RECEIPT OF ALL 35 U.S.C. 371 REQUIREMENTS |

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE, THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

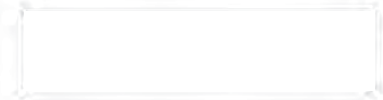
- Indication of Small Entity Status
- Copy of the International Application filed on 02/08/2002
- Copy of the International Search Report filed on 02/08/2002
- Oath or Declaration filed on 07/23/2002
- Small Entity Statement filed on 02/08/2002
- Request for Immediate Examination filed on 02/08/2002
- U.S. Basic National Fees filed on 02/08/2002

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

CHARITTA A BURT
Telephone: (703) 305-3734

PART 3 - OFFICE COPY

FORM PCT/DO/EO/903 (371 Acceptance Notice)



EAST Search History

| Ref # | Hits | Search Query | DBs | Default Operator | Plurals | Time Stamp |
|-------|---------|---|-----------------|------------------|---------|------------------|
| L1 | 32 | watermark same message adj digest | US-PGPUB; USPAT | OR | OFF | 2006/03/22 16:53 |
| L2 | 58 | third adj watermark | US-PGPUB; USPAT | OR | OFF | 2006/03/22 16:53 |
| L3 | 3 | I2 with fragile | US-PGPUB; USPAT | OR | OFF | 2006/03/22 16:53 |
| S1 | 1 | "secure electronic content distributor" | US-PGPUB; USPAT | OR | OFF | 2006/03/15 14:57 |
| S2 | 0 | "secure content distributor" | US-PGPUB; USPAT | OR | OFF | 2006/03/15 14:57 |
| S3 | 2032275 | content (media adj file\$1) movie song audio video data | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:08 |
| S4 | 1211819 | distributor distribution distribute delivery server | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:17 |
| S5 | 743145 | S3 and S4 | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:18 |
| S6 | 41193 | S3 adj S4 | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:20 |
| S7 | 238 | S6 same watermark | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:23 |
| S8 | 32 | S6 same (digital adj watermark) | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:21 |
| S9 | 206 | S7 not S8 | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:53 |
| S10 | 0 | "08154866".ap. | US-PGPUB; USPAT | OR | OFF | 2006/03/15 15:53 |
| S11 | 7 | "154866".ap. | US-PGPUB; USPAT | OR | OFF | 2006/03/15 17:07 |
| S12 | 6 | "049101".ap. | US-PGPUB; USPAT | OR | OFF | 2006/03/15 17:07 |
| S13 | 17 | (US-20050044481-\$ or US-20050018874-\$ or US-20040255236-\$ or US-20040128514-\$ or US-20030231785-\$ or US-20040037449-\$ or US-20030133702-\$ or US-20030174861-\$).did. or (US-6996722-\$ or US-6965682-\$ or US-6889211-\$ or US-6668246-\$ or US-6665489-\$ or US-6823455-\$ or US-6405203-\$ or US-6522769-\$ or US-6141754-\$).did. | US-PGPUB; USPAT | OR | OFF | 2006/03/20 14:10 |

EAST Search History

| | | | | | | |
|-----|----|---|--------------------|----|-----|------------------|
| S14 | 14 | S13 and ((second "than one") same water\$mark\$3) | US-PGPUB; USPAT | OR | OFF | 2006/03/20 14:12 |
| S15 | 1 | "6522769".pn. | US-PGPUB; USPAT | OR | OFF | 2006/03/20 15:26 |
| S16 | 0 | "secure personal data server" | US-PGPUB; USPAT | OR | OFF | 2006/03/22 10:50 |
| S17 | 36 | "personal data server" | US-PGPUB; USPAT | OR | OFF | 2006/03/22 15:53 |



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-----------------|----------------------|----------------------------|------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 | 8028 |
| | 7590 04/03/2006 | | EXAMINER HAST, NATHAN D | |
| Wiley Rein & Fielding Intellectual Property Department 1776 K Street NW Washington, DC 20006 | | | ART UNIT | PAPER NUMBER |
| | | | 2136 | |
| DATE MAILED: 04/03/2006 | | | | |

Please find below and/or attached an Office communication concerning this application or proceeding.



e

| | | | |
|------------------------------|-------------------------------|-------------------------------------|--|
| Office Action Summary | Application No. 10/049,101 | Applicant(s) MOSKOWITZ, SCOTT A. | |
| | Examiner Nathan D. Hast | Art Unit 2136 | |

- The MAILING DATE of this communication appears on the cover sheet with the correspondence address -

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 October 2004.
- 2a) This action is FINAL.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-30 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-30 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 23 July 2002 is/are: a) accepted or b) objected to by the Examiner.
 - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-949)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/09)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____

DETAILED ACTION

Acknowledgement of Papers

1. This office action is in response to all papers sent and received as of 03/24/2003.

Priority

2. The examiner acknowledges that there is a claim to priority in a previous application, a provisional (Application # 60/147,134) filed on 08/04/1999.

Information Disclosure Statement

3. The examiner notes that are no Information Disclosure Statements are available for consideration or review at the time of examination.

Claim Objections

4. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered **consecutively** beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim second 26 been renumbered 27.

Misnumbered claim original 27 been renumbered 28.

Misnumbered claim original 28 been renumbered 29.

Misnumbered claim original 29 been renumbered 30.

Misnumbered claim original 30 been renumbered 31.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-30 rejected under 35 U.S.C. 102(e) as being anticipated by Rhoads et al. (Rhoads) via United States Patented number US 6,522,769 B1.

7. As per claim 1, a local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication (Column 25, Lines 17-18, "serial port or network connection") for connecting the system via a network (Column 3, Lines 39-41, "internet") to at least one Secure Electronic Content Distributor (Figure 1, "E-music Distributor", "is a diagram showing the participants, and channels, involved in the distribution of music") (SECD), said SECD capable of storing (Column 10, Lines 3-6, "database") a plurality of data sets, capable of receiving a request (Column 10, Lines 3-6, "requested data") to transfer at least one content data set (Column 3, Lines 51-53,

"download"), and capable of transmitting the at least one content data set in a secured transmission;

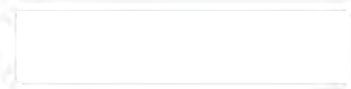
b) a rewritable storage medium (Column 3, Lines 51-53, "personal digital audio players") whereby content received (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) from outside the LCS may be stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) and retrieved,

c) a domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and

d) a programmable address (Column 4, Lines 51-56, "Master Global Address (MGA)", "Unique Identifier or UID") module which can be programmed with an identification code uniquely associated with the LCS; and

said domain processor, permitting the LCS to receive (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) digital content (Column 3, Lines 45-53, "music label", "digital media outlets", "download") from outside the LCS provided the LCS first determines that the digital content being delivered (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) to the LCS is authorized for use by the LCS.

8. Regarding claim 2, the LCS of claim 1 further comprising



e) an interface (Column 3, Lines 45-53, "music label", "digital media outlets", "download") to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) and transmitting digital content (Column 6, Lines 7-65, "Class 2", "digital output", "Class 3", it is possible to move content to and from the portable device to a personal computer);

and wherein said domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") permits the LCS to receive (Column 3, Lines 51-53, "download") digital content from an SECD (Figure 1, "E-music Distributor", "record label", "is a diagram showing the participants, and channels, involved in the distribution of music") that is connected to the LCS's communication port (Column 25, Lines 17-18, "serial port or network connection"), provided the LCS first determines that digital content being received is authorized (Column 6, Lines 7-65, "A device to which such MP3 audio is provided would check the usage control string data to determine whether it is authorized to utilize the audio.") for use by the LCS,

and wherein said domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") permits the LCS to deliver (Column 3, Lines 51-53, "download") digital content to an SU that may be connected to the LCS's interface (Column 3, Lines 45-53, "music label", "digital media outlets", "download"), provided the LCS first determines that digital content being received is authorized (Column 6, Lines 7-11, "authorized") for use by the SU

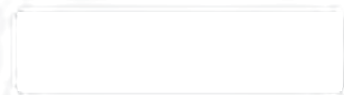


9. As per claim 3, A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port (Column 25, Lines 17-18, "serial port or network connection") in communication for connecting the system via a network (Column 3, Lines 39-41, "internet") to at least one Secure Electronic Content Distributor (Figure 1, "E-music Distributor", "is a diagram showing the participants, and channels, involved in the distribution of music") (SECD), said SECD (Figure 1, "E-music Distributor", "record label", "is a diagram showing the participants, and channels, involved in the distribution of music") capable of storing (Column 10, Lines 3-6, "database") a plurality of data sets, capable of receiving a request (Column 10, Lines 3-6, "requested data") to transfer at least one content data set, and capable of transmitting (Column 3, Lines 51-53, "download") the at least one content data set in a secured transmission;

b) an interface (Column 3, Lines 45-53, "music label", "digital media outlets", "download") to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving (Column 3, Lines 51-53, "download") and transmitting (Figure 1, "internet download", "streaming delivery") digital content; and

c) a rewritable storage medium whereby content received (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) from an SECD and from an SU may be stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) and retrieved;



d) a domain processor that imposes rules (Column 2, Lines 9-11 and 15-19, "detector", "rules") and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU, and

e) a programmable address module (Column 4, Lines 51-56, "Master Global Address (MGA)", "Unique Identifier or UID") which can be programmed with an identification code uniquely associated with the LCS;

said domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") permitting the LCS to deliver (Figure 1, "internet download", "streaming delivery") digital content to and receive (Column 10, Lines 3-6, "requested data") digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) to the SU is authorized (Column 6, Lines 7-11, "authorized") for use by the SU or that the digital content being received (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) is authorized for use by the LCS,

and said domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") permitting the LCS to receive digital content from an SECD (Column 3, Lines 45-53, "music label", "digital media outlets", "download") that is connected to the LCS's communication port provided the LCS first determines that digital content being received is authorized (Column 6, Lines 7-11, "authorized") for use by the LCS,

10. Regarding claim 4, the system of claim 3, wherein said domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") determines whether digital content is authorized (Column 6, Lines 7-11, "authorized") for use by extracting (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") a watermark from the digital content being transferred.

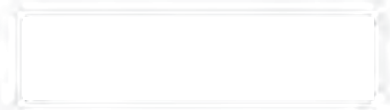
11. Regarding claim 5, the system of claim 3, wherein said domain processor comprises:

means for obtaining an identification code (Column 4, Lines 44-45, "digital object identifier") from an SU connected to the LCS's interface;

an analyzer to analyze the identification code (Column 6, Lines 7-65, "the usage control string") from the SU to determine if the SU is an authorized (Column 6, Lines 7-11, "authorized") device for communicating with the LCS;

means for analyzing digital content (Column 6, Lines 7-65, "A device to which such MP3 audio is provided would check the usage control string data to determine whether it is authorized to utilize the audio.") received from an SU;

said system permitting the digital content (Column 6, Lines 7-65, "Class 2", "digital output", "Class 3", it is possible to move content from and portable device to a personal computer) to be stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) in the LCS if i) an analysis of the digital content received from the SU concludes that the content is authenticated (Column 6, Lines 7-65, "pre-authorization"), or ii) an analysis of the digital content received from the SU concludes that the content cannot (Column 6, Lines 7-65, "0 - no playback permitted") be



authenticated because no authentication data (Column 6, Lines 7-11, "authorized") is embedded in the content, and

said system preventing (Column 11, Lines 30-34, "copy-protection") the digital content from being stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) on the LCS if i) an analysis of the digital content received from the SU concludes that the content is unauthenticated.

12. Regarding claim 6, the system of claim 4, wherein said analyzer of the domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules") comprises means for extracting digital (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code (Column 4, Lines 51-56, "Master Global Address (MGA)", "Unique Identifier or UID") of the LCS.

13. Regarding claim 7, the system of claim 4, wherein said system permits the digital content to be stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) in the LCS at a degraded quality (Column 13, Lines 34-45, "lower quality") level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated (Column 6, Lines 7-11, "authorized") because there is no authentication (Column 19, Lines 61-64, "watermark", "missing" or "garbled") data embedded in the content.



14. Regarding claim 8, the system of claim 4, further comprising at least one SU (Column 3, Lines 51-53, "personal digital audio players"), each such SU being capable of communicating with the LCS.

15. Regarding claim 9, the system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message (Column 9-10, Lines 63-6, "the appliance can contact the remote database") from the SU to confirm that the SU is authorized to use the LCS;

means to retrieve a copy of the (Column 10, Lines 1-2, "forward data") requested content data set;

means to embed (Column 1, Lines 44-49, "embedded") at least one robust (Column 5, Lines 52-55, "robustness") open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized"),

means to embed a second watermark (Column 14, Lines 20-25, "second watermark") into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the watermarked content data set to the SU for its use.

16. Regarding claim 10, the system of claim 8, further comprising a SECD (Figure 1, "E-music Distributor", "is a diagram showing the participants, and channels, involved in the distribution of music"), said SECD capable of receiving a request (Column 10, Lines 3-6, "requested data") to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

17. Regarding claim 11, the system of claim 10,

wherein the SU includes means to (Column 9-10, Lines 63-6, "the appliance can contact the remote database") send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) on the LCS, but which the LCS can obtain (Column 3, Lines 51-53, "download") from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve (Column 10, Lines 1-2, "forward data") a copy of the requested content data set;

means to embed at least one robust (Column 5, Lines 52-55, "robustness") open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized");

means to embed a second watermark (Column 14, Lines 20-25, "second watermark") into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the watermarked content data set to the LCS for its use; and

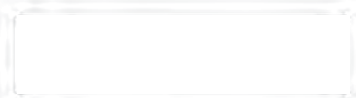
wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized (Column 6, Lines 7-11, "authorized") to use the LCS;

means to receive (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) a copy of the requested content data set as transmitted by the SECD (Figure 1, "E-music Distributor", "record label", "is a diagram showing the participants, and channels, involved in the distribution of music");

means to extract (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") at least one watermark to confirm that the content data is authorized (Column 6, Lines 7-11, "authorized") for use by the LCS;

means to embed at least one robust (Column 5, Lines 52-55, "robustness") open watermark into the copy of the requested content data set,



said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized");

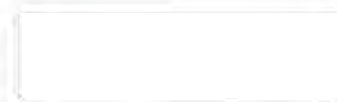
means to embed a second watermark (Column 14, Lines 20-25, "second watermark") into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the watermarked content data set to the SU for its use.

18. Regarding claim 12, the system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized (Column 6, Lines 7-11, "authorized") to use the LCS;

means receive (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) a copy of the content data set;



means to determine if a robust (Column 5, Lines 52-55, "robustness") open watermark is embedded (Column 1, Lines 44-49, "embedded") in the content data set, and to extract the robust open watermark if it is determined that one exists;

means to analyze any extracted robust (Column 5, Lines 52-55, "robustness") open watermarks to determine if the content data set can be authenticated (Column 6, Lines 7-11, "authorized");

means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates (Column 6, Lines 7-11, "authorized") the content data set, or ii) the LCS determines that no robust (Column 5, Lines 52-55, "robustness") open watermark is embedded (Column 1, Lines 44-49, "embedded") in the content signal.

19. Regarding claim 13, the system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized (Column 6, Lines 7-11, "authorized") for use by the SU or which has been determined to be legacy content such the data contains no additional information to permit authentication.

20. Regarding claim 15, the system of claim 5, wherein the LCS further comprises:

means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) in the rewritable storage medium.

21. As per claim 16, a system for creating a secure environment for digital content, comprising:



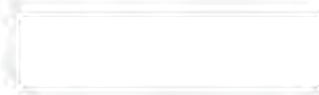
a Secure Electronic Content Distributor (Figure 1, "E-music Distributor", "record label", "is a diagram showing the participants, and channels, involved in the distribution of music") (SECD);

a Local Content Server (Figure 1, "Consumer PC") (LCS);

a communications network (Column 3, Lines 39-41, "internet")
interconnecting the SECD to the LCS; and

a Satellite Unit (SU) capable (Column 3, Lines 51-53, "personal digital audio players") of interfacing (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) with the LCS;

said SECD (Figure 1, "E-music Distributor", "record label", "is a diagram showing the participants, and channels, involved in the distribution of music") comprising: a storage device for storing (Column 10, Lines 3-6, "database") a plurality of data sets, an input for receiving (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise securitizing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network (Column 3, Lines 39-41, "internet") to the LCS;



said LCS comprising: a domain processor (Column 2, Lines 9-11 and 15-19, "detector", "rules"); a first interface (Column 3, Lines 45-53, "music label", "digital media outlets", "download") for connecting to a communications network (Column 3, Lines 39-41, "internet"); a second interface for communicating with the SU, a memory device for storing (Column 10, Lines 3-6, "database") a plurality of data sets; and a programmable address (Column 4, Lines 51-56, "Master Global Address (MGA)", "Unique Identifier or UID") module which can be programmed with an identification code uniquely associated with the LCS; and

said SU being a portable module comprising: a memory for accepting secure digital content from a LCS; an interface (Column 3, Lines 45-53, "music label", "digital media outlets", "download") for communicating with the LCS, and a programmable address (Column 4, Lines 51-56, "Master Global Address (MGA)", "Unique Identifier or UID") module which can be programmed with an identification code uniquely associated with the SU.

22. As per claim 17, a method for creating a secure environment for digital content for a consumer, comprising the following steps:

 sending a message indicating that a user is requesting (Column 10, Lines 3-6, "requested data") a copy of a content data set;

 retrieving a (Column 10, Lines 1-2, "forward data") copy of the requested content data set.

embedding at least one robust (Column 5, Lines 52-55, "robustness") open watermark into the copy of the requested content data set said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized");

embedding a second watermark (Column 14, Lines 20-25, "second watermark") into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting users;

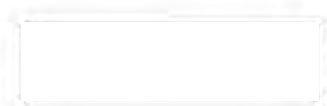
transmitting the watermarked content data (Column 3, Lines 51-53, "download") set to the requesting consumer via an electronic network (Column 3, Lines 39-41, "internet");

receiving (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the transmitted watermarked content data set into a Local Content Server (LCS) of the user;

extracting (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") at least one watermark from the transmitted watermarked content data set; and

permitting use of the content data set if the LCS determines that use is authorized (Column 6, Lines 7-11, "authorized").

23. Regarding claim 18, the Method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized (Column 6, Lines 7-11, "authorized") comprises:



checking to see if a watermark extracted (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") from the content data set includes information which matches unique information which is associated with the user; and

permitting the storage of the content data set in a storage unit for the LCS

24. Regarding claim 19, the Method of claim 17, further comprising:

connecting a Satellite Unit (SU) to an LCS, and wherein the step of permitting use of the content data set if the LCS determines that use is authorized (Column 6, Lines 7-11, "authorized") comprises:

checking to see if a watermark extracted (Column 2, Lines 9-11 and 15-19, "detector", "rules", "watermark signal extracted") from the content data set includes information which matches unique information which is associated with the user; and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the content data set to the SU for its use.

25. As per claim 20, a method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to (Column 3, Lines 58-62, "personal audio appliance", "personal computer", "Electronic music download", with the personal computer as an "intermediary" it is implied that all are connected to it) an local content server (LCS),

sending a message indicating that the SU is requesting (Column 10, Lines 3-6, "requested data") a copy of a content data set that is stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized (Column 6, Lines 7-11, "authorized") to use the LCS; and

retrieving (Column 10, Lines 1-2, "forward data") a copy of the requested content data set;

assessing whether a secured connection (Column 3, Lines 39-41, "internet", "secure links") exists between the LCS and the SU;

if a secured connection exists, embedding (Column 1, Lines 44-49, "embedded") a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the content data set to the SU for its use.

26. Regarding claim 21, the method of claim 20, further comprising:

embedding (Column 1, Lines 44-49, "embedded") an open watermark into the content data to permit enhanced usage of the content data by the user.

27. Regarding claim 22, the method of claim 21, further comprising:



embedding (Column 1, Lines 44-49, "embedded") at least one additional watermark into the content data, said at least one additional (Column 14, Lines 20-25, "second watermark") watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis (Column 25, Lines 7-9, "forensic data") to provide information on the history of the content data's use.

28. Regarding claim 23, the method of claim 20, wherein the content data can be stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) at a level of quality (Column 21, Lines 27-35, "preventing the user's full enjoyment", reduces quality of the stored media) which is selected by a user.

29. As per claim 24, a method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) (Column 3, Lines 58-62, "personal audio appliance", "personal computer", "Electronic music download", with the personal computer as an "intermediary" it is implied that all are connected to it) to an local content server (LCS),

sending a message indicating that the SU is requesting (Column 10, Lines 3-6, "requested data") a copy of a content data set that is stored (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized (Column 6, Lines 7-11, "authorized") to use the LCS, and

retrieving (Column 10, Lines 1-2, "forward data") a copy of the requested content data set;

assessing whether a secured connection (Column 3, Lines 39-41, "internet", "secure links") exists between the LCS and the SU;

if a secured connection exists, embedding (Column 1, Lines 44-49, "embedded") a watermark into the copy of the requested (Column 10, Lines 3-6, "requested data") content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) the watermarked content data set to the SU for its use.

30. Regarding 25, the method of claim 24, further comprising:

embedding (Column 1, Lines 44-49, "embedded") at least one robust (Column 5, Lines 52-55, "robustness") open watermark into the copy of the requested content data set before the requested content data is delivered (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) to the SU, said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized").

31. Regarding 26, the method of claim 25, wherein the robust (Column 5, Lines 52-55, "robustness") watermark is embedded using any one of a plurality of embedding algorithms (Column 1, Lines 44-49, "embedded").

32. Regarding 27, the method of claim 24, further comprising:



embedding (Column 1, Lines 44-49, "embedded") a watermark which includes a hash value from a one-way hash function generated using the content data (Column 5, Line 10, "checksum", can be an include parameter on a watermark).

33. Regarding 28, the method of claim 25, wherein the robust (Column 5, Lines 52-55, "robustness") watermark can be periodically replaced (Column 5, Lines 37-43, "replace previously-stored data") with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.

34. Regarding 29, the method of claim 24, further comprising the step of; embedding additional robust (Column 5, Lines 52-55, "robustness") open watermarks into the copy of the requested content data set before the requested content data is delivered (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) to the SU, using a new algorithm; and

re-saving the newly watermarked (Column 5, Lines 37-43, "replace previously-stored data") copy to the LCS.

35. Regarding 30, the method of claim 24, further comprising the step of:

saving a copy of the requested content data with the robust (Column 5, Lines 52-55, "robustness") watermark to the rewritable media of the LCS.

36. Regarding 31, a method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting (Column 25, Lines 17-18, "serial port or network connection") a Satellite Unit (SU) to an local content server (LCS).



sending a message indicating that the SU is requesting to store (Figure 1, "CD-R HARDDRIVE DVD-R TAPE", storage on a re-writable format) a copy of a content data on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized (Column 6, Lines 7-11, "authorized") to use the LCS, and

receiving a copy (Column 3, Lines 45-61, "music label", "digital media outlets", "download", to "personal digital audio player" or "writeable media" such as a personal computer) of the content data set;

assessing whether the content data set is authenticated (Column 6, Lines 7-11, "authorized");

if the content data is unauthenticated (Column 6, Lines 7-85, "0 – no playback permitted"), denying access (Column 11, Lines 30-34, "copy-prevention") to the LCS storage unit; and

if the content data is not capable of authentication, accepting the data at a predetermined quality level (Column 13, Lines 34-45, "lower quality"), said predetermined quality level having been set for legacy content.

Claim Rejections - 35 USC § 103

37. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

38. Claim 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Rhoads et al. (Rhoads) in view of Quackenbush et al. (Quackenbush).

39. Rhoads discloses, the system of claim 5, wherein the LCS further comprises:

means to embed at least one robust (Column 5, Lines 52-55, "robustness") open watermark into a copy of content data, said watermark indicating that the copy is authenticated (Column 6, Lines 7-11, "authorized");

means to embed a second watermark (Column 14, Lines 20-25, "second watermark") into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS.

40. Rhoads does not expressly disclose, means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

41. Quackenbush discloses, means to embed a third watermark (Column 5, Lines 14-17, "third watermark"), more specifically as fragile (Column 7, Line 63, "Least Significant Bit (LSB)") watermark.

42. Rhoads and Quackenbush are analogous art because they are from the similar problem solving area of copy protection and document authentication.

43. At the time of invention it would have been obvious to a person of ordinary skill in the art to add a third and fragile watermark to the already embedded first and second watermarks for the addition protection provided.

44. The motivation for doing so would have been that it will be appreciated that a fragile watermark is designed to be lost or predictably degrade upon certain types of signal processing, which would help to ensure copy-prevention.

45. Therefore, it would have been obvious to combine Rhoads with Quackenbush for the benefit of increase rule enforcement to obtain the invention as specified in claim 14.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892 for additional art.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nathan D. Hast whose telephone number is (571) 272-6558. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nathan D. Hast
Examiner
Art Unit 2136


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

| | | | |
|-----------------------------------|---------------------------------------|--|-------------|
| Notice of References Cited | Application/Control No. 10/049,101 | Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A. | |
| | Examiner Nathan D. Hast | Art Unit 2136 | Page 1 of 1 |

U.S. PATENT DOCUMENTS

| * | | Document Number Country Code-Number-Kind Code | Date MM-YYYY | Name | Classification |
|---|---|--|-----------------|---------------------|----------------|
| * | A | US-6,522,769 B1 | 02-2003 | Rhoads et al. | 382/100 |
| * | B | US-2005/0160271 A9 | 07-2005 | Brundage et al. | 713/176 |
| * | C | US-6,665,489 B2 | 12-2003 | Collart, Todd R. | 386/94 |
| * | D | US-2004/0128514 A1 | 07-2004 | Rhoads, Geoffrey B. | 713/176 |
| * | E | US-2004/0037449 A1 | 02-2004 | Davis et al. | 382/100 |
| * | F | US-6,823,455 B1 | 11-2004 | Macy et al. | 713/176 |
| * | G | US-2003/0133702 A1 | 07-2003 | COLLART, TODD R. | 386/125 |
| * | H | US-6,668,246 B1 | 12-2003 | Yeung et al. | 705/57 |
| * | I | US-6,405,203 B1 | 06-2002 | Collart, Todd R. | 707/10 |
| * | J | US-6,141,754 A | 10-2000 | Choy, David M. | 726/1 |
| | K | US- | | | |
| | L | US- | | | |
| | M | US- | | | |

FOREIGN PATENT DOCUMENTS

| * | | Document Number Country Code-Number-Kind Code | Date MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
| | N | | | | | |
| | O | | | | | |
| | P | | | | | |
| | Q | | | | | |
| | R | | | | | |
| | S | | | | | |
| | T | | | | | |

NON-PATENT DOCUMENTS

| * | | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
| | U | |
| | V | |
| | W | |
| | X | |

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 8028

| | | | | |
|-----------------------------|--|--------------|------------------------|-----------------------------------|
| SERIAL NUMBER 10/049,101 | FILING DATE 07/23/2002 RULE <i>ADH</i> | CLASS 713 | GROUP ART UNIT 2136 | ATTORNEY DOCKET NO. 80408.0011 |
|-----------------------------|--|--------------|------------------------|-----------------------------------|

APPLICANTS

Scott A. Moskowitz, Miami, FL: *ADH*

** CONTINUING DATA **

This application is a 371 of PCT/US00/21189 08/04/2000
 which claims benefit of 60/147,134 08/04/1999
 and claims benefit of 60/213,489 06/23/2000 *ADH*

** FOREIGN APPLICATIONS **

** SMALL ENTITY **

| | | | | |
|--|---|------------------------|--------------------|-------------------------|
| Foreign Priority claimed <input type="checkbox"/> yes <input checked="" type="checkbox"/> no | STATE OR COUNTRY FL | SHEETS DRAWING 7 | TOTAL CLAIMS 30 | INDEPENDENT CLAIMS 7 |
| 35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after allowance | Verified and Acknowledged <i>ADH</i> Examiner's Signature | Initials <i>ADH</i> | | |

ADDRESS

Wiley Rein & Fielding
 Intellectual Property Department
 1776 K Street NW
 Washington, DC
 20006 *ADH*

TITLE

Secure personal content server

| | | |
|----------------------------|---|--|
| FILING FEE RECEIVED 702 | FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following: | <input checked="" type="checkbox"/> All Fees <i>ADH</i> <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other |
|----------------------------|---|--|

Index of Claims



Application/Control No.

10/049,101

Examiner

Nathan D. Hast

Applicant(s)/Patent under Reexamination

MOSKOWITZ, SCOTT A.

Art Unit

2136

| | |
|---|----------|
| X | Rejected |
| = | Allowed |

| | |
|---|--------------------------------|
| - | (Through numeral) Cancelled |
| + | Restricted |

| | |
|---|--------------|
| N | Non-Elected |
| I | Interference |

| | |
|---|----------|
| A | Appeal |
| O | Objected |

| Claim | | Date | |
|-------|----------|---------|--|
| Final | Original | | |
| | | 3/15/01 | |
| 1 | X | | |
| 2 | X | | |
| 3 | X | | |
| 4 | X | | |
| 5 | X | | |
| 6 | X | | |
| 7 | X | | |
| 8 | X | | |
| 9 | X | | |
| 10 | X | | |
| 11 | X | | |
| 12 | X | | |
| 13 | X | | |
| 14 | X | | |
| 15 | X | | |
| 16 | X | | |
| 17 | X | | |
| 18 | X | | |
| 19 | X | | |
| 20 | X | | |
| 21 | X | | |
| 22 | X | | |
| 23 | X | | |
| 24 | X | | |
| 25 | X | | |
| 26 | X | | |
| 27 | X | | |
| 28 | X | | |
| 29 | X | | |
| 30 | X | | |
| 31 | | | |
| 32 | | | |
| 33 | | | |
| 34 | | | |
| 35 | | | |
| 36 | | | |
| 37 | | | |
| 38 | | | |
| 39 | | | |
| 40 | | | |
| 41 | | | |
| 42 | | | |
| 43 | | | |
| 44 | | | |
| 45 | | | |
| 46 | | | |
| 47 | | | |
| 48 | | | |
| 49 | | | |
| 50 | | | |

| Claim | | Date | |
|-------|----------|------|--|
| Final | Original | | |
| 51 | | | |
| 52 | | | |
| 53 | | | |
| 54 | | | |
| 55 | | | |
| 56 | | | |
| 57 | | | |
| 58 | | | |
| 59 | | | |
| 60 | | | |
| 61 | | | |
| 62 | | | |
| 63 | | | |
| 64 | | | |
| 65 | | | |
| 66 | | | |
| 67 | | | |
| 68 | | | |
| 69 | | | |
| 70 | | | |
| 71 | | | |
| 72 | | | |
| 73 | | | |
| 74 | | | |
| 75 | | | |
| 76 | | | |
| 77 | | | |
| 78 | | | |
| 79 | | | |
| 80 | | | |
| 81 | | | |
| 82 | | | |
| 83 | | | |
| 84 | | | |
| 85 | | | |
| 86 | | | |
| 87 | | | |
| 88 | | | |
| 89 | | | |
| 90 | | | |
| 91 | | | |
| 92 | | | |
| 93 | | | |
| 94 | | | |
| 95 | | | |
| 96 | | | |
| 97 | | | |
| 98 | | | |
| 99 | | | |
| 100 | | | |

| Claim | | Date | |
|-------|----------|------|--|
| Final | Original | | |
| 101 | | | |
| 102 | | | |
| 103 | | | |
| 104 | | | |
| 105 | | | |
| 106 | | | |
| 107 | | | |
| 108 | | | |
| 109 | | | |
| 110 | | | |
| 111 | | | |
| 112 | | | |
| 113 | | | |
| 114 | | | |
| 115 | | | |
| 116 | | | |
| 117 | | | |
| 118 | | | |
| 119 | | | |
| 120 | | | |
| 121 | | | |
| 122 | | | |
| 123 | | | |
| 124 | | | |
| 125 | | | |
| 126 | | | |
| 127 | | | |
| 128 | | | |
| 129 | | | |
| 130 | | | |
| 131 | | | |
| 132 | | | |
| 133 | | | |
| 134 | | | |
| 135 | | | |
| 136 | | | |
| 137 | | | |
| 138 | | | |
| 139 | | | |
| 140 | | | |
| 141 | | | |
| 142 | | | |
| 143 | | | |
| 144 | | | |
| 145 | | | |
| 146 | | | |
| 147 | | | |
| 148 | | | |
| 149 | | | |
| 150 | | | |



Tim

PTO/SB/01 (05-04)
 Approved for use through 07/31/2005. OMB 0651-0031
 U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Project of 1995, no response is required to respond to a collection of information unless it displays a valid OMB control number.

| | | | |
|--|----------------------|----------------------------|------------|
| TRANSMITTAL FORM <small>(to be used for all correspondence after initial filing)</small> | Application Number | 10/049,101 | |
| | Filing Date | July 23, 2002 | |
| | First Named Inventor | Scott A. MOSKOWITZ, et al. | |
| | Art Unit | 2136 | |
| | Examiner Name | Nathan D. Hast | |
| Total Number of Pages in This Submission | 3 | Attorney Docket Number | 80408.0011 |

| ENCLOSURES (Check all that apply) | | |
|---|---|---|
| <input type="checkbox"/> Fee Transmittal Form | <input type="checkbox"/> Drawing(s) | <input type="checkbox"/> After Allowance Communication to TC |
| <input type="checkbox"/> Fee Attached | <input type="checkbox"/> Licensing-related Papers | <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences |
| <input type="checkbox"/> Amendment/Reply | <input type="checkbox"/> Petition | <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) |
| <input type="checkbox"/> After Final | <input type="checkbox"/> Petition to Convert to a Provisional Application | <input type="checkbox"/> Proprietary Information |
| <input type="checkbox"/> Affidavits/declaration(s) | <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address | <input type="checkbox"/> Status Letter |
| <input type="checkbox"/> Extension of Time Request | <input type="checkbox"/> Terminal Disclaimer | <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): |
| <input type="checkbox"/> Express Abandonment Request | <input type="checkbox"/> Request for Refund | Revocation of Power of Attorney (Michael Berty); Revocation of Power of Attorney (Scott A. Moskowitz); Revocation of Power of Attorney (Blue Spike) |
| <input type="checkbox"/> Information Disclosure Statement | <input type="checkbox"/> CD, Number of CD(s) _____ | |
| <input type="checkbox"/> Certified Copy of Priority Document(s) | <input type="checkbox"/> Landscape Table on CD | |
| <input type="checkbox"/> Reply to Missing Parts/Incomplete Application | Remarks | |
| <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53 | | |

| SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT | | | |
|--|---------------------------|----------|--------|
| Firm Name | Wilay Rein & Fielding LLP | | |
| Signature | <i>Floyd B. Chapman</i> | | |
| Printed name | Floyd B. Chapman | | |
| Date | June 6, 2006 | Reg. No. | 40,555 |

| CERTIFICATE OF TRANSMISSION/MAILING | | |
|---|----------|------|
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below: | | |
| Signature | <i>F</i> | |
| Typed or printed name | | Date |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. 8028
Applicant : Scott A. MOSKOWITZ
and Michael BERRY
Filed : July 23, 2002
TC/A.U. : 2136
Examiner : Nathan D. HAST
Docket No. : 80408.0011

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REVOCATION OF POWER OF ATTORNEY

I, Michael Berry, residing at 12401 Princess Jeanne, Albuquerque, New Mexico 87112, being one of the two co-inventors in the above-identified patent application, hereby revoke all powers of attorney previously given in connection with U.S. Application No. 10/049,101 (including without limitation the powers of attorney previously granted to the attorneys of Wiley Rein & Fielding).

Please update the correspondence address as follows:

Scott A. Moskowitz
16711 Collins Avenue, #2505
Miami, FL 33160

Telephone/Facsimile: 305-956-9041

Date: 5/24, 2006


Michael Berry



THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. 8028
Applicant : Scott A. Moskowitz et al.
Filed : 02/08/2002
TC/A.U. : 2136
Examiner : Hast, Nathan D.
Docket No. : 80408.0011
Title : Secure Personal Content Server

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REVOCATION OF POWER OF ATTORNEY

I, Scott A. Moskowitz, residing at 16711 Collins Avenue, No. 2505, Miami, Florida 33160, being one of two co-inventors in the above-identified patent application, hereby revoke all powers of attorney previously given in connection with U.S. Application No. 10/049,101 (including without limitation the powers of attorney previously granted to the attorneys of Wiley Rein & Fielding).

Please update the correspondence address as follows:

Scott A. Moskowitz
16711 Collins Avenue, #2505
Miami, FL 33160

Telephone/Facsimile: 305-956-9041

Date: June 1, 2006

Scott A. Moskowitz



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. 8028
Applicant : Scott A. Moskowitz et al.
Filed : 02/08/2002
TC/A.U. : 2136
Examiner : Hast, Nathan D.

Docket No. : 80408.0011

Title : Secure Personal Content Server

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

REVOCATION OF POWER OF ATTORNEY

I, Scott A. Moskowitz, as president of assignee Blue Spike, Inc., the sole owner of the entire right to the above identified application, hereby revoke all powers of attorney previously given in connection with this case (including without limitation the power of attorney previously granted to the attorneys of Wiley Rein & Fielding under 37 CFR 3.71, which was filed on or about July 23, 2002).

Please update the correspondence address as follows:

Scott A. Moskowitz
Blue Spike, Inc.
16711 Collins Avenue, #2505
Miami, FL 33160

Telephone/Facsimile: 305-956-9041

Date: June 1, 2006

By:

Scott A. Moskowitz, as President of
Blue Spike, Inc.



UNITED STATES PATENT AND TRADEMARK OFFICE

JR

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 | 8028 |

7590 06/15/2006
Wiley Rein & Fielding
Intellectual Property Department
1776 K Street NW
Washington, DC 20006

EXAMINER

AVERY, JEREMIAH L

ART UNIT PAPER NUMBER

2131

DATE MAILED: 06/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



| | | | |
|--------------------------|--------------------------------------|--|--|
| Interview Summary | Application No. 10/049,101 | Applicant(s) MOSKOWITZ, SCOTT A. | |
| | Examiner Jeremiah Avery | Art Unit 2131 | |

All participants (applicant, applicant's representative, PTO personnel):

- (1) Jeremiah Avery (3) _____
(2) Scott Moskowitz (4) _____

Date of Interview: 09 June 2006

Type: a) Telephonic b) Video Conference
c) Personal [copy given to: 1) applicant 2) applicant's representative]

Exhibit shown or demonstration conducted: d) Yes e) No.
If Yes, brief description: _____

Claim(s) discussed: _____

Identification of prior art discussed: _____

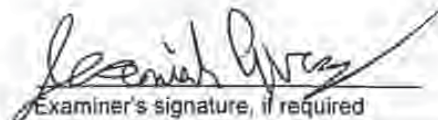
Agreement with respect to the claims f) was reached, g) was not reached, h) N/A.

Substance of interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Discussed the relevancy of the prior art with respect to the claimed invention as pertaining to signal quality, subreference quality and other such aspects.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.


Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135, (35 U.S.C. 132).

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section B12.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action).

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

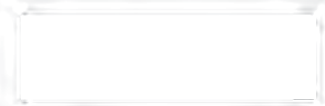
A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted.
- 2) an identification of the claims discussed.
- 3) an identification of the specific prior art discussed.
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner.
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner.
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed; and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.





Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. 8028
Applicant : Scott A. Moskowitz, et al.
Filed : July 23, 2002
TC/A.U. : 2131 (originally, 2136)
Examiner : Jeremiah AVERY (originally, Nathan D. HAST)

Docket No. : 80408.0011

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

In response to the Office Action of April 3, 2006 Applicants provide the following remarks:



Amendments to the Claims:

Please amend the claim numbering, without prejudice or disclaimer, in accordance with the express requests stated in the Office Action dated April 3, 2006. Please amend the following: Claims 1, 3, 13, 16, 17, 18, 19, 20, 21, 22, 24, and 31 without prejudice or disclaimer. The amendments to claims 13, 18, 19, 21, 22 and 31 are being made to correct typographical errors and are not being made for reasons of patentability. This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:
 - a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;
 - b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved;
 - c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS;and
 - d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and
said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS[.]and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

2. (original) The LCS of claim 1 further comprising
- e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS, and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.
3. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:
- a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;
 - b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and
 - c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved;
 - d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU; and

e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS;

said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS, and if the digital content is not authorized for use, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content,

and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS[,] and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

4. (original) The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred.
5. (original) The system of claim 3, wherein said domain processor comprises:
 - means for obtaining an identification code from an SU connected to the LCS's interface;
 - an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS;
 - means for analyzing digital content received from an SU;

said system permitting the digital content to be stored in the LCS if
i) an analysis of the digital content received from the SU concludes that
the content is authenticated, or ii) an analysis of the digital content
received from the SU concludes that the content cannot be authenticated
because no authentication data is embedded in the content, and
said system preventing the digital content from being stored on the
LCS if i) an analysis of the digital content received from the SU concludes
that the content is unauthenticated.

6. (original) The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code of the LCS.
7. (original) The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated because there is no authentication data embedded in the content.
8. (original) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.
9. (original) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:
means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS;
and

means to deliver the watermarked content data set to the SU for its use.

10. (original) The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11. (original) The system of claim 10, wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS;
and

means to deliver the watermarked content data set to the SU for its use.

12. (original) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means receive a copy of the content data set;

means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated;



Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. (currently amended) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such that the data contains no additional information to permit authentication.

14. (original) The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS; and

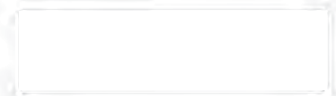
means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

15. (original) The system of claim 5, wherein the LCS further comprises:

means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium.

16. (currently amended) A system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD);



Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

a Local Content Server (LCS);
a communications network interconnecting the SECD to the LCS;
and
a Satellite Unit (SU) capable of interfacing with the LCS;
said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise secur[itz]ing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network to the LCS;
said LCS comprising: a domain processor; a first interface for connecting to a communications network; a second interface for communicating with the SU; a memory device for storing a plurality of data sets; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and
said SU being a portable module comprising: a memory for accepting secure digital content from a LCS, said digital content comprising data which can be authorized for use or which has been determined to be legacy content such that the data contains no additional information to permit authentication; an interface for communicating with the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the SU.

17. (currently amended) A [M]ethod for creating a secure environment for digital content for a consumer, comprising the following steps:
sending a message indicating that a user is requesting a copy of a content data set;



Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

retrieving a copy of the requested content data set;
embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;
embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;
transmitting the watermarked content data set to the requesting consumer via an electronic network;
receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;
extracting at least one watermark from the transmitted watermarked content data set; [and]
permitting use of the content data set if the LCS determines that use is authorized[.] ; and
permitting use of the content data set at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

18. (currently amended) The [M]method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:
checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and
permitting the storage of the content data set in a storage unit for the LCS.

19. (currently amended) The [M]method of claim 17, further comprising:
- connecting a Satellite Unit (SU) to an LCS,

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering the content data set to the SU for its use.

20. (currently amended) A [M]method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to an local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the content data set to the SU for its use, said content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

21. (currently amended) The [M]method of claim 20, further comprising:
embedding an open watermark into the content data to permit
enhanced usage of the content data by the user.
22. (currently amended) The [M]method of claim 21, further comprising:
embedding at least one additional watermark into the content data,
said at least one additional watermark being based on information about
the user, the LCS and an origin of the content data, said watermark
serving as a forensic watermark to permit forensic analysis to provide
information on the history of the content data's use.
23. (original) The method of claim 20, wherein the content data can be stored at
a level of quality which is selected by a user.
24. (currently amended) A [M]method for creating a secure environment for
digital content for a consumer, comprising the following steps:
connecting a Satellite Unit (SU) to an local content server (LCS),
sending a message indicating that the SU is requesting a copy of a
content data set that is stored on the LCS, said message including
information about the identity of the SU;
analyzing the message to confirm that the SU is authorized to use
the LCS; and
retrieving a copy of the requested content data set;
assessing whether a secured connection exists between the LCS
and the SU;
if a secured connection exists, embedding a watermark into the
copy of the requested content data set, said watermark being created
based upon information transmitted by the SU and information about the
LCS; and

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

delivering the watermarked content data set to the SU for its use,
said watermarked content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

25. (original) The method of claim 24, further comprising:

embedding at least one robust open watermark into the copy of the requested content data set before the requested content data is delivered to the SU, said watermark indicating that the copy is authenticated.

26. (original) The method of claim 25, wherein the robust watermark is embedded using any one of a plurality of embedding algorithms.

[26.] 27. (original) The method of claim 24, further comprising:

embedding a watermark which includes a hash value from a one-way hash function generated using the content data.

[27.] 28. (original) The method of claim 25, wherein the robust watermark can be periodically replaced with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.

[28.] 29. (original) The method of claim 24, further comprising the step of:

embedding additional robust open watermarks into the copy of the requested content data set before the requested content data is delivered to the SU, using a new algorithm; and
re-saving the newly watermarked copy to the LCS.

[29.] 30. (original) The method of claim 24, further comprising the step of:

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

[30.] 31. (original) A [M]ethod for creating a secure environment for digital content for a consumer, comprising the following steps:

- connecting a Satellite Unit (SU) to an local content server (LCS),
- sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;
- analyzing the message to confirm that the SU is authorized to use the LCS; and
- receiving a copy of the content data set;
- assessing whether the content data set is authenticated;
- if the content data is unauthenticated, denying access to the LCS storage unit; and
- if the content data is not capable of authentication, accepting the data at a predetermined quality level, said predetermined quality level having been set for legacy content.

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

REMARKS/ARGUMENTS

The Applicants thank Examiner Avery for the time and consideration to discuss the proposed amended claims and the prior art. These discussions took place on June 9, 2006. Examiner Avery acknowledged the differences between the Applicants' invention[s] as being patentable over Rhoads et al. with regards to "signal quality, subreference quality and other such aspects" including the handling of legacy content at a plurality of quality levels. Claims 1, 3, 16, 17, 20, 24, and 31 were discussed as having significant advantages over Rhoads et al. and the prior art demonstrating patentability over Rhoads et al.

Rejections under 35 U.S.C. § 102

§ 102 Rejections based on U.S. Patent 6,522,769 ("Rhoads")

Claims 1-31 (claims have been renumbered to correct a typographical error) stand rejected as allegedly anticipated by U.S. Patent No. 6,522,769 issued to Rhoads (hereafter "Rhoads"). See Page 3 of the April 3, 2006 Office Action.

Claims 1-31

In order for a reference to anticipate a claim, the reference must disclose each and every limitation of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. See *Atlas Powder Co. v. Ireco Inc.*, 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1476, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Currently Amended Independent Claim 1 [emphasis added] recites, "A local content server system (LCS) for creating a secure environment for digital content, comprising: a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission; b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content." The Section 102 rejection of Claim 1

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

is improper for at least the reason that Rhoads fails to disclose "legacy content". Second, Rhoads predicates content use on "pre-authorization" (see, for example, Rhoads at Col. 6 ll. 7-56). This inherently prevents use of legacy content and content in existence prior to Rhoads' alleged LCS being deployed. For this additional reason the 102 rejection should be withdrawn.

The Examiner asserts that Rhoads et al. discloses a local content server ("LCS"), April 3, 2006 Office Action at Page 3. The Applicants respectfully disagree. First, Rhoads relies exclusively on detecting watermarks in content—"legacy content" is denied access to Rhoads' alleged LCS. Second, Rhoads' content carries "pre-authorized" usage rules as "watermark payloads" (for instance, Rhoads at Col. 6 ll. 7-55 describing a "usage control string"). This assumes that any content under Rhoads must have been *both* pre-authorized and watermarked by at least a "usage control string", inherently excluding *legacy content* and content that existed prior to the deployment of an LCS. Third, subsequent "usage control" (see, for instance, Rhoads at Col. 13 ll. 15-50 addressing "embedded watermark data") teaches away from the instant invention's LCS, as per the claim[s] limitations, which can admit legacy content and unwatermarked content to the LCS without use restrictions.

Rhoads, thus, teaches away from enabling access to *any* content that lacks a "watermark payload". See Rhoads at Col. 6 ll. 7-55; more specifically, Rhoads at Col. 6 ll. 48-56 [emphasis added]:

The usage control string can also include a two-bit field (bits ten and eleven) indicating recording permissions. A value of 0 means that data corresponding to the MP3 audio (regardless of digital format) *should never be made available to another digital device*. A value of 1 means that the data corresponding to the MP3 data may be made available once to another digital device. A value of 2 means that the data may be made available an unlimited number of times to other digital devices.

One of ordinary skill in the art can readily appreciate the widespread existence of content in any number of digital formats—released prior to copy protection schemes or released without any use restrictions (e.g., the compact disc). Practically speaking, why seek content with usage control if you can obtain access to legacy content *sans* such usage control (e.g., music ripped from a compact disc)? Second, Rhoads' approach logically requires that all market participants agree to watermark content with "pre-authorization". This presents a largely impractical requirement, as different parties are likely to want different protocols or methods to protect their own content—or leave content without any modifications. The instant invention[s] can handle legacy content and

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

unwatermarked content in a seamless manner. On the other hand, Rhoads' assumption necessarily excludes access to unwatermarked content (from his alleged LCS), limiting the availability of media under his proposed schema. This is why the Applicants' invention offers a significant advantage over the alleged security taught by Rhoads.

Last, Rhoads describes a system focused on usage controls carried by watermark payloads. In contrast, the Applicants' invention represents an advantageous means to handle legacy content (which is likely to continue to exist outside of any system, even those contemplated by Rhoads). One of ordinary skill in the art can readily appreciate the benefits of migrating legacy content as new content is introduced, or when it comes into contact with the instant invention[s], in a manner consistent with protecting copyrights. Rhoads and the prior art fail to mention or describe methods as required by the present invention[s] claim limitations—Rhoads teaches that this content should be **rejected without exception**, Rhoads at Col. 13 ll. 15-25 [emphasis added]:

To illustrate, consider watermarked music. The media owner would be best served if the watermark serves dual purposes: permissive and restrictive. Permissively, music appliances can be designed to play (or record) only music that includes an embedded watermark signaling that such activity is authorized. **By this arrangement, if music is obtained from an unauthorized source and does not include the necessary watermark, the appliance will recognize that it does not have permission to use the music, so will refuse requests to play (or record).**

Rhoads fails to disclose all of the elements of the claimed invention[s], thus, Claim 1 (and all claims that depend therefrom) is patentable over Rhoads. For these additional reasons the section 102 rejections of Claim 1 (and all claims depending therefrom) based on Rhoads should be withdrawn.

Currently Amended Independent Claim 3 (and all claims depending therefrom), Currently Amended Independent Claim 16 (and all claims depending therefrom), Currently Amended Independent Claim 17 (and all claims depending therefrom), Currently Amended Independent Claim 20 (and all claims depending therefrom), and Currently Amended Independent Claim 24 (and all claims depending therefrom) similarly enable content to be used or played in a manner consistent with the content's provenance without additional processing being required by content owners, a significant improvement over Rhoads and the prior art, as argued in connection with Claim 1: "accepting the digital content at a predetermined quality level, said predetermined quality level having been set for

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

legacy content" (Claim 3); "or which has been determined to be legacy content such that the data contains no additional information to permit authentication" (Claim 16); "permitting use of the content data set at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized" (Claim 17); "said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized" (Claim 20); and "said watermarked content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized" (Claim 24). These newly amended independent claims are all distinguished from Rhoads and the prior art as argued previously in connection with Claim 1 (and all claims that depend therefrom).

The Section 102 rejection is improper because Rhoads does not disclose a means for handling legacy content. For at least this reason and the reasons discussed above, Claims 1-31 are patentable over Rhoads. Applicants request that the Examiner withdraw the 102 rejections for Claims 1-31.

Rejections under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. According to the MPEP, "[i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references. MPEP 2142 (citing *Ex parte Clapp*, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing *Ex Parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int'l Royalty Corp. v. Ching-Rong*

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

Wang, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000): "Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" Winner, 202 F. 3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is dispositive in an obviousness determination." *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997).

Applicant submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them. Even assuming *arguendo* that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." *Ex parte Levengood*, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

1. a) § 103 Rejections based on Rhoads in view of Quackenbush et al. (U.S. Patent 6,493,457) as applied to Claim 14

Claim 14 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rhoads in view of Quackenbush et al. (herein after "Quackenbush"). The Examiner asserts that "... Rhoads and Quackenbush are analogous art because they are from the similar problem solving area of copy protection and document authentication ...". April 3, 2006 Office Action at Page 24. Claim 14 depends from Claim 5, which depends from Independent Claim 3. Applicants respectfully disagree. The Applicant discloses legacy content which is admissible to the claimed local content server, or "LCS"—Rhoads prohibits legacy content from his alleged LCS. Quackenbush does not cure the deficiency disclosing an alleged method for watermarking.

Next, the combination of Rhoads and Quackenbush fails to disclose an LCS to handle legacy content, neither reference mentioning the term. In combination, it would appear that Quackenbush could be any of the so-called watermarking methods Rhoads claims are available for implementation within his scheme. It is not clear to the Applicants if the two references would be used in combination. Nevertheless, the combinations fail to disclose all of the elements of the claimed invention— Claim 14 depends from Claim 5, which depends from Independent Claim 3.

Last, there is no motivation to combine these two references in accordance with the claimed invention. Rhoads is apparently directed at

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

reconfiguring a watermark detector; Quackenbush is apparently directed at watermark insertion. Neither can handle legacy content with watermarked content in a seamless manner as disclosed by the instant invention[s]. Practically speaking, why rely on usage control, if you can obtain access to legacy content *sans* such usage control (e.g., music ripped from a compact disc)? As is understood by one of ordinary skill in the art, this is why the Applicants' invention[s] offers a significant advantage over the alleged security taught by Rhoads in combination with Quackenbush. The Examiner is using the instant invention as a roadmap to combine the references. Applicants therefore request the Examiner withdraw the Section 103 rejections of Claim 14 (which depends from Claim 5, which depends from Independent Claim 3).

Appl'n No. 10/049,101
Responsive Amendment dated July 3, 2006
Reply to Office Action of April 3, 2006

Conclusion

Applicants maintain that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with the Applicants, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

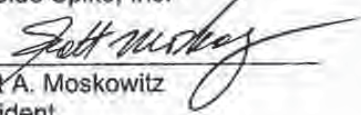
Date: July 3, 2006

By:



Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.



Scott A. Moskowitz
President



PTO/SB/17 (3/02)
 Approved for use through 07/31/2006. OMB 0627-0022
 U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE
 Under the Password Reduction Act of 1980, no password are required to respond to a collection of information unless it displays a valid OMB control number.

| | | | |
|---|--|--------------------------|--------------------|
| FEE TRANSMITTAL For FY 2006 | | Complete if Known | |
| | | Application Number: | 10/D49, 101 |
| <input checked="" type="checkbox"/> Applicant claims small entity status. (See 37 CFR 1.27) | | Filing Date: | July 23, 2005 |
| TOTAL AMOUNT OF PAYMENT (\$) 180.00 | | First Named Inventor: | Scott A. MOSKOWITZ |
| | | Examiner Name: | Nathan D. HAST |
| | | Art Unit: | 2136 |
| | | Attorney Docket No.: | B0408.0011 |

METHOD OF PAYMENT (check all that apply)

Check Credit Card Money Order None Other (please identify): _____
 Deposit Account Deposit Account Number: _____ Deposit Account Name: _____
 For the above identified deposit account, the Director is hereby authorized to: (check all that apply)
 Charge fee(s) indicated below Charge fee(s) indicated below, except for the filing fee
 Charge any additional fee(s) or underpayments of fee(s) Credit any overpayments
 under 37 CFR 1.16 and 1.17
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION (All the fees below are due upon filing or may be subject to a surcharge.)

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

| Application Type | FILING FEES | | SEARCH FEES | | EXAMINATION FEES | | Fees Paid (\$) |
|------------------|-------------|-----------------------|-------------|-----------------------|------------------|-----------------------|----------------|
| | Fee (\$) | Small Entity Fee (\$) | Fee (\$) | Small Entity Fee (\$) | Fee (\$) | Small Entity Fee (\$) | |
| Utility | 300 | 150 | 500 | 250 | 200 | 100 | |
| Design | 200 | 100 | 100 | 50 | 130 | 65 | |
| Plant | 200 | 100 | 300 | 150 | 160 | 80 | |
| Reissue | 100 | 150 | 500 | 250 | 600 | 300 | |
| Provisional | 200 | 100 | 0 | 0 | 0 | 0 | |

2. EXCESS CLAIM FEES

| Fee Description | Fee (\$) | Small Entity Fee (\$) | | | | |
|---|---------------------|-----------------------|----------------------|----------------------------------|-----------------|----------------------|
| Each claim over 20 (including Reissues) | 50 | 25 | | | | |
| Each independent claim over 3 (including Reissues) | 200 | 100 | | | | |
| Multiple dependent claims | 360 | 180 | | | | |
| Total Claims | Extra Claims | Fee (\$) | Fee Paid (\$) | Multiple Dependent Claims | Fee (\$) | Fee Paid (\$) |
| - 20 or 10 = | * | = | | | | |
| HP = highest number of total claims paid for, if greater than 20 | | | | | | |
| Independent Claims | Extra Claims | Fee (\$) | Fee Paid (\$) | | | |
| - 3 or HP = | * | = | | | | |
| HP = highest number of independent claims paid for, if greater than 3 | | | | | | |

3. APPLICATION SIZE FEE
 If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(g).

| Total Sheets | Extra Sheets | Number of each additional 50 or fraction thereof | Fee (\$) | Fee Paid (\$) |
|--------------|--------------|--|----------|---------------|
| - 100 = | / 50 = | (round up to a whole number) * | | |

4. OTHER FEE(S)

| Description | Fee (\$) | Fees Paid (\$) |
|--|--------------------------------------|----------------|
| Non-English Specification | \$130 fee (no small entity discount) | |
| Other (e.g., late filing surcharge) (05 after first Office Action) | | \$180.00 |

| | | |
|--------------------------------------|----------------------------------|--------------------------|
| SUBMITTED BY | | |
| Signature | Registration No. (Address/Agent) | Telephone (305) 856 9041 |
| Name (Print/Type) Scott A. MOSKOWITZ | | Date July 3, 2005 |

This collection of information is required by 37 CFR 1.126. The information is required to obtain or retain a benefit by the public which is to be (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. The collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. B028
Applicant : Scott A. MOSKOWITZ
Filed : July 22, 2002
TC/A.U. : 2131
Examiner : AVERY, Jeremiah L.

Docket No. : 80408.0011

MAIL STOP AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicants submit copies of the references listed on the attached SB08 Form for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicants state the following:

Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

07/07/2006 H02E1R1 00000040 10049101

01 FE:1805

160.00 0P

Page 1 of 5

In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of \$180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicants reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, Applicant wishes to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application:

EXAMINER'S INITIALS:

- ____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";
- ____ EPO Application No. 96919405.9, entitled "Steganographic Method and Device";
- ____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";
- ____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking";

- _____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" now U.S. Patent No. 6,598,162, July 22, 2003;
- _____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ Jap. App. No.2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";
- _____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";
- _____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- _____ U.S. Patent Application No. 09/789,711, filed Feb. 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- _____ U.S. Patent Application No.09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems";
- _____ U.S. Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions";
- _____ U.S. Patent Application No. 10/049,101, filed Feb. 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);
- _____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";
- _____ U.S. Patent Application No. 09/657,181, filed 09/07/00, entitled "Method And Device For Monitoring And Analyzing Signals"

- ____ U.S. Patent Application No. 10/805,484, filed 03/22/04, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed 09/29/00, which is a CIP of U.S. Patent Application No. 09/657,181);
- ____ U.S. Patent Application No. 09/956,262, filed 09/20/01, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects"
- ____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks";
- ____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation ...";
- ____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";
- ____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";
- ____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";
- ____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";
- ____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";
- ____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";
- ____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";
- ____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";
- ____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection and Detection...";
- ____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection and Detection...";
- ____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

Appl. No. 10/049,101
Information Disclosure Statement dated July 3, 2006

- ____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";
- ____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking".

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

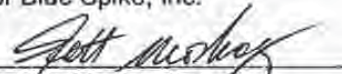
Date: July 3, 2006

By:



Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.



Scott A. Moskowitz
President

07-05-06

IFW 2136
\$



PTO/SB/21 (09-04)
Approved for use through 07/31/2006 QMS 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no actions are required in regard to a collection of information unless it displays a valid OMB control number.

| | | |
|--|------------------------|--------------------|
| TRANSMITTAL FORM <small>(To be used for all correspondence after initial filing)</small> | Application Number | 10049101 |
| | Filing Date | July 28, 2006 |
| | First Named Inventor | Scott A. MOSKOWITZ |
| | Art Unit | 2136 |
| | Examiner Name | Nathan D. HAST |
| Total Number of Pages in This Submission: | Attorney Docket Number | 004910011 |

| ENCLOSURES (Check all that apply) | | |
|---|---|---|
| <input checked="" type="checkbox"/> Fee Transmittal Form <input checked="" type="checkbox"/> Fee Attached <input checked="" type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input checked="" type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53 | <input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation <input type="checkbox"/> Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> GD Number of CD(s) <input type="checkbox"/> Landscape Table on CD | <input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below) |
| Remarks: | | |

| SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT | |
|--|---------------------------|
| Firm Name | |
| Signature | <i>Scott A. Moskowitz</i> |
| Printed name | Scott A. MOSKOWITZ |
| Date | July 3, 2006 |
| Reg. No. | |

| CERTIFICATE OF TRANSMISSION/MAILING | |
|---|------------------------|
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below: | |
| Signature | <i>Scott Moskowitz</i> |
| Typed or printed name | Scott A. MOSKOWITZ |
| Date | July 3, 2006 |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing this form, call 1-800-PTO-9199 and select option 2.

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number

10/049101

CLAIMS AS FILED - PART I

| | (Column 1) | (Column 2) |
|----------------------------------|--------------------------|--------------|
| TOTAL CLAIMS | | |
| FOR | NUMBER FILED | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS | 30 minus 20 = | 10 |
| INDEPENDENT CLAIMS | 7 minus 3 = | 4 |
| MULTIPLE DEPENDENT CLAIM PRESENT | <input type="checkbox"/> | |

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

7-3-06

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|--------------------------|
| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | 31 Minus 30 = | 1 |
| | Independent | 7 Minus 7 = | 0 |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | | | <input type="checkbox"/> |

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|--------------------------|
| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | Minus | |
| | Independent | Minus | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | | | <input type="checkbox"/> |

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|--------------------------|
| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| | Total | Minus | |
| | Independent | Minus | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | | | <input type="checkbox"/> |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SMALL ENTITY TYPE OR

OTHER THAN SMALL ENTITY

| RATE | FEE | OR | RATE | FEE |
|-----------|-----|----|-----------|-----|
| BASIC FEE | 370 | OR | BASIC FEE | |
| X\$9= | 990 | OR | X\$18= | |
| X42= | 168 | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL | 228 | OR | TOTAL | |

SMALL ENTITY OR OTHER THAN SMALL ENTITY

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$9= | 0 | OR | X\$18= | |
| X42= | 0 | OR | X84= | |
| +140= | 0 | OR | +280= | |
| TOTAL ADDIT. FEE | 0 | OR | TOTAL ADDIT. FEE | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$9= | | OR | X\$18= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$9= | | OR | X\$18= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

Best Available Copy



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22315-1450
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371 (c) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|------------------------|-----------------------|------------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 |

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

CONFIRMATION NO. 8028




Date Mailed: 08/02/2006

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/06/2006.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.


WUBALEM TSIGE
PTOSS (703) 305-3006

OFFICE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

| APPLICATION NUMBER | FILING OR 371 (c) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|------------------------|-----------------------|------------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 |

Wiley Rein & Fielding
 Intellectual Property Department
 1776 K Street NW
 Washington, DC 20006

CONFIRMATION NO. 8028




OC000000019864569

Date Mailed: 08/02/2006

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/06/2006.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).


 WUBALEM TSIGIE
 PTOSS (703) 305-3006

OFFICE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

9A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 | 8028 |

7590 10/12/2006
Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER

AVERY, JEREMIAH L

ART UNIT PAPER NUMBER

2131

DATE MAILED: 10/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Notice of Non-Compliant
Amendment (37 CFR 1.121)**

| | | |
|-----------------|---------------------|--|
| Application No. | Applicant(s) | |
| 10/049,101 | MOSKOWITZ, SCOTT A. | |
| Examiner | Art Unit | |
| Jeremiah Avery | 2131 | |

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —

The amendment document filed on 03 July 2006 is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT

- 1. Amendments to the specification:
 - A. Amended paragraph(s) do not include markings.
 - B. New paragraph(s) should not be underlined.
 - C. Other _____
- 2. Abstract:
 - A. Not presented on a separate sheet. 37 CFR 1.72.
 - B. Other _____
- 3. Amendments to the drawings:
 - A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
 - B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
 - C. Other _____
- 4. Amendments to the claims:
 - A. A complete listing of all of the claims is not present.
 - B. The listing of claims does not include the text of all pending claims (including withdrawn claims).
 - C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
 - D. The claims of this amendment paper have not been presented in ascending numerical order.
 - E. Other: See Continuation Sheet
- 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4).

For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance. If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.
2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a *Quayle* action. If any of above boxes 1. to 4. are checked, the correction required is only the **corrected section** of the non-compliant amendment in compliance with 37 CFR 1.121.

Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

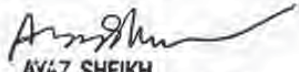
Failure to timely respond to this notice will result in:

- Abandonment** of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or
- Non-entry** of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable

Telephone No.

Continuation of 4(e) Other: According to MPEP chapter 714, paragraph C, section 2, this amendment is in a state of non-compliance due to claims 1, 3 and 17 using single brackets, instead of double brackets to indicate deleted subject matter. Further, several objections to several claims are also noted. Claim 12 is objected to because of the following informalities: grammatical errors. In line 7, "means receive a copy...", the word "to" should be inserted between the words "means" and "receive". Also, in line 9, "open watermark if it is...", the first "is" should be removed after "if". Appropriate correction is required. Claims 20 and 31 objected to because of the following informalities: grammatical error. In line 3, of each of these claims, "to an local content server" should be "to a local content server". Appropriate correction is required..


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100



10-23-06

TFW

2131

Approved for use through 03/31/2007. OMB 0551-0031 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Copyright Registration Act of 1976, this document is required to register to a collection of information unless it displays a valid OMB control number.

| | | |
|---|----------------------|------------------------------------|
| TRANSMITTAL FORM | Application Number | 10000101 |
| | Filing Date | July 23, 2002 |
| | First Named Inventor | Scott A. MOSKOWITZ |
| | Art Unit | 2131 |
| | Examiner Name | Jennifer L. AVERY |
| Total Number of Pages in This Submission: | | Attorney Docket Number: 00408 0011 |

| ENCLOSURES (Check all that apply) | | |
|---|---|---|
| <input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/Declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53 | <input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation <input type="checkbox"/> Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimers <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD | <input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): |
| Remarks <input checked="" type="checkbox"/> Reply to Notice of Non Compliant Amendment (37 CFR 1.121) | | |

| SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT | |
|--|--------------------|
| Firm Name | |
| Signature | |
| Printed name | Scott A. MOSKOWITZ |
| Date | October 20, 2006 |
| Reg. No. | |

| CERTIFICATE OF TRANSMISSION/MAILING | |
|---|--------------------|
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below: | |
| Signature | |
| Typed or printed name | SCOTT A. MOSKOWITZ |
| Date | October 20, 2006 |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is in the (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|------------|---|----------------------------|-----------------------|
| Appl. No. | : | 10/049,101 | Confirmation No. 8028 |
| Applicant | : | Scott A. Moskowitz, et al. | |
| Filed | : | July 23, 2002 | |
| TC/A.U. | : | 2131 | |
| Examiner | : | Jeremiah AVERY | |
| Docket No. | : | 80408.0011 | |

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT/SUPPLEMENT

In response to the Notice of Non-Compliant Amendment (37 CFR 1.121) dated October 12, 2006, Applicant provides the following corrections:

Corrected spelling and grammatical errors in claims 1, 3, 12, 17-22, 24 and 31 attached herein.

Amendments to the Claims:

Please amend the following: Claims 1, 3, 12, 17-22, 24 and 31 without prejudice or disclaimer. The amendments to claims 1, 3, 12, 17-22, 24 and 31 are being made to correct typographical errors and are not being made for reasons of patentability. This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:
 - a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;
 - b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved;
 - c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and
 - d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS; andsaid domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

2. (original) The LCS of claim 1 further comprising

Appl'n No. 10/049,101

Responsive Amendment dated Oct 20, 2006

Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content;

and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS,

and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.

3. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;

b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and

c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved;

d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU; and

e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS;

said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS, and if the digital content is not authorized for use, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content,

and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS[[.]] and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

4. (original) The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred.
5. (original) The system of claim 3, wherein said domain processor comprises:
 - means for obtaining an identification code from an SU connected to the LCS's interface;
 - an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS;
 - means for analyzing digital content received from an SU;
 - said system permitting the digital content to be stored in the LCS if
 - i) an analysis of the digital content received from the SU concludes that the content is authenticated, or
 - ii) an analysis of the digital content

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

received from the SU concludes that the content cannot be authenticated because no authentication data is embedded in the content, and said system preventing the digital content from being stored on the LCS if i) an analysis of the digital content received from the SU concludes that the content is unauthenticated.

6. (original) The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code of the LCS.
7. (original) The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated because there is no authentication data embedded in the content.
8. (original) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.
9. (original) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:
 - means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;
 - means to retrieve a copy of the requested content data set;

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

10. (original) The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11. (original) The system of claim 10, wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

wherein the LCS comprises:

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS;
and

means to deliver the watermarked content data set to the SU for its use.

12. (currently amended) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the content data set;

means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated;

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. (previously presented) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such that the data contains no additional information to permit authentication.

14. (original) The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS; and

means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

15. (original) The system of claim 5, wherein the LCS further comprises:

means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium,

16. (previously presented) A system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD);

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

a Local Content Server (LCS);
a communications network interconnecting the SECD to the LCS;
and
a Satellite Unit (SU) capable of interfacing with the LCS;
said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise secur[itz]ing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network to the LCS;
said LCS comprising: a domain processor; a first interface for connecting to a communications network; a second interface for communicating with the SU; a memory device for storing a plurality of data sets; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and
said SU being a portable module comprising: a memory for accepting secure digital content from a LCS, said digital content comprising data which can be authorized for use or which has been determined to be legacy content such that the data contains no additional information to permit authentication; an interface for communicating with the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the SU.

17. (currently amended) A ~~[[M]]~~method for creating a secure environment for digital content for a consumer, comprising the following steps:
sending a message indicating that a user is requesting a copy of a content data set;

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

retrieving a copy of the requested content data set;
embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;
embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;
transmitting the watermarked content data set to the requesting consumer via an electronic network;
receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;
extracting at least one watermark from the transmitted watermarked content data set; [and]
permitting use of the content data set if the LCS determines that use is authorized[[.]]; and
permitting use of the content data set at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

18. (currently amended) The [[M]]method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:
checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and
permitting the storage of the content data set in a storage unit for the LCS.

19. (currently amended) The [[M]]method of claim 17, further comprising:
connecting a Satellite Unit (SU) to an LCS,

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering the content data set to the SU for its use.

20. (currently amended) A ~~[[M]]~~method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to a~~[[n]]~~ local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the content data set to the SU for its use, said content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

21. (currently amended) The ~~[[M]]~~method of claim 20, further comprising:
embedding an open watermark into the content data to permit enhanced usage of the content data by the user.
22. (currently amended) The ~~[[M]]~~method of claim 21, further comprising:
embedding at least one additional watermark into the content data, said at least one additional watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis to provide information on the history of the content data's use.
23. (original) The method of claim 20, wherein the content data can be stored at a level of quality which is selected by a user.
24. (currently amended) A ~~[[M]]~~method for creating a secure environment for digital content for a consumer, comprising the following steps:
connecting a Satellite Unit (SU) to a~~[[n]]~~ local content server (LCS),
sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;
analyzing the message to confirm that the SU is authorized to use the LCS; and
retrieving a copy of the requested content data set;
assessing whether a secured connection exists between the LCS and the SU;
if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

delivering the watermarked content data set to the SU for its use,
said watermarked content data set delivered at a predetermined quality
level, said predetermined quality level having been set for legacy content if
the LCS determines that use is not authorized.

25. (original) The method of claim 24, further comprising:

embedding at least one robust open watermark into the copy of the
requested content data set before the requested content data is delivered
to the SU, said watermark indicating that the copy is authenticated.

26. (original) The method of claim 25, wherein the robust watermark is
embedded using any one of a plurality of embedding algorithms.

27. (original) The method of claim 24, further comprising:

embedding a watermark which includes a hash value from a one-
way hash function generated using the content data.

28. (original) The method of claim 25, wherein the robust watermark can be
periodically replaced with a new robust watermark generated using a new
algorithm with payload that is no greater than that utilized by the old robust
watermark.

29. (original) The method of claim 24, further comprising the step of:

embedding additional robust open watermarks into the copy of the
requested content data set before the requested content data is delivered
to the SU, using a new algorithm; and
re-saving the newly watermarked copy to the LCS.

30. (original) The method of claim 24, further comprising the step of:

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

31. (original) A [[M]]method for creating a secure environment for digital content for a consumer, comprising the following steps:
- connecting a Satellite Unit (SU) to a[[n]] local content server (LCS),
 - sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;
 - analyzing the message to confirm that the SU is authorized to use the LCS; and
 - receiving a copy of the content data set;
 - assessing whether the content data set is authenticated;
 - if the content data is unauthenticated, denying access to the LCS storage unit; and
 - if the content data is not capable of authentication, accepting the data at a predetermined quality level, said predetermined quality level having been set for legacy content.

Appl'n No. 10/049,101
Responsive Amendment dated Oct 20, 2006
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of Oct 12, 2006

Conclusion

Applicant maintains that this application is in condition for issuance, and such disposition is earnestly solicited.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

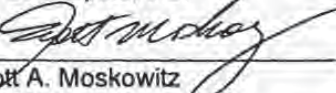
Date: October 20, 2006

By:



Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.



Scott A. Moskowitz
President

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or DocId Number

10/049101

CLAIMS AS FILED - PART I

| | (Column 1) | (Column 2) |
|----------------------------------|--------------------------|--------------|
| TOTAL CLAIMS | | |
| FOR | NUMBER FILED | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS | 30 minus 20 = | + 11 |
| INDEPENDENT CLAIMS | 7 minus 3 = | 4 |
| MULTIPLE DEPENDENT CLAIM PRESENT | <input type="checkbox"/> | |

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE OR OTHER THAN SMALL ENTITY

| RATE | FEE | OR | RATE | FEE |
|-----------|-----|----|-----------|-----|
| BASIC FEE | 370 | OR | BASIC FEE | |
| X\$ 9= | 92 | OR | X\$18= | |
| X\$2= | 168 | OR | X\$4= | |
| +140= | | OR | +250= | |
| TOTAL | 218 | OR | TOTAL | |

CLAIMS AS AMENDED - PART II

7-3-06

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | 31 | 30 | 0 |
| Independent | 7 | 7 | 0 |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

SMALL ENTITY OR OTHER THAN SMALL ENTITY

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | 0 | OR | X\$18= | |
| X\$2= | 0 | OR | X\$4= | |
| +140= | 0 | OR | +250= | |
| TOTAL ADDIT. FEE | 0 | OR | TOTAL ADDIT. FEE | |

10/20/06

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | | | |
| Independent | | | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X\$2= | | OR | X\$4= | |
| +140= | | OR | +250= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | | | |
| Independent | | | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X\$2= | | OR | X\$4= | |
| +140= | | OR | +250= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Best Available Copy



5
UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|--------------------|--|--------------------------------|------------------|
| 10/049,101 | 07/23/2002 | Scott A. Moskowitz | 80408.0011 | 8028 |
| | 7590 01/09/2007 | Scott A. Moskowitz #2505 16711 Collins Avenue Miami, FL 33160 | EXAMINER AVERY, JEREMIAH L. | |
| | | | ART UNIT 2131 | PAPER NUMBER |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|--|------------|---------------|
| 30 DAYS | 01/09/2007 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Notice of Non-Compliant
Amendment (37 CFR 1.121)**

| | | |
|-----------------|--------------------|--|
| Application No. | Applicant(s) | |
| 10/049 101 | MOSKOWITZ SCOTT A. | |
| Examiner | Art Unit | |
| Jeremiah Avery | 2131 | |

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —

The amendment document filed on 20 October 2006 is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT

- 1. Amendments to the specification:
 - A. Amended paragraph(s) do not include markings
 - B. New paragraph(s) should not be underlined
 - C. Other _____
- 2. Abstract:
 - A. Not presented on a separate sheet 37 CFR 1.72
 - B. Other _____
- 3. Amendments to the drawings:
 - A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d)
 - B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required
 - C. Other _____
- 4. Amendments to the claims:
 - A. A complete listing of all of the claims is not present.
 - B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
 - C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended)
 - D. The claims of this amendment paper have not been presented in ascending numerical order
 - E. Other: See Continuation Sheet
- 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4):

For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE

- Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance. If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.
- Applicant is given **one month, or thirty (30) days, whichever is longer**, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a *Quayle* action. If any of above boxes 1. to 4. are checked, the correction required is only the corrected section of the non-compliant amendment in compliance with 37 CFR 1.121.

Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

Failure to timely respond to this notice will result in:

- Abandonment** of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or
- Non-entry** of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable

Telephone No.



Continuation of 4(e) Other: Though the inclusion of double brackets overcomes the previous reasons for non-compliance, as stated in the Notice of Non-Compliance filed 10/12/06, new reasons for non-compliance exist. The previously submitted amendment, filed on 07/03/06, indicated additional limitations to the claims in the form of underlining said additional limitations. However, in the amendment filed on 10/20/06, these newly added limitations are not underlined. Newly submitted amendments serve to replace all prior versions of the claims, in the application. Please refer to MPEP 714, section c for further clarification. Thus, the Examiner recommends resubmitting the claims with the necessary underlining, along with the necessary double brackets..



2-8-07

THW 2131

PTO/SB/21 (09-06)
 Approved for use through 03/31/2007. OMB 0631-0031
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
 Under the Paperwork Reduction Act of 1995, no response is required to a collection of information unless it displays a valid OMB control number.

| | | |
|--|------------------------|--------------------|
| TRANSMITTAL FORM <small>(to be used for all correspondence after initial filing)</small> | Application Number | 10449,101 |
| | Filing Date | July 23, 2002 |
| | First Named Inventor | Scott A. MOSKOWITZ |
| | Art Unit | 3121 |
| | Examiner Name | Jeremiah AVERY |
| | Attorney Docket Number | 80488.0011 |
| Total Number of Pages in This Submission | | |

| ENCLOSURES (Check all that apply) | | |
|---|---|---|
| <input type="checkbox"/> Fee Transmittal Form | <input type="checkbox"/> Drawing(s) | <input type="checkbox"/> After Allowance Communication in TC |
| <input type="checkbox"/> Fee Attached | <input type="checkbox"/> Licensing-related Papers | <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences |
| <input checked="" type="checkbox"/> Amendment/Reply | <input type="checkbox"/> Petition | <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) |
| <input type="checkbox"/> After Final | <input type="checkbox"/> Petition to Convert to a Provisional Application | <input type="checkbox"/> Proprietary Information |
| <input type="checkbox"/> Affidavits/declarations(s) | <input type="checkbox"/> Power of Attorney, Revocation | <input type="checkbox"/> Status Letter |
| <input type="checkbox"/> Extension of Time Request | <input type="checkbox"/> Change of Correspondence Address | <input type="checkbox"/> Other Enclosure(s) (please identify below): |
| <input type="checkbox"/> Express Abandonment Request | <input type="checkbox"/> Terminal Disclaimer | |
| <input type="checkbox"/> Information Disclosure Statement | <input type="checkbox"/> Request for Refund | |
| <input type="checkbox"/> Certified Copy of Priority Document(s) | <input type="checkbox"/> CD, Number of CD(s) | |
| <input type="checkbox"/> Reply to Missing Parts/Incomplete Application | <input type="checkbox"/> Landscape Table on CD | |
| <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53 | Remarks 37 CFR 1.121 | |

| SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT | |
|--|--------------------|
| Firm Name | |
| Signature | |
| Printed name | Scott A. MOSKOWITZ |
| Date | February 7, 2007 |
| Reg. No. | |

| CERTIFICATE OF TRANSMISSION/MAILING | | | |
|---|--------------------|------|------------------|
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below: | | | |
| Signature | | | |
| Typed or printed name | Scott A. MOSKOWITZ | Date | February 7, 2007 |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Appl'n No. 10/049,101
Responsive Amendment dated February 7, 2007
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of January 9, 2007



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|------------|---|----------------------------|-----------------------|
| Appl. No. | : | 10/049,101 | Confirmation No. 8028 |
| Applicant | : | Scott A. Moskowitz, et al. | |
| Filed | : | July 23, 2002 | |
| TC/A.U. | : | 2131 | |
| Examiner | : | Jeremiah AVERY | |
| Docket No. | : | 80408.0011 | |

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT/SUPPLEMENT

In response to the Notice of Non-Compliant Amendment (37 CFR 1.121) dated January 9, 2007, Applicant provides the following corrections:

Corrected bracketing and underlining in claims

Amendments to the Claims:

Please amend the following: Claims **1, 3, 12, 13, 16-22, 24 and 31** without prejudice or disclaimer. The amendments to claims **12, 13, 18, 19, 21, 22 and 31** are being made to correct typographical and spelling errors and are not being made for reasons of patentability. This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;

b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved;

c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and

d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and

said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS[[.]] and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

2. (original) The LCS of claim 1 further comprising

e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content;

and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS,

and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.

3. (currently amended) A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;

b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and

c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved;

d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU; and

e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS;

said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS, and if the digital content is not authorized for use, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content,

and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS, and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

4. (original) The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred

5. (original) The system of claim 3, wherein said domain processor comprises:
means for obtaining an identification code from an SU connected to the LCS's interface;

an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS;

means for analyzing digital content received from an SU;

said system permitting the digital content to be stored in the LCS if
i) an analysis of the digital content received from the SU concludes that
the content is authenticated, or ii) an analysis of the digital content
received from the SU concludes that the content cannot be authenticated
because no authentication data is embedded in the content, and

said system preventing the digital content from being stored on the
LCS if i) an analysis of the digital content received from the SU concludes
that the content is unauthenticated.

6. (original) The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code of the LCS.
7. (original) The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated because there is no authentication data embedded in the content.
8. (original) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.
9. (original) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:
means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

10. (original) The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11. (original) The system of claim 10, wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

12. (currently amended) The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means receive a copy of the content data set;

means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if [[is]] it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated;

means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. (currently amended) The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such that the data contains no additional information to permit authentication.

14. (original) The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS; and

means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

15. (original) The system of claim 5, wherein the LCS further comprises:

means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium

16. (currently amended) A system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD);

a Local Content Server (LCS);

a communications network interconnecting the SECD to the LCS;

and

a Satellite Unit (SU) capable of interfacing with the LCS;

said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise secur[[iliz]]ing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network to the LCS;

said LCS comprising: a domain processor; a first interface for connecting to a communications network; a second interface for communicating with the SU; a memory device for storing a plurality of data sets; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and

said SU being a portable module comprising: a memory for accepting secure digital content from a LCS, said digital content comprising data which can be authorized for use or which has been determined to be legacy content such that the data contains no additional information to permit authentication; an interface for communicating with the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the SU.

17. (currently amended) A [[M]]method for creating a secure environment for digital content for a consumer, comprising the following steps:

sending a message indicating that a user is requesting a copy of a content data set;

retrieving a copy of the requested content data set;

embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;

transmitting the watermarked content data set to the requesting consumer via an electronic network;

receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;

extracting at least one watermark from the transmitted watermarked content data set; [[and]]

permitting use of the content data set if the LCS determines that use is authorized [[]]; and

permitting use of the content data set at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

18. (currently amended) The [[M]]method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

permitting the storage of the content data set in a storage unit for the LCS.

19. (currently amended) The [[M]]method of claim 17, further comprising:
connecting a Satellite Unit (SU) to an LCS,

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering the content data set to the SU for its use.

20. (currently amended) A ~~[[M]]~~method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to a~~[[n]]~~ local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the content data set to the SU for its use, said content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized.

Appl'n No. 10/049,101

Responsive Amendment dated February 7, 2007

Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of January 9, 2007

21. (currently amended) The [[M]]method of claim 20, further comprising:
embedding an open watermark into the content data to permit enhanced usage of the content data by the user.
22. (currently amended) The [[M]]method of claim 21, further comprising:
embedding at least one additional watermark into the content data, said at least one additional watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis to provide information on the history of the content data's use.
23. (original) The method of claim 20, wherein the content data can be stored at a level of quality which is selected by a user.
24. (currently amended) A [[M]]method for creating a secure environment for digital content for a consumer, comprising the following steps:
connecting a Satellite Unit (SU) to a^{[[n]]} local content server (LCS),
sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;
analyzing the message to confirm that the SU is authorized to use the LCS; and
retrieving a copy of the requested content data set;
assessing whether a secured connection exists between the LCS and the SU;
if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the watermarked content data set to the SU for its use,
said watermarked content data set delivered at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized

25. (original) The method of claim 24, further comprising:
embedding at least one robust open watermark into the copy of the requested content data set before the requested content data is delivered to the SU, said watermark indicating that the copy is authenticated.
26. (original) The method of claim 25, wherein the robust watermark is embedded using any one of a plurality of embedding algorithms.
- [[26.]] 27. (original) The method of claim 24, further comprising:
embedding a watermark which includes a hash value from a one-way hash function generated using the content data.
- [[27.]] 28. (original) The method of claim 25, wherein the robust watermark can be periodically replaced with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.
- [[28.]] 29. (original) The method of claim 24, further comprising the step of:
embedding additional robust open watermarks into the copy of the requested content data set before the requested content data is delivered to the SU, using a new algorithm; and
re-saving the newly watermarked copy to the LCS.
- [[29.]] 30. (original) The method of claim 24, further comprising the step of:

Appl'n No. 10/049,101

Responsive Amendment dated February 7, 2007

Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of January 9, 2007

saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

[[30.]] 31. (original) A [[M]]method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) to a[[n]] local content server (LCS),

sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

receiving a copy of the content data set;

assessing whether the content data set is authenticated;

if the content data is unauthenticated, denying access to the LCS storage unit; and

if the content data is not capable of authentication, accepting the data at a predetermined quality level, said predetermined quality level having been set for legacy content.

Appl'n No. 10/049,101
Responsive Amendment dated February 7, 2007
Reply to Notice of Non-Compliant Amendment 37 CFR 1.121 of January 9, 2007

Conclusion


Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with the Applicant, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

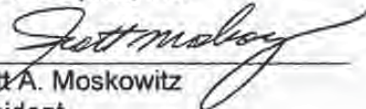
Date: February 7, 2007

By:



Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.



Scott A. Moskowitz
President

PATENT APPLICATION - FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number

10/049101

CLAIMS AS FILED - PART I

| | (Column 1) | (Column 2) |
|----------------------------------|--------------------------|--------------|
| TOTAL CLAIMS | | |
| FOR | NUMBER FILED | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS | 306 minus 20 = | + 11 |
| INDEPENDENT CLAIMS | 7 minus 3 = | 4 |
| MULTIPLE DEPENDENT CLAIM PRESENT | <input type="checkbox"/> | |

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

7-3-06

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | 31 | 30 | 0 |
| Independent | 7 | 7 | 0 |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

2-7-07

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | 31 | 31 | |
| Independent | 7 | 7 | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

AMENDMENT C

| | (Column 1) | (Column 2) | (Column 3) |
|--|----------------------------------|------------------------------------|---------------|
| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | | | |
| Independent | | | |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM | <input type="checkbox"/> | | |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" in THIS SPACE is less than 20, enter "20."
 *** If the "Highest Number Previously Paid For" in THIS SPACE is less than 5, enter "5."
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 2.

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

| RATE | FEE | OR | RATE | FEE |
|-----------|-----|----|-----------|-----|
| BASIC FEE | 370 | OR | BASIC FEE | |
| X3 S= | 928 | OR | X31B= | |
| X42= | 168 | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL | 168 | OR | TOTAL | |

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X3 9= | 0 | OR | X31B= | |
| X42= | 0 | OR | X84= | |
| +140= | 0 | OR | +280= | |
| TOTAL ADJUT. FEE | 0 | OR | TOTAL ADJUT. FEE | |

RATE

ADDITIONAL FEE

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X3 9= | | OR | X31B= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADJUT. FEE | | OR | TOTAL ADJUT. FEE | |

RATE

ADDITIONAL FEE

| RATE | ADDITIONAL FEE | OR | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X3 9= | | OR | X31B= | |
| X42= | | OR | X84= | |
| +140= | | OR | +280= | |
| TOTAL ADJUT. FEE | | OR | TOTAL ADJUT. FEE | |

Best Available Copy



04-18-07

TFW

2/31

PTO/SB/21 (09-00)

Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1996, no person is required to respond to a collection of information unless it displays a valid OMB control number.

| | | |
|--|------------------------|-----------------|
| TRANSMITTAL FORM <small>(to be used for all correspondence after initial filing)</small> | Application Number | 10,049 (01) |
| | Filing Date | July 29, 2009 |
| | First Named Inventor | Scott MOSKOWITZ |
| | Art Unit | 2131 |
| | Examiner Name | Jonathan AVERY |
| | Attorney Docket Number | 00486 DO11 |
| Total Number of Pages in This Submission | | |

| ENCLOSURES (Check all that apply) | | |
|---|--|--|
| <input checked="" type="checkbox"/> Fee Transmittal Form <input checked="" type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavit/Declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input checked="" type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53 | <input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation/Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD | <input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below): |
| Remarks: | | |

| SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT | | | |
|--|-----------------|----------|--|
| Firm Name | | | |
| Signature | | | |
| Printed name | Scott MOSKOWITZ | | |
| Date | April 17, 2007 | Reg. No. | |

| CERTIFICATE OF TRANSMISSION/MAILING | | | |
|---|-----------------|------|----------------|
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below: | | | |
| Signature | | | |
| Typed or printed name | Scott MOSKOWITZ | Date | April 17, 2007 |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the entity which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to average 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Approved for use through 02/28/2007 OMB No. 1-0532
 U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE
 Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 1/01/2007.
 Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL For FY 2007

Applicant claims small entity status. See 37 CFR 1.27.

| TOTAL AMOUNT OF PAYMENT | | (\$) | | \$180.00 | |
|-------------------------|--|-----------------|--|----------|--|
| Application Number | | 10/049,101 | | | |
| Filing Date | | July 23, 2007 | | | |
| First Named Inventor | | Scott MOSKOWITZ | | | |
| Examiner Name | | Jeremiah AVERY | | | |
| Art. Unit | | 2131 | | | |
| Attorney/Agent No. | | 80-408 0011 | | | |

METHOD OF PAYMENT (check all that apply)

Check Credit Card Money Order None Other (please identify): _____

Deposit Account Deposit Account Number: _____ Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

Charge fee(s) indicated below Charge fee(s) indicated below, except for the filing fee

Charge any additional fee(s) or underpayments of fee(s) Credit any overpayments under 37 CFR 1.16 and 1.17

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2026.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

| Application Type | FILING FEES | | SEARCH FEES | | EXAMINATION FEES | | Fees Paid (\$) |
|------------------|-------------|-----------------------|-------------|-----------------------|------------------|-----------------------|----------------|
| | Fee (\$) | Small Entity Fee (\$) | Fee (\$) | Small Entity Fee (\$) | Fee (\$) | Small Entity Fee (\$) | |
| Utility | 300 | 150 | 500 | 250 | 200 | 100 | _____ |
| Design | 200 | 100 | 100 | 50 | 130 | 65 | _____ |
| Plant | 200 | 100 | 300 | 150 | 160 | 80 | _____ |
| Reissue | 300 | 150 | 500 | 250 | 600 | 300 | _____ |
| Provisional | 200 | 100 | 0 | 0 | 0 | 0 | _____ |

2. EXCESS CLAIM FEES

| Fee Description | Fee (\$) | Small Entity Fee (\$) |
|--|----------|-----------------------|
| Each claim over 20 (including Reissues) | 30 | 25 |
| Each independent claim over 3 (including Reissues) | 200 | 100 |
| Multiple dependent claims | 350 | 180 |

Total Claims _____ **Extra Claims** _____ **Fee (\$)** _____ **Fee Paid (\$)** _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ **Extra Claims** _____ **Fee (\$)** _____ **Fee Paid (\$)** _____

IP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specifications and drawings exceed 100 sheets of paper (including electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application (see fee table) \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(a).

Total Sheets _____ **Extra Sheets** _____ **Number of each additional 50 or fraction thereof** _____ **Fee (\$)** _____ **Fee Paid (\$)** _____

_____ : 100 = _____ : 50 = _____ (round up to a whole number) * _____ = _____

4. OTHER FEE(S)

Non-English Specification: \$150 fee (no small entity discount) **Fees Paid (\$)**

Other (e.g., late filing surcharge): Information Disclosure Statement \$180.00

SUBMITTED BY

| | | | |
|-------------------|-----------------|--------------------------------|------------------------|
| Signature | | Registration No. (Atomw/Agent) | Telephone 305 956 9041 |
| Name (Print Type) | Scott MOSKOWITZ | | Date April 17, 2007 |

This collection of information is required by 37 CFR 1.136. The information is required to issue or retain a patent by the public which is in file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is assumed to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-0199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/049,101 Confirmation No. 8028
Applicant : Scott A. MOSKOWITZ et al.
Filed : July 23, 2002
TC/A.U. : 2131
Examiner : Jeremiah AVERY

Docket No. : 80408.0011

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicants submit copies of the references listed on the attached SB08 Form for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicants state the following.

Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.55(c) more than three months prior to the filing of this Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of \$180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicants reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, Applicant wishes to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application:

EXAMINER'S INITIALS

- _____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";
- _____ EPO Application No. 96919405.9, entitled "Steganographic Method and Device";
- _____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device";
- _____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

- ____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking";
- ____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking";
- ____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking";
- ____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation";
- ____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";
- ____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ Jap. App. No 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- ____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";
- ____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- ____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- ____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- ____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

- _____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";
- _____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";
- _____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems";
- _____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems";
- _____ U.S. Patent Application No. 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions";
- _____ U.S. Patent Application No. 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions";
- _____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);
- _____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";
- _____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals";
- _____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181);
- _____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";
- _____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";
- _____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks";

- _____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks";
- _____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";
- _____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";
- _____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";
- _____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";
- _____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";
- _____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";
- _____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";
- _____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";
- _____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";
- _____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";
- _____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";
- _____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";
- _____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

- _____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";
- _____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";
- _____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";
- _____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";
- _____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";
- _____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";
- _____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";
- _____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";
- _____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";
- _____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects"

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: April 17, 2007

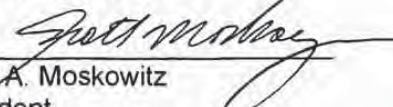
By.

Appl. No. 10/049,101
Information Disclosure Statement dated April 17, 2007



Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.



Scott A. Moskowitz
President



Approved for use through 03/31/2007. OMB No. 16031
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
 Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number.

| | | |
|---|--------------------------|---------------------------|
| Substitute for Form PTO/SF 100 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary) | Complete if Known | |
| | Application Number | 10/049,101 |
| | Filing Date | July 23, 2002 |
| | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | Art Unit | 2131 |
| | Examiner Name | Jeremiah AVERY |
| Sheet 1 of 6 | Attorney Docket Number | 80408.0011 |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|-----------------------|---|----------------|
| Examiner Initials* | Cite No. ¹ | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T ² |
| | | Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996 | |
| | | Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 46, 1997 | |
| | | Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p.207 | |
| | | Brealy, et al., Principles of Corporate Finance, "Appendix A-Using Option Valuation Models", 1984, pp. 448-449 | |
| | | Copeland, et al., Real Options: A Practitioner's Guide, 2001 pp. 106-107, 201-202, 204-208. | |
| | | Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995. http://www.press.ymich.edu/ian/works/SarkAsses.html on | |
| | | Crawford, D.W. "Pricing Network Usage: A Market for Bandwidth of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995. http://www.press.ymich.edu/ian/works/CrawMarket.html on March | |
| | | LOW, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citeseer.nj.nec.com/366503.html | |
| | | Caronni, Germano, "Assuring Ownership Rights for Digital Images" published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed.), Mewing Publishing Company, Germany, 1995 | |
| | | Zhao, Jian, "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the European conf. on Multimedia Applications, Services & Techniques Louvain-La-Neuve, Belgium, May 1996 | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reviewed considered, whether oral opinion is in conformance with MPEP 609. Drawings through plate # not in conformance and not considered. Include copy of this form with oral communication to applicant.
¹ Applicant's unique citation designation number (optional). ² Applicant's file place a check mark here if English language Translation is attached.
 This collection of information is required by 37 CFR 1.58. The information is required to obtain or retain a benefit by the public which is to be filed by the USPTO to process an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22312-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22312-1450.

If you need assistance in completing this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | | | |
|--|---|--------------------------|---------------------------|
| Substitutable for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary) | | Complete if Known | |
| | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| | | Attorney Docket Number | 80408.0011 |
| Sheet | 2 | of | 6 |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|----------|--|---|
| Examiner (initials) | Cite No. | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate) title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T |
| | | Gruhl, Daniel et al., Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science, Cambridge, England (May/June 1996) | |
| | | Oomen, A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J. Audio Eng. Soc., Vol. 43, No. 1/2, pp. 23-28 (1995). | |
| | | Ten Kate, W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng. Soc., Vol. 40, No. 5, pp. 376-383 (1992) | |
| | | Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993) | |
| | | Sklar, Bernard, Digital Communications, pp. 601-603 (1988) | |
| | | Jayant, N. S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs, NJ, pp. 486-509 (1984) | |
| | | Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., Vol. 2420, pp. 164-173, 1995. | |
| | | Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995. | |
| | | Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997 | |
| | | Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994. | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw one through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant to place a check mark here if English language Translation is attached.
 This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to be (and by the USPTO in process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-2199 (1-800-786-9199) and select option 3

| | | | |
|--|-------------|--------------------------|---------------------------|
| Subject to the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number. | | Complete if Known | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary) | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 Jeremiah AVERY |
| | | Examiner Name | 80408,0011 |
| Sheet <u>3</u> | of <u>6</u> | Attorney Docket Number | |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|-----------|---|----|
| Examiner Initials* | Cite No.† | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, etc.), symposium, catalog, etc., date, page(s), volume-issue number(s), publisher, city and/or country where published. | TS |
| | | ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990) | |
| | | van Schyndel, et al. A digital Watermark, IEEE Int'l Computer Processing Conference, Austin, TX, Nov 13-16, 1994, pp. 86-90 | |
| | | Smith, et al. Modulation and Information Hiding in Images, Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-June 1, 1996, pp. 207-227 | |
| | | Kutter, Martin et al., Digital Signature of Color Images Using Amplitude Modulation, SPIE-E197, vol. 3022, pp. 518-527 | |
| | | Puata, Joan et al., Using Fractal Compression Scheme to Embed a Digital Signature into an Image, SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118 | |
| | | Swanson, Mitchell D., et al., Transparent Robust Image Watermarking, Proc. of the 1996 IEEE Int'l Conf. on Image Processing, Vol. 111, 1996, pp. 211-214 | |
| | | Swanson, Mitchell D., et al. Robust Data Hiding for Images, 7th IEEE Digital Signal Processing Workshop, Leon, Norway, Sept. 1-4, 1996, pp. 37-40 | |
| | | Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, Proceeding of the Know Right '95 Conference, pp. 242-251 | |
| | | Koch, E., et al. Towards Robust and Hidden Image Copyright Labeling, 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun 1995, Naxos Marmaras, pp. 4 | |
| | | Van Schyndel, et al., Towards a Robust Digital Watermark, Second Asian Image Processing Conference, Dec. 6-8, 1995, Singapore, Vol. 2, pp. 504-508 | |

| | | | |
|--------------------|--|-----------------|--|
| Examiner Signature | | Date Considered | |
|--------------------|--|-----------------|--|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 † Applicant's unique citation designation number (optional). ‡ Applicant is to place a check mark here if English language translation is attached.
 This collection of information is required by 37 CFR 1.85. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.8. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form (and/or suggestions for reducing this burden), should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing this form, call 1-800-PTO-9199 (1-800-785-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it carries a valid OMB control number.

| | | | |
|---|---|--------------------------|---------------------------|
| Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary) | | <i>Complete if Known</i> | |
| | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| Sheet | 4 | of | 6 |
| | | Attorney Docket Number | |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|-----------|---|----------------|
| Examiner Initials* | Cite No.† | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T ² |
| | | Tirkel, A.Z., A Two-Dimensional Digital Watermark, DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8, 1995, pp. 7 | |
| | | Tirkel, A.Z., Image Watermarking-A Spread Spectrum Application, ISSSTA 96, Sept. 96, Mainz, German, pp. 6. | |
| | | O'Ruanaidh, et al., Watermarking Digital Images for Copyright Protection, IEEE Proceedings, Vol. 143, No. 4, Aug. 96, pp. 250-256 | |
| | | Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institute, Technical Report 95-10, pp. 33 | |
| | | Kahn, D., The Code Breakers, The MacMillan Company, 1969, pp. xiii, 81-83, 513, 516, 522-526, 863. | |
| | | Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480. | |
| | | Dept. of Electrical Engineering, Del Ft University of Technology, Del Ft The Netherlands, Cr C, Langelaar et al., Copy Protection for Multimedia Data based on Labeling Techniques, July 1996, 9 pp. | |
| | | F. Hartung, et al., Digital Watermarking of Raw and Compressed Video, SPIE Vol. 2952, pp. 205-213. | |
| | | Craver, et al., Can Invisible Watermarks Resolve Rightful Ownerships? IBM Research Report, RC 20509 (July 25, 1996) 21 pp. | |
| | | Press, et al., Numerical Recipes In C, Cambridge Univ. Press, 1988, pp. 398-417. | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if response considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 † Applicant's unique citation designation number (optional). ‡ Applicant is to place a check mark next to English language translation if attached.
 This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to be (and) by the USPTO in process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including searching, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22315-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22315-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-785-9199) and select option 1.

Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number.

| | | | |
|--|---|--------------------------|--------------------------|
| Substitute for form 1449PTO | | Complete if Known | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| | | Attorney Docket Number | 80408.0011 |
| Sheet | 5 | of | 6 |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|----------|---|---|
| Examiner Initials* | Cite No. | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | |
| | | Pohlmann, Ken C., Principles of Digital Audio, 3rd Ed., 1995, pp. 32-37, 40-48, 138, 147-149, 332, 333, 364, 499-501, 508-509, 564-571 | 7 |
| | | Pohlmann, Ken C., Principles of Digital Audio, 2nd Ed., 1991, pp. 1-9, 19-25, 30-33, 41-48, 54-57, 86-107, 375-387. | |
| | | Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc., New York, 1994, pp. 68, 69, 387-392, 1-57, 273-275, 321-324. | |
| | | Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, June 17-23 1996 Hiroshima, Japan 0-8186-7436-9/96 pp. 473-480. | |
| | | Johnson, et al., Transform Permuted Watermarking for Copyright Protection of Digital Video, IEEE Globecom 1998, Nov 8-12, 1998, New York, New York, Vol. 2, 1998, pp. 684-689 (ISBN 0-7803-4985-7) | |
| | | Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, May 7 1996, pp. 1-18. | |
| | | Bender, et al., Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos 3 & 4, 1996, pp. 313-336. | |
| | | Moskowitz, Bandwidth as Currency, IEEE Multimedia, Jan-Mar 2003, pp. 14-21. | |
| | | Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction-Digital Rights Management" pp. 3-22 | |
| | | Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, April 27, 2001, pp. 1-18 | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 809. Draw line-through circles if not in conformance and not considered. Include copy of this form with oral communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to assess or verify a benefit by the public which is to be paid by the USPTO to promote an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| | | | |
|---|---|--------------------------|---------------------------|
| Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary) | | <i>Complete if Known</i> | |
| | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | Jeremiah AVERY |
| | | Examiner Name | 80408.0011 |
| Sheet | 6 | of | 6 |
| | | Attorney Docket Number | |

| NON PATENT LITERATURE DOCUMENTS | | | |
|---------------------------------|-----------|---|----------------|
| Examiner Initials* | Cite No.† | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. | T ² |
| | | Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in <i>Electronic Commerce and Web Technologies Proceedings (ECWEB)</i> | |
| | | Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking Trade-offs of Security, Robustness and Quality", <i>IEEE Computer Society Proceedings of ITCC 2002 April 10 2002 pp. 80-84</i> | |
| | | Lemina, et al. "Secure Watermark Embedding through Partial Encryption", <i>International Workshop on Digital Watermarking ("IWDW" 2006) Springer Lecture Notes in Computer Science 2006 (to appear) 13</i> | |
| | | Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Cryptography Research, Inc. 2002-2003, 14 pages. | |
| | | Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", <i>Digest of Papers of the Computer Society Computer Conference (Spring) 5 March 1995 pp. 20-25 vol. CONF40</i> | |
| | | Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", <i>Computer Networks and ISDN Systems, 30 Sept 1998 pp. 1501-1510 Vol. 30 No. 16-18, NL, North Holland</i> | |
| | | Konrad, K. et al., "Trust and Electronic Commerce-more than a technical problem," <i>Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems 19-22 October 1999 pp. 360-365 Lausanne</i> | |
| | | Kini, a. et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", <i>Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216) 6-9 January 1998 pp. 51-61, Los</i> | |
| | | Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", <i>Standard View, Sept. 1997, pp. 118-124, vol. 5 No. 3, ACM, USA</i> | |
| | | Hartung, et al. "Multimedia Watermarking Techniques", <i>Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp. 1079-1107 July 1999, Vol. 87, No. 7, IEEE</i> | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 508. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 † Applicant's unique citation designation number (optional). ‡ Applicant is to place a check mark here if English language Translation is attached.
 This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and) by the USPTO (a process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199, 7-0001-780-2199 and select option 2



Approved for use through 03/31/2007 OMB 0651-0021
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Freedom of Information Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449PTO

Complete if Known

| | | | | | | | | | | | | | |
|---|--|--------------------|------------|-------------|---------------|----------------------|---------------------------|----------|------|---------------|----------------|------------------------|------------|
| <p style="text-align: center;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)</p> | <table border="1" style="width: 100%;"> <tr> <td>Application Number</td> <td>10/049,101</td> </tr> <tr> <td>Filing Date</td> <td>July 23, 2002</td> </tr> <tr> <td>First Named Inventor</td> <td>Scott A. MOSKOWITZ et al.</td> </tr> <tr> <td>Air Unit</td> <td>2131</td> </tr> <tr> <td>Examiner Name</td> <td>Jeremiah AVERY</td> </tr> <tr> <td>Attorney Docket Number</td> <td>80408.0011</td> </tr> </table> | Application Number | 10/049,101 | Filing Date | July 23, 2002 | First Named Inventor | Scott A. MOSKOWITZ et al. | Air Unit | 2131 | Examiner Name | Jeremiah AVERY | Attorney Docket Number | 80408.0011 |
| Application Number | 10/049,101 | | | | | | | | | | | | |
| Filing Date | July 23, 2002 | | | | | | | | | | | | |
| First Named Inventor | Scott A. MOSKOWITZ et al. | | | | | | | | | | | | |
| Air Unit | 2131 | | | | | | | | | | | | |
| Examiner Name | Jeremiah AVERY | | | | | | | | | | | | |
| Attorney Docket Number | 80408.0011 | | | | | | | | | | | | |

Sheet 1 of 1

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|---|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number and Date ² (if known) | | | |
| | | US-4,939,515 | 07/03/1990 | Edison | |
| | | US-5,161,210 | 11/03/1992 | Druyvesteyn, et al. | |
| | | US-5,450,490 | 09/12/1995 | Jensen, et al. | |
| | | US-5,530,751 | 06/25/1998 | Morris | |
| | | US-5,579,124 | 11/26/1996 | Ajaja, et al. | |
| | | US-5,721,788 | 02/24/1998 | Powell, et al. | |
| | | US-5,828,325 | 10/27/1998 | Wolose Wicz, et al. | |
| | | US-5,912,972 | 06/15/1999 | Barton | |
| | | US-5,930,377 | 07/27/1999 | Powell, et al. | |
| | | US-5,583,488 | 12/10/1996 | Sala, et al. | |
| | | US-5,748,783 | 05/06/1998 | Rhoads | |
| | | US-6,330,672 | 12/11/2001 | Shui | |
| | | US-5,243,423 | 09/07/1993 | Deusan, et al. | |
| | | US-5,819,735 | 06/07/1994 | Freuss, et al. | |
| | | US-5,113,497 | 05/12/1992 | Best, et al. | |
| | | US-4,876,817 | 10/24/1989 | Best, et al. | |
| | | US-5,379,345 | 01/03/1995 | Greenberg | |
| | | US-5,646,997 | 07/08/1997 | Barton | |
| | | US-4,672,605 | 06/09/1987 | Husig, et al. | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|----------|---|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Country, Code ¹ , Number ¹ and Code ² (if known) | | | |
| | | European Patent No. EP0585947A1 | 10/20/1993 | Kiucarna, Juha | |
| | | WO 95/14289 | 05/26/1995 | Rhoads, Geoffrey | |
| | | European Patent No. 0581317A2 | 02/02/1994 | Powell, Robert et al. | |
| | | European Patent No. 0372601A1 | 06/13/1990 | Druyvesteyn, Wm. et al. | |
| | | W098/37513 | 08/27/1998 | Biggar, Michael et al. | |
| | | European Patent No. 0651554A | 05/03/1995 | Eastman Kodak Co. | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 809. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kiud's Code of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by its two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.15 if possible. ⁶ Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is in the (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 102 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| | | | |
|--|------------|--------------------------|---------------------------|
| Substitute for form 1449/PTO | | Complete if Known | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| Attorney Docket Number | BO408.0011 | | |
| Sheet <u>2</u> of <u>12</u> | | | |

U. S. PATENT DOCUMENTS

| Examiner Initials* | Cite No.† | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|--------------------|-----------|------------------------|--------------------------------|---|---|
| | | Number-Kind Code‡/¶/§/ | | | |
| | | US-4,748,688 | 05/31/1988 | Bhamir, et al. | |
| | | US-4,789,928 | 12/06/1988 | Fujisaki | |
| | | US-4,908,873 | 03/13/1990 | Phibbert, et al. | |
| | | US-4,980,782 | 12/25/1990 | Sinkel | |
| | | US-5,073,925 | 12/17/1991 | Nagata, et al. | |
| | | US-5,243,515 | 09/07/1993 | Lee | |
| | | US-5,287,407 | 02/15/1994 | Holmes | |
| | | US-5,428,606 | 06/27/1995 | Moskowitz | |
| | | US-5,365,586 | 11/15/1994 | Indeck, et al. | |
| | | US-5,394,324 | 02/28/1995 | Clearwater | |
| | | US-5,408,505 | 04/18/1995 | Indeck, et al. | |
| | | US-5,412,718 | 05/02/1995 | Narasimhan, et al. | |
| | | US-5,487,168 | 01/23/1996 | Serner, et al. | |
| | | US-5,493,677 | 02/20/1996 | Balogh, et al. | |
| | | US-5,530,759 | 05/25/1996 | Braudaway, et al. | |
| | | US-5,608,609 | 02/25/1997 | Hooser, et al. | |
| | | US-5,613,004 | 03/18/1997 | Cooperman, et al. | |
| | | US-5,617,119 | 04/01/1997 | Briggs, et al. | |
| | | US- | | | |

FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No.† | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | T [§] |
|--------------------|-----------|---|--------------------------------|---|---|----------------|
| | | Country Code [¶] Number and Code [§] (if known) | | | | |
| | | WO 99/62044 | 12/02/1999 | Handa, Theodore et al. | | |
| | | WIPO 96/29795 | 09/26/1996 | Micali | | |
| | | WIPO 97/24833 | 07/10/1997 | Micali | | |
| | | EP 0649261 | 04/19/1995 | Enari | | |
| | | NL 100523 | 09/1998 | | | |

| | |
|--------------------|----------------|
| Examiner Signature | Date Completed |
|--------------------|----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in compliance with MPEP 606. Draw line through citation if not in compliance and not considered. Include copy of this form with next communication to applicant. †Applicant's unique citation designation number (optional). ‡See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 801.04. †Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). † For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. †Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. †Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.57 and 1.58. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the summarized application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-5199 (1-800-726-9199) and select option 3.

| | | | | | | | | | | | | | |
|---|---|--------------------|------------|-------------|---------------|----------------------|---------------------------|---------|------|---------------|----------------|------------------------|------------|
| Substitution for form 1449PTO <h2 style="text-align: center;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT</h2> <p style="text-align: center;"><i>(Use as many sheets as necessary)</i></p> | <p style="text-align: right;">Complete if Known</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Application Number</td> <td>10/049,101</td> </tr> <tr> <td>Filing Date</td> <td>July 23, 2002</td> </tr> <tr> <td>First Named Inventor</td> <td>Scott A. MOSKOWITZ et al.</td> </tr> <tr> <td>An Unit</td> <td>2131</td> </tr> <tr> <td>Examiner Name</td> <td>Jeremiah AVEHY</td> </tr> <tr> <td>Attorney Docket Number</td> <td>80408.0011</td> </tr> </table> | Application Number | 10/049,101 | Filing Date | July 23, 2002 | First Named Inventor | Scott A. MOSKOWITZ et al. | An Unit | 2131 | Examiner Name | Jeremiah AVEHY | Attorney Docket Number | 80408.0011 |
| Application Number | 10/049,101 | | | | | | | | | | | | |
| Filing Date | July 23, 2002 | | | | | | | | | | | | |
| First Named Inventor | Scott A. MOSKOWITZ et al. | | | | | | | | | | | | |
| An Unit | 2131 | | | | | | | | | | | | |
| Examiner Name | Jeremiah AVEHY | | | | | | | | | | | | |
| Attorney Docket Number | 80408.0011 | | | | | | | | | | | | |
| Sheet <u>1</u> of <u>1</u> | | | | | | | | | | | | | |

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|--|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Kind Code ² (if known) | | | |
| | | US-4,528,588 | 07/09/1985 | Lofberg | |
| | | US-5,832,119 | 11/03/1998 | Rhoads | |
| | | US-5,859,920 | 01/12/1999 | Daly et al. | |
| | | US-4,979,210 | 12/18/1990 | Nagata et al. | |
| | | US-5,774,452 | 06/30/1998 | Wolosewicz | |
| | | US-4,405,829 | 09/20/1983 | Rivetti et al. | |
| | | US-6,330,335 | 12/11/2001 | Rhoads | |
| | | US-3,986,624 | 10/19/1976 | Cates Jr. et al. | |
| | | US-5,363,448 | 11/08/1994 | Koopman et al. | |
| | | US-5,568,570 | 10/22/1996 | Fabbiani | |
| | | US-5,636,292 | 06/03/1997 | Rhoads | |
| | | US-4,972,471 | 11/20/1990 | Gross et al. | |
| | | US-5,893,067 | 04/06/1999 | Bender et al. | |
| | | US-5,689,587 | 11/18/1997 | Bender et al. | |
| | | US-3,984,624 | 10/05/1976 | Waggoner | |
| | | US-4,038,596 | 07/26/1977 | Lee | |
| | | US-4,200,770 | 04/29/1980 | Hellman, et al. | |
| | | US-4,218,582 | 08/19/1980 | Hellman, et al. | |
| | | US-4,424,414 | 01/03/1984 | Hellman, et al. | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|----------|---|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Country Code ¹ Number ² Kind Code ³ (if known) | | | |
| | | WO 9744736 | 11/27/1997 | Wehrenberg | |
| | | WO 9952271 | 10/14/1999 | MOSKOWITZ | |
| | | WO 9963443 | 12/09/1999 | Hs. Anthony Tung Shuen | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|--------------------|----------------|
| Examiner Signature | Date Completed |
|--------------------|----------------|

EXAMINER: Initial a reference considered, whether or not citation is in compliance with MPEP §600. Draw line through citation if not in compliance and not amended. Include copy of this form with next communication to applicant. * Applicant's unique citation designation number (optional). ² See Kind Code of USPTO Patent Documents at www.uspto.gov or MPEP §01.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard 3T.3). ⁴ For Japanese patent documents, the indicia of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Use of document by the appropriate symbols as indicated on the document under WIPO Standard 5T.10 if possible. ⁶ Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the priority which is to file (in) by the USPTO to process an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.54. The collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. There will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1460, Alexandria, VA 22313-1460. DO NOT SEND FEE OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1460, Alexandria, VA 22313-1460.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it carries a valid OMB control number.

| | | | | | | | | | | | | | |
|---|---|--------------------|------------|-------------|---------------|----------------------|---------------------------|----------|------|---------------|----------------|------------------------|------------|
| Substitutes for form 1449/PTO <h2 style="text-align: center; margin: 0;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT</h2> <p style="text-align: center; font-size: small;">(Use as many sheets as necessary)</p> | <h3 style="text-align: center; margin: 0;">Complete if Known</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Application Number</td> <td>10/049,101</td> </tr> <tr> <td>Filing Date</td> <td>July 23, 2002</td> </tr> <tr> <td>First Named Inventor</td> <td>Scott A. MOSKOWITZ et al.</td> </tr> <tr> <td>Art Unit</td> <td>2131</td> </tr> <tr> <td>Examiner Name</td> <td>Jeremiah AVERY</td> </tr> <tr> <td>Attorney Doctel Number</td> <td>80408.0011</td> </tr> </table> | Application Number | 10/049,101 | Filing Date | July 23, 2002 | First Named Inventor | Scott A. MOSKOWITZ et al. | Art Unit | 2131 | Examiner Name | Jeremiah AVERY | Attorney Doctel Number | 80408.0011 |
| Application Number | 10/049,101 | | | | | | | | | | | | |
| Filing Date | July 23, 2002 | | | | | | | | | | | | |
| First Named Inventor | Scott A. MOSKOWITZ et al. | | | | | | | | | | | | |
| Art Unit | 2131 | | | | | | | | | | | | |
| Examiner Name | Jeremiah AVERY | | | | | | | | | | | | |
| Attorney Doctel Number | 80408.0011 | | | | | | | | | | | | |
| Sheet <u>4</u> of <u>12</u> | | | | | | | | | | | | | |

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|-----------|-----------------------------|------------------|---|---|
| Examiner Initials* | Cite No.† | Document Number | Publication Date | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Kind Code‡(if known) | MM-DD-YYYY | | |
| | | US-5,640,589 | 06/17/1997 | Miller, et al. | |
| | | US-5,659,726 | 08/19/1997 | Sandford, II, et al. | |
| | | US-5,664,018 | 09/02/1997 | Leighton | |
| | | US-5,687,236 | 11/11/1997 | Moskowitz, et al. | |
| | | US-5,734,752 | 03/31/1998 | Knox | |
| | | US-5,745,589 | 04/28/1998 | Moskowitz, et al. | |
| | | US-5,506,795 | 04/09/1998 | Yamakawa | |
| | | US-5,680,462 | 10/21/1997 | Miller, et al. | |
| | | US-5,696,828 | 12/09/1997 | Koopman, Jr. | |
| | | US-5,740,244 | 04/14/1998 | Indeck, et al. | |
| | | US-5,751,811 | 05/12/1998 | Koopman, Jr. | |
| | | US-5,757,923 | 05/26/1998 | Koopman, Jr. | |
| | | US-5,889,868 | 03/30/1999 | Moskowitz, et al. | |
| | | US-6,208,745 | 03/27/2001 | Florenio, et al. | |
| | | US-6,285,775 | 09/04/2001 | Wu, et al. | |
| | | US-6,385,329 | 05/07/2002 | Bharna, et al. | |
| | | US-6,530,021 | 03/04/2003 | Epstein, et al. | |
| | | US-6,425,081 | 07/23/2002 | wamura | |
| | | US- | | | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|-----------|---|------------------|---|---|
| Examiner Initials* | Cite No.† | Foreign Patent Document | Publication Date | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Agency Code‡ Number‡ Kind Code‡(if known) | MM-DD-YYYY | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. †Applicant's unique citation designation number (optional). ‡See Kind Codes at USPTO Patent Documents at www.uspto.gov or MPEP 801.04. † Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ‡ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. † Kind of document by the appropriate symbol as indicated on the document under WIPO Standard ST 16 if possible. ‡ Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to the (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 3 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form, or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1460, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-8199 (1-800-785-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it carries a valid OMB control number.

Substitute for form 1449(PTO)

Complete if Known

| | |
|--|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | Application Number: 10/049,101 Filing Date: July 23, 2002 First Named Inventor: Scott A. MOSKOWITZ et al. Art Unit: 2131 Examiner Name: Jeremiah AVERY Attorney Docket Number: 80-408.0011 |
|--|---|

Sheet 5 of 12

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|--|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patent or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number/Kind Code ¹ (if known) | | | |
| | | US-6,522,789 | 02/18/2003 | Rhoads, et al. | |
| | | US-2005/0160271 | 07/21/2005 | Brundage, et al. | |
| | | US-6,665,489 | 12/16/2003 | Collart | |
| | | US-2004/0128514 | 07/01/2004 | Rhoads | |
| | | US-2004/0037449 | 02/26/2004 | Davis, et al. | |
| | | US-6,823,455 | 11/23/2004 | Macy, et al. | |
| | | US-2003/0133702 | 07/17/2003 | Collart | |
| | | US-6,668,246 | 12/23/2003 | Yeung, et al. | |
| | | US-6,405,203 | 06/11/2002 | Collart | |
| | | US-6,141,754 | 10/31/2000 | Froy | |
| | | US-6,493,457 | 12/10/2002 | Quackenbush | |
| | | US-5,629,980 | 05/13/1997 | Siefik, et al. | |
| | | US-5,943,422 | 08/24/1999 | Van Wie, et al. | |
| | | US-5,636,276 | 06/03/1997 | Brugge | |
| | | US-5,341,429 | 08/23/1994 | Stringer, et al. | |
| | | US-6,754,822 | 08/22/2004 | Chao | |
| | | US-6,131,162 | 10/10/2000 | Yoshimura et al. | |
| | | US-7,058,570 | 06/06/2006 | WU, et al. | |
| | | US- | | | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|----------|---|-----------------------------|---|---|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear |
| | | Country Code ¹ Number ¹ Kind Code ¹ (if known) | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|---------------------------|-----------------------|
| Examiner Signature: _____ | Date Completed: _____ |
|---------------------------|-----------------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). ²See Kind Code of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Entry Office that issued the document, by the two-letter code (WIPO Standard 57.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard 57.16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. This information is required to obtain or retain a benefit by the public which is to be paid by the USPTO in process an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.18. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

| | | | |
|--|------------------------|--------------------------|---------------------------|
| Submittal for form 1440PTO | | Complete if Known | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| Sheet <u>6</u> of <u>12</u> | Attorney Docket Number | 80408.0011 | |

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|--|--------------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Kind Code ² (if known) | | | |
| | | US-5,930,369 | 07/27/1999 | Caw, et al. | |
| | | US-6,415,041 | 07/02/2002 | Osani, et al. | |
| | | US-6,141,753 | 10/31/2000 | Zhao, et al. | |
| | | US-2002/0097873 | 07/25/2002 | Petrovic | |
| | | US-6,785,815 | 08/31/2004 | Serret-Avila, et al. | |
| | | US-6,523,113 | 02/18/2003 | Wehrenberg | |
| | | US-6,233,347 | 05/15/2001 | Chen, et al. | |
| | | US-6,233,684 | 05/15/2001 | Stelik, et al. | |
| | | US-2006/0013395 | 01/19/2006 | Brundage, et al. | |
| | | US-7,043,050 | 05/09/2006 | Mival | |
| | | US-5,809,160 | 09/15/1998 | Powell, et al. | |
| | | US-6,272,634 | 08/07/2001 | Tawfik, et al. | |
| | | US-6,282,650 | 08/28/2001 | Davis | |
| | | US-6,557,103 | 04/29/2003 | Boncalet, Jr., et al. | |
| | | US-2003/0126445 | 07/03/2003 | Wehrenberg | |
| | | US-6,978,370 | 12/20/2005 | Kocher | |
| | | US-2006/0005029 | 01/05/2006 | Petrovic, et al. | |
| | | US-6,278,791 | 08/21/2001 | Horsinger, et al. | |
| | | US- | | | |

| FOREIGN PATENT DOCUMENTS | | | | | | |
|--------------------------|----------|---|--------------------------------|---|---|----------------|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear | 7 ^o |
| | | Country Code ² (USPTO Kind Code) ³ (if known) | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique station designation number (optional). ²See Kind Codes of USPTO Patent Documents at www.uspto.gov in MPEP 901.04. ³Entry Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WPO Standard ST.16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.07 and 1.56. The information is required to obtain or retain a patent by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 422 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed response form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-756-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid CMS control number.

| | | | |
|--|---|--------------------------|---------------------------|
| Substitute for form 1 (USPTO) | | Complete if Known | |
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | | Application Number | 10/049,101 |
| | | Filing Date | July 23, 2002 |
| | | First Named Inventor | Scott A. MOSKOWITZ et al. |
| | | Art Unit | 2131 |
| | | Examiner Name | Jeremiah AVERY |
| | | Attorney Docket Number | 80408.0011 |
| Sheet | 3 | of | 12 |

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|---|--------------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Ford Code ¹ (Mandatory) | | | |
| | | US-6,061,793 | 05/09/2000 | Tewfik, et al. | |
| | | US-5,809,139 | 09/15/1998 | Grrod, et al. | |
| | | US-5,848,155 | 12/08/1998 | Cox | |
| | | US-5,915,027 | 06/22/1999 | Cox et al. | |
| | | US-5,940,134 | 08/17/1999 | Wirtz | |
| | | US-5,991,426 | 11/23/1999 | Cox, et al. | |
| | | US-6,069,914 | 05/30/2000 | Gos | |
| | | US-5,943,422 | 08/24/1999 | Van Wm, et al. | |
| | | US-6,539,475 | 03/25/2003 | Cox, et al. | |
| | | US-6,310,962 | 10/30/2001 | Chung, et al. | |
| | | US-6,154,571 | 11/28/2000 | Cox, et al. | |
| | | US-4,969,204 | 11/06/1990 | Johns, et al. | |
| | | US-6,687,683 | 02/03/2004 | Harada, et al. | |
| | | US-6,373,892 | 04/16/2002 | Ichien, et al. | |
| | | US-5,870,474 | 02/09/1999 | Wasilewski, et al. | |
| | | US-5,418,713 | 05/23/1995 | Allen | |
| | | US-6,078,664 | 06/20/2000 | Moskowitz, et al. | |
| | | US-6,009,176 | 12/28/1999 | Bennaro, et al. | |
| | | US-6,081,587 | 06/27/2000 | Hoffstein, et al. | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|----------|---|--------------------------------|---|---|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Country Code ¹ / Number ² / Ford Code ³ (if known) | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in compliance with MPEP 609. Draw line through citation if not in compliance and not considered. Include copy of this form with next communication to Applicant. Applicant's unique citation designation number (optional). See Kind Codes at USPTO Patent Documents at www.uspto.gov or MPEP 601.04. ¹Enter Office that issued the document, by the two-letter code (WIPO Standard ST 3). ²For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ³Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST 10 if possible. ⁴Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is a fee (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.34. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEE OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-706-9199) and select option 2.

Under the Paperwork Reduction Act of 1996, no person is required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1462PTO

Complete if Known

| | | | | | | | | | | | | | |
|--|--|--------------------|------------|-------------|---------------|----------------------|--------------------------|----------|------|---------------|----------------|------------------------|------------|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i> | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Application Number</td><td>10/049,101</td></tr> <tr><td>Filing Date</td><td>July 29, 2002</td></tr> <tr><td>First Named Inventor</td><td>Scott A. MOSKOWITZ et al</td></tr> <tr><td>Art Unit</td><td>2131</td></tr> <tr><td>Examiner Name</td><td>Jeremiah AVERY</td></tr> <tr><td>Attorney Docket Number</td><td>80408.0011</td></tr> </table> | Application Number | 10/049,101 | Filing Date | July 29, 2002 | First Named Inventor | Scott A. MOSKOWITZ et al | Art Unit | 2131 | Examiner Name | Jeremiah AVERY | Attorney Docket Number | 80408.0011 |
| Application Number | 10/049,101 | | | | | | | | | | | | |
| Filing Date | July 29, 2002 | | | | | | | | | | | | |
| First Named Inventor | Scott A. MOSKOWITZ et al | | | | | | | | | | | | |
| Art Unit | 2131 | | | | | | | | | | | | |
| Examiner Name | Jeremiah AVERY | | | | | | | | | | | | |
| Attorney Docket Number | 80408.0011 | | | | | | | | | | | | |

Sheet 3 of 12

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|-----------|------------------------------|-----------------------------|---|---|
| Examiner Initials* | Cite No.† | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Kind Code‡ (if known) | | | |
| | | US-6,598,182 | 07/22/2003 | Moskowitz | |
| | | US-6,275,988 | 08/14/2001 | Nagashima, et al. | |
| | | US-6,051,029 | 04/18/2000 | Paterson, et al. | |
| | | US-5,917,915 | 05/29/1998 | Hirose | |
| | | US-6,775,772 | 08/10/2004 | Bimling, et al. | |
| | | US-6,686,246 | 12/23/2003 | Yeung, et al. | |
| | | US-6,351,765 | 02/28/2002 | Pietropoli, et al. | |
| | | US-6,049,838 | 04/11/2000 | Miller, et al. | |
| | | US-5,398,285 | 03/14/1995 | Bergelt, et al. | |
| | | US-5,737,733 | 04/07/1998 | Eller | |
| | | US-2002/0103883 | 08/01/2002 | Vivierstock, et al. | |
| | | US-5,673,316 | 09/30/1997 | Auerbach, et al. | |
| | | US-6,647,424 | 11/11/2003 | Pearson, et al. | |
| | | US-6,977,894 | 12/20/2005 | Achilles, et al. | |
| | | US-6,453,252 | 09/17/2002 | Arcebe | |
| | | US-5,077,665 | 12/31/1991 | Biverman, et al. | |
| | | US-5,136,581 | 08/04/1992 | Machrows | |
| | | US-5,341,477 | 08/23/1994 | Hilli, et al. | |
| | | US-5,581,703 | 12/03/1996 | Baugher, et al. | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|-----------|--|-----------------------------|---|---|
| Examiner Initials* | Cite No.† | Foreign Patent Document‡ | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Country Code, Number, and Kind Code (if known) | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|--------------------|----------------|
| Examiner Signature | Date Completed |
|--------------------|----------------|

*EXAMINER: initial if reference considered, whether or not citation is in conformance with MPEP 618. Draw lines through citation if not in conformance and not considered. (Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). † See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ‡ EPO: Office that issued the document; by the two-letter code (WIPO Standard ST.3). † For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. † Mark of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16. † Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to (a) and by the USPTO in processing an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22315-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22315-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number.

| | | | | | | | | | | | | | |
|--|--|---------------------|------------|--------------|---------------|-----------------------|---------------------------|-----------|------|----------------|----------------|-------------------------|------------|
| Submission for form 1449-PTO <h2 style="text-align: center; margin: 0;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT</h2> <p style="text-align: center; font-size: small;">(Use as many sheets as necessary)</p> | <p style="text-align: center; font-weight: bold; margin: 0;">Complete if Known</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Application Number:</td><td>10/049,101</td></tr> <tr><td>Filing Date:</td><td>July 23, 2002</td></tr> <tr><td>First Named Inventor:</td><td>Scott A. MOSKOWITZ et al.</td></tr> <tr><td>Art Unit:</td><td>2131</td></tr> <tr><td>Examiner Name:</td><td>Jeremiah AVERY</td></tr> <tr><td>Attorney Docket Number:</td><td>80408.0011</td></tr> </table> | Application Number: | 10/049,101 | Filing Date: | July 23, 2002 | First Named Inventor: | Scott A. MOSKOWITZ et al. | Art Unit: | 2131 | Examiner Name: | Jeremiah AVERY | Attorney Docket Number: | 80408.0011 |
| Application Number: | 10/049,101 | | | | | | | | | | | | |
| Filing Date: | July 23, 2002 | | | | | | | | | | | | |
| First Named Inventor: | Scott A. MOSKOWITZ et al. | | | | | | | | | | | | |
| Art Unit: | 2131 | | | | | | | | | | | | |
| Examiner Name: | Jeremiah AVERY | | | | | | | | | | | | |
| Attorney Docket Number: | 80408.0011 | | | | | | | | | | | | |
| Sheet <u>7</u> of <u>12</u> | | | | | | | | | | | | | |

| U. S. PATENT DOCUMENTS | | | | | |
|------------------------|----------|--------------------------------------|--------------------------------|---|---|
| Examiner Initials* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Number-Kind Code ² / Name | | | |
| | | US-5,548,579 | 08/20/1998 | Lebrun, et al. | |
| | | US-5,905,975 | 05/18/1999 | Aisubel | |
| | | US-6,457,058 | 09/24/2002 | Ulum et al. | |
| | | US-6,381,618 | 04/30/2002 | Jones et al. | |
| | | US-2002/0026343 | 02/28/2002 | Duenke | |
| | | US-6,230,268 | 05/08/2001 | Miwa et al. | |
| | | US-6,199,058 | 03/06/2001 | Wong et al. | |
| | | US-5,920,900 | 07/06/1999 | Pools et al. | |
| | | US-5,884,033 | 03/16/1999 | Dirvall et al. | |
| | | US-5,478,990 | 12/26/1995 | Montanari et al. | |
| | | US-6,430,302 | 08/06/2002 | Rhoads | |
| | | US-6,725,372 | 04/20/2004 | Lewis et al. | |
| | | US-6,606,593 | 08/12/2003 | Xie et al. | |
| | | US-6,584,125 | 06/24/2003 | Katko | |
| | | US-6,442,283 | 08/27/2002 | Tewell et al. | |
| | | US-6,377,625 | 04/23/2002 | Kim | |
| | | US-6,282,300 | 08/28/2001 | Bloom et al. | |
| | | US-6,205,249 | 03/20/2001 | Moskowitz | |
| | | US-6,029,126 | 02/22/2000 | Maizer | |

| FOREIGN PATENT DOCUMENTS | | | | | |
|--------------------------|----------|---|--------------------------------|---|---|
| Examiner Initials* | Cite No. | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
| | | Country Code ³ Number ⁴ Kind Code ⁵ (if known) | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of the form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 801.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind or document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or issue a benefit by the public which it is filed and by the USPTO in process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, organizing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, responses are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449PTO

**INFORMATION DISCLOSURE
 STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Sheet 10 of 12

Complete if Known

| | |
|------------------------|--------------------------|
| Application Number | 10/049,101 |
| Filing Date | July 23, 2002 |
| First Named Inventor | Scott A. MOSKOWITZ et al |
| Att. Unit | 2131 |
| Examiner Name | Jeremiah AVERY |
| Attorney Docket Number | 80408.0011 |

U. S. PATENT DOCUMENTS

| Examiner/Inventor* | Cite No. | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|--------------------|----------|--|--------------------------------|---|---|
| | | Number-Kind Code ¹ (if known) | | | |
| | | US-5,754,697 | 05/19/1998 | Fu et al. | |
| | | US-5,479,210 | 12/26/1995 | Cawley et al. | |
| | | US-3,947,825 | 03/30/1976 | Cassada | |
| | | US-5,903,721 | 05/11/1999 | Sixtus | |
| | | US-5,750,677 | 08/04/1998 | Fox et al. | |
| | | US-5,243,515 | 09/07/1993 | Clearwater | |
| | | US-4,339,134 | 07/13/1982 | Machiel | |
| | | US-4,827,508 | 05/02/1989 | Shear | |
| | | US-4,896,275 | 01/23/1990 | Jackson | |
| | | US-4,977,594 | 12/11/1990 | Shear | |
| | | US-5,050,213 | 09/17/1991 | Shear | |
| | | US-5,369,707 | 11/29/1994 | Follandore, III | |
| | | US-5,406,627 | 04/11/1995 | Thompson et al | |
| | | US-5,410,598 | 04/25/1995 | Shaw | |
| | | US-5,469,538 | 11/21/1995 | Blank | |
| | | US-5,497,419 | 03/05/1996 | Hill | |
| | | US-5,513,261 | 04/30/1996 | Mahe | |
| | | US-5,530,739 | 06/25/1996 | Orada | |
| | | US-5,598,470 | 01/28/1997 | Cooper et al. | |

FOREIGN PATENT DOCUMENTS

| Examiner/Inventor* | Cite No. ¹ | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | TF |
|--------------------|-----------------------|---|--------------------------------|---|---|----|
| | | Country Code ² /Number ³ /Kind Code ⁴ (if known) | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | |
|--------------------|-----------------|
| Examiner Signature | Date Considered |
|--------------------|-----------------|

*EXAMINER: Indicate reference citations, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of the form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.93 and 1.86. The information is required to assist or assist in the public which is to be used by the USPTO to process an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Substitute for form MPEP 702

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 12

Complete if Known

| | |
|------------------------|--------------------------|
| Application Number | 10/049,101 |
| Filing Date | July 23, 2002 |
| First Named Inventor | Scott A. MOSKOWITZ et al |
| Art Unit | 2131 |
| Examiner Name | Jeremiah AVERY |
| Attorney Docket Number | 80408.0011 |

U. S. PATENT DOCUMENTS

| Examiner Initials* | Cite No. ¹ | Document Number | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|--------------------|-----------------------|--|-----------------------------|---|---|
| | | Number-Kind Code ² // Month | | | |
| | | US-5,825,690 | 04/29/1997 | Michel et al | |
| | | US-5,833,932 | 05/27/1997 | Davis et al | |
| | | US-5,719,937 | 02/17/1998 | Warren et al | |
| | | US-5,737,416 | 04/07/1998 | Cooper et al | |
| | | US-5,765,152 | 06/09/1998 | Erickson | |
| | | US-5,799,083 | 08/25/1998 | Brothers et al | |
| | | US-5,973,731 | 10/26/1999 | Schwab | |
| | | US-5,894,521 | 04/13/1999 | Conkly | |
| | | US-5,905,800 | 05/18/1999 | Moskowitz et al | |
| | | US-5,963,909 | 10/05/1999 | Warren et al | |
| | | US-5,974,141 | 10/26/1999 | Sawyer | |
| | | US-5,999,217 | 12/07/1999 | Berners-Lee | |
| | | US-6,041,316 | 03/21/2000 | Allen | |
| | | US-6,081,251 | 06/27/2000 | Sawai et al | |
| | | US-6,278,780 | 08/21/2001 | Shimada | |
| | | US-6,301,663 | 10/09/2001 | Kato et al | |
| | | US-6,240,121 | 05/29/2001 | Sanoh | |
| | | US- | | | |
| | | US- | | | |

FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No. ¹ | Foreign Patent Document | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages, Or Relevant Figures Appear | † |
|--------------------|-----------------------|---|-----------------------------|---|--|---|
| | | Country Code ² Number ³ Kind Code ⁴ (if known) | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | |
|--------------------|--------------|
| Examiner Signature | Date Colored |
|--------------------|--------------|

*EXAMINER: Initial if reference considered, whether or not citation is in accordance with MPEP 609. Draw line through citation if not in accordance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See kind codes of USPTO Patent Documents at www.uspto.gov or MPEP 801.04. ³ Enter Office that issued the document, by the two letter code (WIPO Standard ST 3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST 16 if possible. ⁶ Applicant is to place a check mark here if English language translation is attached.

The collection of information is required by 37 CFR 1.97 and 1.98. This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the complete application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1460, Alexandria, VA 22313-1460. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1460, Alexandria, VA 22313-1460.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

XP-000825846

Transform Permuted Watermarking for Copyright Protection of Digital Video.

Andrew Johnson* and Michael Bigger

Telstra Research Laboratories
770 Blackburn Rd, Clayton,
Victoria, Australia.**Abstract**

As we move into an age of widespread availability and distribution of digital video content, the content production industry has justifiable concerns about copyright violations; digital copies are simple, cheap and exact. Embedded invisible digital watermarks have been discussed and proposed in the past as a means of providing proof of ownership in cases where digital video copyright violations are claimed. However, previous solutions have suffered from a lack of true security and unmanageable limitations such as the requirement to have an authenticated original present when reading a watermark. In this paper, a new watermarking solution is described, based on a unique data randomisation approach, which provides excellent security while simultaneously achieving invisibility of the watermark and robustness to picture manipulation and distortion. The solution is easily implemented, tolerant of video compression and even digital-to-analogue and analogue-to-digital conversion, yet does not require availability of the original content to read the watermark.

1. Introduction

Provision of copyright protection for digital video source material is a concern for the owners of multimedia content worldwide. This is because a digital copy is an exact duplicate. There is no degradation introduced by copying. In contrast to copying of analogue video, one method of protecting the intellectual property rights of digital video is through the use of digital watermarking technology [6]. A watermark is a means of sending information embedded into the digital content, to identify the owner of that content. The watermark is checked whenever the legal right to use the content is questioned. Visible watermarks are commonly seen on TV broadcasts, in the form of the broadcaster's logo, visibly overlaid on the displayed picture in a corner. Whilst useful for the purposes of broadcaster identification, visible watermarks are not suitable for copyright protection as they do not offer a high level

of security. A visible watermark of this type can be removed or rendered ineffective using simple signal processing techniques.

An invisible watermark is preferable for copyright protection. In this case, data is embedded into the image content using signal processing techniques generally based upon spread spectrum technology. Though invisible to the viewer, the embedded watermark must be robust (still can be extracted even after, for example, digital compression, multiple generation recording or digital to analog and analog to digital conversion) and secure (cannot be removed by deliberately manipulating the picture). The technology proposed in this paper to achieve these objectives, unlike several other known approaches [1] [2], does not require the presence of the original when the watermark is to be read. This is an important feature; without it, it would be necessary, before even trying to read any embedded watermark, to identify (manually or perhaps with some machine assistance) not just the title of the original material, but also the exact segment within it. This would make the process very costly and probably impractical, since it implies trusted third parties with potentially massive archives of copies of original material, along with the processes to attempt to match segments in dispute.

2. Watermarking based upon Transform Techniques

Watermark data can be embedded into an image or image sequence using transform domain techniques. In this approach, an orthogonal transform is applied to the spatial domain image data to produce a set of transform coefficients. A subset of these are selected for modification based upon the watermark data, as shown in Figure 1. For example, the modification could take the form of incrementing selected transform coefficients to encode logic 1 and decrementing coefficients to encode logic 0. An inverse transform is then applied to reconstruct the watermarked spatial domain data.

* Now with Divicom, USA.

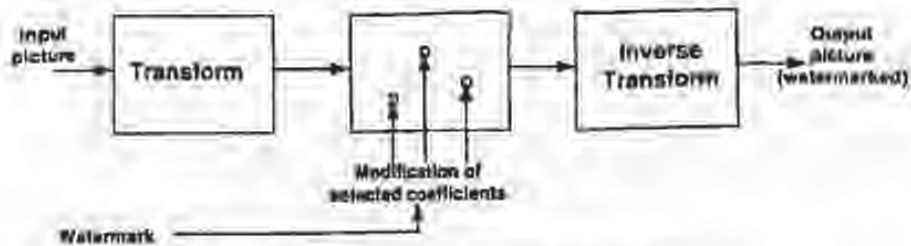


Figure 1. Transform based watermark write operation.

In the spatial domain, the watermark consists of a noise-like sequence, the characteristics of which are determined by the transform used, which coefficient(s) have been modified, the magnitude of the modification and the statistics of the image being watermarked. The Discrete Cosine Transform (DCT), Walsh-Hadamard Transform (WHT), Discrete Fourier Transform (DFT) and Daubechey Wavelet Transform (DWT) have all been proposed as transform operations suited to the watermarking application [1] [2].

To ensure that the watermark is robust using the above mentioned transforms, modifications should be performed on transform coefficients that contain significant energy. Otherwise they could be removed/degraded without impacting on the picture quality. On the other hand, if the watermark is to be essentially invisible and hidden from deliberate attempts to find and remove or alter it, the modifications should be small and applied to insignificant coefficients. It is apparent that the robustness, invisibility and security requirements are conflicting. Typically, the size and location of modifications to coefficients are image sequence dependent and so the original image or image sequence is required as a reference in the watermark reading operation. Such a watermark can only be used for a copyright protection application if the original image or image sequence is certified by a trusted third party. A successfully extracted watermark on its own does not provide proof of ownership, since two parties could each extract their own watermarks from their own copies of what they claim is the original. Clearly, such a restriction limits the usefulness of this technology for protecting the intellectual property for the owners of the digital video content.

3. Transform Permuted Watermarking

The transform based watermarking procedure previously described has some similarities to spread spectrum communications. The spatial frequency content of the image or image sequence can be considered as the communication channel while the watermark is the signal to be transmitted. The purpose

of the inverse transform is to perform an energy spreading operation, transmitting the narrowband signal over a larger bandwidth. It is apparent, however, that the proposed transforms have spectral characteristics that are quite the inverse of what is required by a system based upon spread spectrum technology. In fact, the DCT, WHT and DWT have all found applications in image compression where it is desirable, for a given coded bitrate, to contain signal energy to the least number of transform coefficients. That is, they perform energy compaction. In contrast, we shall show that performance benefits can be obtained if the transform operation in question has an energy spreading capability.

The watermarking solution proposed in this paper relies on an energy spreading transform which is unique to each content producer, or distributor or, if required, even to each piece of content (eg. movie)¹. One approach to energy spreading is to apply a pseudo-random reversible function to the image data, prior to the application of the analysis transform. This function performs a spectral whitening operation on the image data that is repeatable, even in the presence of noise and/or distortion. Many pseudo-random functions could be used, but one that offers good performance in terms of its noise rejection capability, spectral whitening performance and simplicity of implementation is a permutation of the data block based upon a keyed random number generator. This approach is termed TPW (Transformed Permutation Watermarking).

The TPW watermark insertion procedure is illustrated in Figure 2.

¹ The last example here (unique code for each piece of content) is not recommended. Since the code must be known before the watermark can be read, this requires identification of the likely title before a watermark check can be carried out. If it is necessary to individually mark each piece of content, this is probably best done by alternating two watermarks - one unique to the content owner, and one unique to the content.

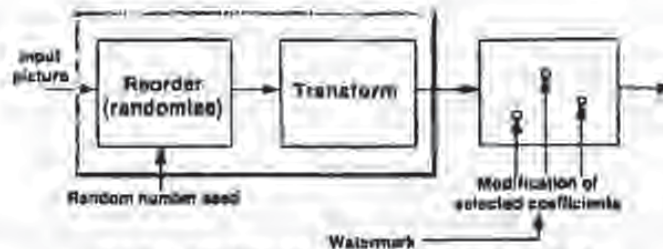


Figure 2. Transform permuted watermark write operation

In an alternative interpretation, the combined data permutation and transform operation is equivalent to, in the one dimensional case, a permutation of the columns making up the basis matrix of the transform in question. Each permutation will therefore yield an orthogonal transform, hence the number of transforms contained in the set is equal to the number of available permutations. Using this interpretation, the security of the watermark relies not just on which transform coefficient has been modified to contain the watermark data, but also on which member of the set of available transforms has been used, and this is determined by a random number seed. Without knowing the seed that defines the permutation, the watermark cannot be read.

The inclusion of this permutation in front of the energy compaction transform block has extensive system implications.

(i) Location of transform coefficient for modification. The generated AC transform coefficients (i.e. all coefficients except the one that contains the block average) have approximately equal variances. A permute operation is selected that performs a spectral whitening which flattens the PSD (Power Spectral Density) of the data block. Because the AC coefficient magnitudes are comparable, modifications for watermark insertion can be comparable, independent of the transform coefficient selected. It will therefore produce comparable distortion (calculated using the Mean Squared Error distortion criteria) in the reconstructed data block. The watermarking procedure is therefore not sensitive to the choice of transform coefficient(s) for modification.

The selection of transform coefficient(s) for modification must be deterministic and be determined by a pseudo random process. Security from the possibility of a statistical attack on the watermarked data is maximised in this case by ensuring that the same transform coefficient in subsequent blocks is not always used to contain watermark data.

(ii) Method of transform coefficient modification. The modification of transform coefficients can reduce to a simple operation that is independent of the transform coefficient selected (i.e. it does not have to change according to some energy distribution). This allows a watermark reading operation that is low in complexity and which does not require access to the original source material. A data watermark bit could be represented by the sign of a selected transform coefficient. A transform coefficient value greater than or equal to zero could represent logic zero and values less than zero represent logic one. Transform coefficient(s) need only be modified if necessary, to ensure that the sign (+/-) corresponds to the digital bit to be embedded (1/0). While the sign determines the watermark data, the magnitude determines the strength of the watermark (that is, its robustness, but also its visibility). The watermark can therefore be tuned for particular application requirements. Apart from its simplicity, this method of coefficient modification offers the advantage that it does not require the presence of the original image or image sequence as a reference in the watermark read operation. The embedded watermark and/or the original image sequence therefore do not need to be verified by a certification authority.

A diagram illustrating the TPW write and read procedure for a single watermark data bit is shown in Figure 3.

4 Read Synchronisation and Watermark Validation

To provide copyright protection for a complete image sequence requires repetition of the watermark data bits making up a watermark message throughout the image sequence. To minimise vulnerability to long term statistical analysis of the picture signal (e.g. a very long term average of picture values might eliminate the picture but leave behind the watermark) the starting location of each packet of watermark data can be randomised. The watermark reader therefore needs to achieve synchronisation

before the message data can be read. Synchronisation can be accomplished by prepending a relatively short header in the watermark message data that provides details such as the length of the message. The header is of fixed length (known by the watermark reader), and is appended with a Cyclic Redundancy Code (CRC). Random numbers are also included in the watermark header data to ensure that the

contents (and CRCs) change with time. The header bits are inserted in the same manner as the watermark message data. At the commencement of the watermark read operation, a search is made for the header and, once found, it provides information concerning the starting location of the watermark message data. The packet based structure of the watermark data is illustrated in figure 4.

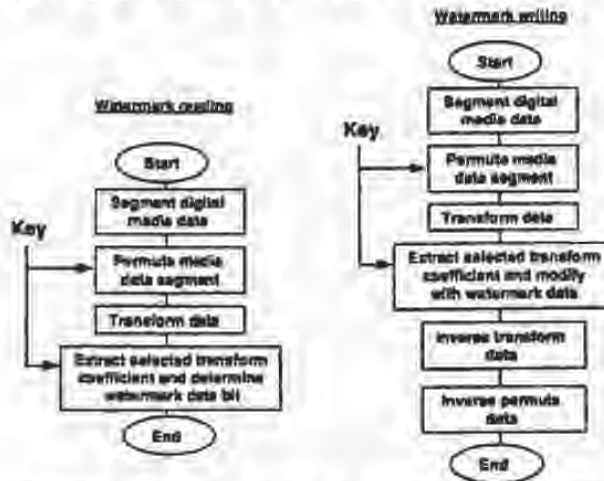


Figure 3 Block diagram for transform based watermark read and write operation

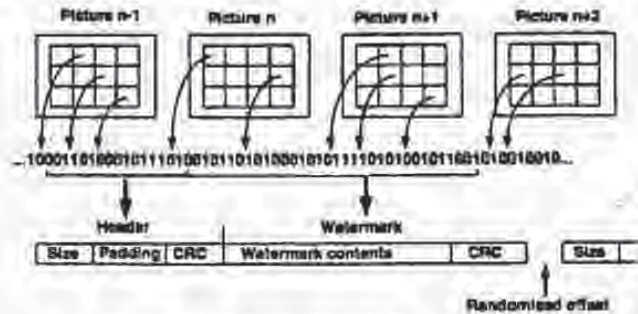


Figure 4 Packet based structure of watermark data

When the watermark is read, it may be subject to a very high error rate due to distortion the picture may have undergone and because we deliberately try to keep the magnitude or strength of the watermark small to minimise its visibility in the image sequence. Another CRC is therefore included with the watermark message data. It is on the basis of this CRC that the watermark reader validates the watermark message. If the CRC is valid, the watermark message (identifying number or ASCII string) can be shown and used for identification purposes.

5 Error correction and robustness to multiple picture formats

While the original picture might be watermarked at a high resolution near the production end of the delivery chain, it is important to protect against two common processes which would otherwise compromise the ability to read the watermark:

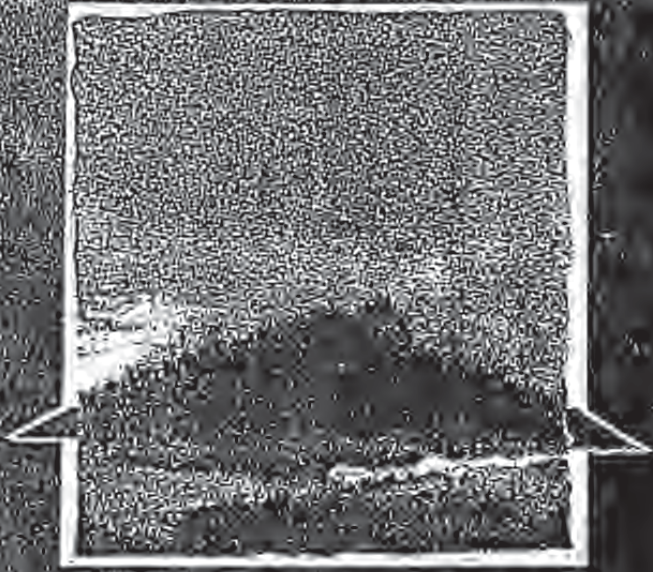
- The picture could be reduced in vertical resolution for delivery at lower rate or via particular delivery systems (eg. "SIF" resolution). This could involve taking just



**SECOND
EDITION**

ever seen... THE ou...
the National Security
Agency wanted never
to be published...
—Wired Magazine

APPLIED CRYPTOGRAPHY



**Protocols, Algorithms,
and Source Code in C**

BRUCE SCHNEIER

BEST AVAILABLE COPY

More recently, people are hiding secret messages in graphic images. Replace the least significant bit of each byte of the image with the bits of the message. The graphical image won't change appreciably—most graphics standards specify more gradations of color than the human eye can notice—and the message can be stripped out at the receiving end. You can store a 64-kilobyte message in a 1024 × 1024 grey-scale picture this way. Several public-domain programs do this sort of thing.

Peter Wayner's *mimic* functions obfuscate messages. These functions modify a message so that its statistical profile resembles that of something else: the classifieds section of *The New York Times*, a play by Shakespeare, or a newsgroup on the Internet [1584, 1585]. This type of steganography won't fool a person, but it might fool some big computers scanning the Internet for interesting messages.

1.3 SUBSTITUTION CIPHERS AND TRANSPOSITION CIPHERS

Before computers, cryptography consisted of character-based algorithms. Different cryptographic algorithms either substituted characters for one another or transposed characters with one another. The better algorithms did both, many times each.

Things are more complex these days, but the philosophy remains the same. The primary change is that algorithms work on bits instead of characters. This is actually just a change in the alphabet size: from 26 elements to two elements. Most good cryptographic algorithms still combine elements of substitution and transposition.

Substitution Ciphers

A substitution cipher is one in which each character in the plaintext is substituted for another character in the ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.

In classical cryptography, there are four types of substitution ciphers:

- A simple substitution cipher, or monoalphabetic cipher, is one in which each character of the plaintext is replaced with a corresponding character of ciphertext. The cryptograms in newspapers are simple substitution ciphers.
- A homophonic substitution cipher is like a simple substitution cryptosystem, except a single character of plaintext can map to one of several characters of ciphertext. For example, "A" could correspond to either 5, 13, 25, or 56, "B" could correspond to either 7, 19, 31, or 42, and so on.
- A polygram substitution cipher is one in which blocks of characters are encrypted in groups. For example, "ABA" could correspond to "RTQ," "ABB" could correspond to "SLL," and so on.
- A polyalphabetic substitution cipher is made up of multiple simple substitution ciphers. For example, there might be five different simple substitution ciphers used; the particular one used changes with the position of each character of the plaintext.



Ko1

APPLIED CRYPTOGRAPHY

Alfred J. Menexes
Paul C. van Oorschot
Scott A. Vanstone

BEST AVAILABLE COPY

Library of Congress Cataloging-in-Publication Data

Menezes, A. J. (Alfred J.), 1965-
Handbook of applied cryptography / Alfred Menezes, Paul van Oorschot,
Scott Vanstone.
p. cm. -- (CRC Press series on discrete mathematics and its
applications)
Includes bibliographical references and index.
ISBN 0-8493-8523-7 (alk. paper)
1. Computers--Access control--Handbooks, manuals, etc.
2. Cryptography--Handbooks, manuals, etc. I. Van Oorschot, Paul C.
II. Vanstone, Scott A., III. Title. IV. Series: Discrete
mathematics and its applications.
QA76.9.A23M463 1996
005.842--dc20

96-27609
CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431.

© 1997 by CRC Press LLC

No claims to original U.S. Government works
International Standard Book Number 0-8493-8523-7
Library of Congress Card Number 96-27609
Printed in the United States of America 3 4 3 6 7 8 9 0
Printed on acid-free paper

BEST AVAILABLE COPY

tamper-resistant hardware. *Steganography* is that branch of information privacy which attempts to obscure the existence of data through such devices as invisible inks, secret compartments, the use of subliminal channels, and the like. Kahn [648] provides an historical account of various steganographic techniques.

Excellent introductions to cryptography can be found in the articles by Diffie and Hellman [347], Massey [786], and Rivest [1054]. A concise and elegant way to describe cryptography was given by Rivest [1054]. *Cryptography is about communications in the presence of adversaries*. The taxonomy of cryptographic primitives (Figure 1.1) was derived from the classification given by Dosselaers, Govaerts, and Vandewalle [175].

§1.3

The theory of functions is fundamental in modern mathematics. The term *range* is often used in place of *image* of a function. The latter, being more descriptive, is preferred. An alternate term for one-to-one is *injective*; an alternate term for onto is *surjective*.

One-way functions were introduced by Diffie and Hellman [345]. A more extensive history is given on page 377. Trapdoor one-way functions were first postulated by Diffie and Hellman [345] and independently by Merkle [850] as a means to obtain public-key encryption schemes; several candidates are given in Chapter 8.

§1.4

The basic concepts of cryptography are treated quite differently by various authors, some being more technical than others. Brassard [192] provides a concise, lucid, and technically accurate account. Schneier [1094] gives a less technical but very accessible introduction. Solomon [1089], Stinson [1178], and Rivest [1054] present more mathematical approaches. Davies and Price [308] provide a very readable presentation suitable for the practitioner.

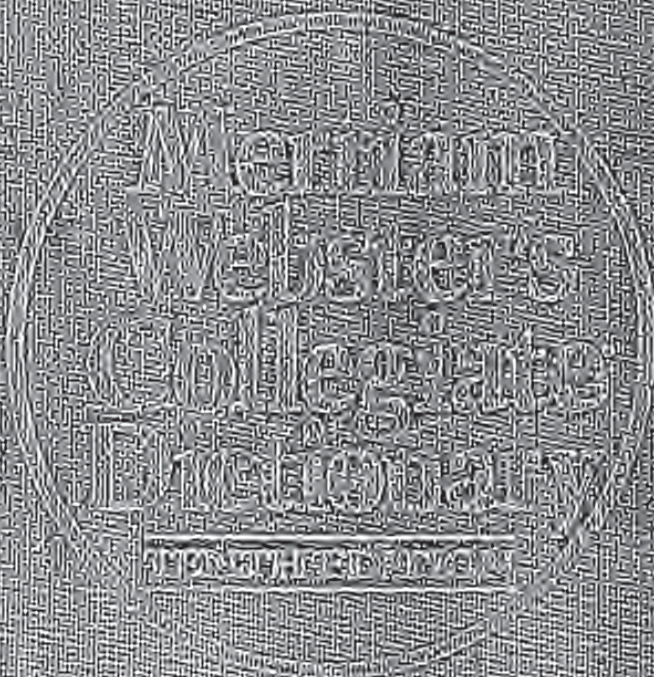
The comparison of an encryption scheme to a resettable combination lock is from Diffie and Hellman [347]. Kerckhoffs' desiderata [668] were originally stated in French. The translation stated here is given in Kahn [648]. Shannon [1121] also gives desiderata for encryption schemes.

§1.5

Symmetric-key encryption has a very long history, as recorded by Kahn [648]. Most systems invented prior to the 1970s are now of historical interest only. Chapter 2 of Denning [326] is also a good source for many of the more well known schemes such as the Caesar cipher, Vigenère and Beaufort ciphers, rotor machines (Enigma and Hagelin), running key ciphers, and so on; see also Davies and Price [308] and Koblitz [705]. Becker and Piper [84] give an in-depth treatment, including cryptanalysis of several of the classical systems used in World War II. Shannon's paper [1121] is considered the seminal work on secure communications. It is also an excellent source for descriptions of various well-known historical symmetric-key ciphers.

Simple substitution and transposition ciphers are the focus of §1.5. Hill ciphers (557), a class of substitution ciphers which substitute blocks using matrix methods, are covered in Example 7.52. The idea of confusion and diffusion (Remark 1.36) was introduced by Shannon [1121].

Kahn [648] gives 1917 as the date when Vernam discovered the cipher which bears Vernam's name, however, Vernam did not publish the result until 1926 [1222]; see page 274 for further discussion. Massey [786] states that reliable sources have suggested that the Moscow-Washington hot-line (channel for very high level communications) is no longer secured with a one-time pad, which has been replaced by a symmetric-key cipher requiring a much shorter key. This change would indicate that confidence and understanding in the



PROPERTY OF U.S. GOVERNMENT

BEST AVAILABLE COPY



A GENUINE MERRIAM-WEBSTER

The name *Webster* alone is no guarantee of excellence. It is used by a number of publishers and may serve mainly to mislead an unwary buyer.

Merriam-Webster™ is the name you should look for when you consider the purchase of dictionaries or other fine reference books. It carries the reputation of a company that has been publishing since 1831 and is your assurance of quality and authority.

Copyright © 1997 by Merriam-Webster, Incorporated.

Philippines Copyright 1997 by Merriam-Webster, Incorporated.

Library of Congress Cataloging in Publication Data
Main entry under title.

Merriam-Webster's collegiate dictionary. — 10th ed.

p. cm.

Includes index.

ISBN 0-87779-708-0 (unindexed : alk. paper). — ISBN 0-87779-709-9 (indexed : alk. paper). — ISBN 0-87779-710-2 (detox : alk. paper). — ISBN 0-87779-707-2 (laminated cover).

I. English language—Dictionaries. I. Merriam-Webster, Inc.

PE1628.M36 1997

473—dc20

96-42529

CFP

Merriam-Webster's Collegiate[®] Dictionary, Tenth Edition principal copyright 1993

COLLEGIATE is a registered trademark of Merriam-Webster, Incorporated.

All rights reserved. No part of this book covered by the copyrights hereon may be reproduced or copied in any form or by any means—graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems—without written permission of the publisher.

Made in the United States of America

1716300RMCR97

Abbrevia

BEST AVAILABLE COPY

SECOND EDITION

PRINCIPLES OF CORPORATE FINANCE

Richard Brealey
London Business School

Stewart Myers
Massachusetts Institute of Technology

omy

ion of Wealth

Finance

ries

McGRAW-HILL BOOK COMPANY

New York St. Louis San Francisco Auckland Bogotá Hamburg
Johannesburg London Madrid Mexico Montreal New Delhi
Panama Paris São Paulo Singapore Sydney Tokyo Toronto

BEST AVAILABLE COPY

This book was set in Optima by Ruttle, Shaw & Wetherill, Inc.
The editors were Patricia A. Mitchell and Scott Amerman;
the designer was Joan E. O'Connor;
the production supervisor was Joe Campanella.
The drawings were done by Fine Line Illustrations, Inc.
R. R. Donnelley & Sons Company was printer and binder.

PRINCIPLES OF CORPORATE FINANCE

Copyright © 1984, 1981 by McGraw-Hill, Inc. All rights reserved.
Printed in the United States of America. Except as permitted under
the United States Copyright Act of 1976, no part of this publication
may be reproduced or distributed in any form or by any means, or
stored in a data base or retrieval system, without the prior written
permission of the publisher.

7890DOCD0C8987

ISBN 0-07-007383-X

Library of Congress Cataloging in Publication Data

Brealey, Richard A.

Principles of corporate finance.

(McGraw-Hill series in finance)

Includes bibliographies and index.

I. Corporations—Finances. I. Myers, Stewart C.

II. Title. III. Series.

HC4026.B667 1984 658.1'5 83-19585

ISBN 0-07-007383-X

BEST AVAILABLE COPY

20-6 SUMMARY

In Chapter 10 we showed you how important it is in capital budgeting decisions to evaluate the option to expand the project at a later date or to abandon it. In this chapter you have come across a number of other financial options. For example, you now know common stock can be thought of as a call option written on the assets of the firm.

There are two basic types of option. An American call is an option to buy an asset at a specified exercise price on or before a specified exercise date. Similarly, an American put is an option to sell the asset at a specified price on or before a specified date. European calls and puts are exactly the same except that they cannot be exercised before the specified exercise date.

What determines the value of a call option? Common sense tells us that it ought to depend on three things:

1. In order to exercise an option you have to pay the exercise price. Other things being equal, the less you are obliged to pay, the better. Therefore, the value of an option increases with the ratio of the asset price to the exercise price.
2. You do not have to pay the exercise price until you decide to exercise the option. Therefore, an option gives you a free loan. The higher the rate of interest and the longer the time to maturity, the more this free loan is worth. Therefore the value of an option increases with the interest rate multiplied by the time to maturity.
3. If the price of the asset falls short of the exercise price, you won't exercise the option. You will, therefore, lose 100 percent of your investment in the option no matter how far the asset depreciates below the exercise price. On the other hand, the more the price rises above the exercise price, the more profit you will make. Therefore the option holder does not lose from increased variability if things go wrong, but gains if they go right. The value of an option increases with the variance per period of the stock return multiplied by the number of periods to maturity.

Ex:

These qualitative relationships have been extended by Black and Scholes in a formal option-valuation formula. Appendix A shows you how to use this formula. We suggested that you look out for ways in which it can be adapted to solve the many option problems that beset the financial manager.

We will use the concepts presented in this chapter to analyze important issues arising later in this book. In this chapter we used option concepts to:

1. Show that underwriters who provide standby agreements in rights offerings provide a valuable service. (We also commented that they seem to overcharge for the service.)
2. Analyze the case for issuing warrants. (Warrants are essentially call options issued by the firm.)

Also, Appendix B shows how to use option pricing concepts to calculate the salvage or abandonment value of an asset.

APPENDIX A USING OPTION-VALUATION MODELS

Does the Black-Scholes option-valuation formula seem a little removed from the real world? It should not. Every day dealers on the Chicago Board Options Exchange use this formula to make huge trades. These dealers are not, for the most part,

trained in the formula's mathematical derivation; they just use a specially programmed calculator or a set of tables to find the value of the option.

Appendix Tables 6 and 7 allow you to use the Black-Scholes formula to value a variety of simple options.²¹ In order to use the tables, follow these three steps:

- **Step 1:** Multiply the standard deviation of the proportionate changes in the asset's value by the square root of time to the option's expiration. For example, suppose that you wish to value a 4-year option on the stock of Wombat Corporation and that the standard deviation of the stock price changes is 40 percent per year.

$$\text{Standard deviation} \times \sqrt{\text{time}} = .40 \times \sqrt{4} = .80$$

- **Step 2:** Calculate the ratio of the asset value to the present value of the option's exercise price. For example, suppose that Wombat's stock price is currently \$140, that the option's exercise price is \$160, and that the interest rate is 12 percent. Then

$$\text{Asset value} = \frac{160}{(1.12)^4} = 1.4$$

- **Step 3:** Depending on whether the option is a call or a put, turn to Table 6 or 7 and look up the entry corresponding to the numbers that you calculated in Steps 1 and 2. For example, Table 6 shows that a four-year call option on Wombat stock would be worth 43.1 percent of the stock price or about \$60. Table 7 shows that a four-year put option would be worth 14.53 percent of the stock price or about \$20.

Example: Valuing a Put Option

James Bagwash is considering the sale of his company, United Bagwash, to World Enterprises (WE). To facilitate this sale, he is prepared to guarantee profits of at least \$10 million in each of the next 4 years. How much are these guarantees worth?

Notice that the guarantees are like a series of put options. Each year WE has the option to give Bagwash the actual profits in exchange for \$10 million. If profits exceed \$10 million, WE will keep the profits; if they are less than \$10 million, WE will receive the guaranteed amount of \$10 million.

When you value an option on a share, you need to know how much that share is currently worth. In the present case you wish to value four options, one for each year's profits. So your first task is to estimate the present value of each year's profits. Let us suppose that you forecast the profits as follows and then calculate their present value at a discount rate of 20 percent:

| YEAR | FORECAST PROFITS (MILLIONS) | PV (PROFITS) AT $r = .20$ (MILLIONS) |
|------|--------------------------------|--|
| 1 | \$ 8.5 | \$ 7.1 |
| 2 | 11.5 | 8.0 |
| 3 | 14.7 | 8.5 |
| 4 | 19.7 | 9.5 |

BEST AVAILABLE COPY

²¹ These tables are grouped with the present value tables at the back of the book.

Determining potential investment opportunities. A number of investment options over the track record of present value. Vladimir Anand will discuss options for investment.

This book provides a clear understanding of everyday decisions every year of experience implementing Copeland's flawed and opportunities. It is to consider the has over the Such options project if resulting down or out to be won.

There are chapters on types of simple expansion, more advanced switching options. Industries uses and discusses implementing real write an Excel combinations. Chapters 9 and tainties.

The analysis case solutions, problems providing insights into the authors also offer in the book, as to the would-it www.corpfinor

This book is printed on acid-free paper.

Copyright © 2001 by Thomas E. Copeland.

Published by

TEXERE LLC
55 East 52nd Street
New York, NY 10055

Tel: +1 (212) 317 5106
Fax: +1 (212) 317 5178
www.texere.com

UK subsidiary office

TEXERE Publishing Limited
71-77 Leadenhall Street
London EC3A 3DE

Tel: +44 (0)20 7204 3644
Fax: +44 (0)20 7208 6701
www.texere.co.uk

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to TEXERE LLC, 55 East 52nd St., 40th Floor, New York, NY 10055.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

Library of Congress Cataloging-in-Publication Data has been applied for.

ISBN: 1-58799-028-8

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

There have been and hundreds for a "how to can take off y theory to ever teen years of e our clients app our experience tool by more c

WHY READ I

The central pa present value, values every i pected future c illustrate a typ evaluating an f million to buil cash flows ove weighted avera the required ir not accept the

The NPV discussing, m: doned after th

This proves that we obtain the same value for the call option using either the risk-neutral approach or the replicating portfolio approach.

COMPARING REAL OPTIONS TO THE BLACK-SCHOLES APPROACH

The famous paper by Fischer Black and Myron Scholes (1973) for the first time, provided a closed-form solution for the equilibrium price of a call option. Although Black prematurely died of cancer, Scholes later won the Nobel prize in economics, along with Robert Merton, for their work.

The Black-Scholes model was the beginning of hundreds of papers that priced various types of options and empirically tested their predictions. It is important to remember the seven assumptions embedded in the Black-Scholes model to understand its limitations for use in real options analysis. The Black-Scholes model assumes:

1. The option may be exercised only at maturity—it is a European option.
2. There is only one source of uncertainty—rainbow options are ruled out (e.g., the interest rate is assumed to be constant).
3. The option is contingent on a single underlying risky asset; therefore, compound options are ruled out.
4. The underlying asset pays no dividends.
5. The current market price and the stochastic process followed by the underlying are known (observable).
6. The variance of return on the underlying is constant through time.
7. The exercise price is known and constant.

To be realistic, most real options problems require analysis that is capable of relaxing one or more of the standard Black-Scholes assumptions. For example, most investment decisions are compound options because they progress in phases, and there are usually several correlated sources of uncertainty. The need to be realistic will cause us to venture far from the Black-Scholes equation, which follows:

$$C_0 = S_0 N(d_1) - Xe^{-rT} N(d_2)$$

an
sh
sit
ho
act
int

out
had
Equ
prox
mat
the
num
estr
bills
piece
ing
se
from
lated

De
pote
mak
of li
over
pro
Vla
opti
for i
T
unc
ever
yes
imp
C
lay
poi
to
had
Su
pr
ing
ou
of
mi
m
ew
in
an
m
w
ce
C
ia
a
p
it
a
h
t
v

ing either

where: S_0 = The price of the underlying (e.g., a share of common stock)

$N(d_1)$ = The cumulative normal probability of unit normal variable d_1

$N(d_2)$ = The cumulative normal probability of unit normal variable d_2

X = The exercise price

T = The time to maturity

r_f = The risk-free rate

e = The base of natural logarithms, constant = 2.71828...

$$d_1 = \frac{\ln(S/X) + r_f T}{\sigma \sqrt{T}} + \frac{1}{2\sigma \sqrt{T}}$$

$$d_2 = d_1 - \sigma \sqrt{T}$$

1) for the price of a later won circuit work of papers predicted in real op-

European

ions are

there-

owed by

through

at is ca-

ptions.

because

prices of

om the

Today, many pocket calculators have Black-Scholes routines built in, and there are numerous personal computer applications. In Chapter 7, we show how a binomial model, which is based on discrete mathematics and simple algebra, approaches the Black-Scholes model as a limit. For now, however, let's work through a simple numerical example that shows exactly how to use the Black-Scholes model. After that, we will discuss the intuition behind the model.

Exhibit 4.11 provides data for Digital Equipment Co., that was taken out of the *Wall Street Journal* on October 4, during the late 1970s when it had not yet paid a dividend. For close-to-the-money calls on Digital Equipment, the assumptions of the Black-Scholes model are closely approximated. Therefore, we should be able to use it to give reasonable estimates of the price of the calls. Most of the necessary information to value the call is in Exhibit 4.11. The stock price, the exercise price, and the number of days to maturity are given for each option. The risk-free rate is estimated by using the average of the bid and ask quotes on U.S. Treasury bills of approximately the same maturity as the option. The only missing piece of information is the instantaneous variance of the stock (underlying security) rate of return. We shall use the implicit variance estimated from one call price in valuing the others. The implicit variance is calculated by simply using the actual call price and the four known exogenous

EXTENDING THE BINOMIAL APPROACH TO MANY TIME PERIODS

Continuing with our assumption of a multiplicative process, the general form of the payoff function, where T is the total number of periods, and n is the number of upward movements in the value of the underlying risky asset, may be written as

$$\text{MAX}\{0, u^n d^{T-n} V_0 - X\}$$

Using the expression for binomial probabilities that was developed earlier, the probability of each payoff is:

$$B(n|T, p) = \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n}$$

Multiplying the payoffs by the probabilities and summing across all possible payoffs, we have

$$C_0 = \left\{ \sum_{n=0}^T \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} \text{MAX}\{0, u^n d^{T-n} V_0 - X\} \right\} + (1+r_f)^T$$

Although this formula will suffice, we want to compare it with the Black-Scholes formula. To do so, we extend the analysis.

First, we note that many of the final payoffs will be zero because the option finishes out-of-the-money in many states of nature. Denote a as the positive integer that bounds those states of nature where the option has a nonnegative value. Then we can rewrite the general form of the binomial equation as follows:

$$C_0 = \left\{ \sum_{n=a}^T \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} \{u^n d^{T-n} V_0 - X\} \right\} + (1+r_f)^T$$

All of the states of nature where $n < a$ have zero payoffs because the call option will not be exercised. Next, we separate the equation into two parts:

$$C_0 = V_0 \left[\sum_{n=a}^T \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} \frac{u^n d^{T-n}}{(1+r_f)^T} \right] - X(1+r_f)^{-T} \left[\sum_{n=a}^T \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} \right]$$

The second bracketed expression is the discounted exercise price, $X(1+r_f)^{-T}$, multiplied by what is called the complementary binomial distribution, $B(n \geq a | T, p)$. It is the cumulative probability of having an in-the-money option (i.e. where $n \geq a$) where the probabilities are the certainty-equivalent probabilities determined by the risk-free hedge portfolio. For example, if we go back to Exhibit 7.2 as a starting point, and let V_0 equal \$100, let $u = 1.5$ (i.e., 150% per year), the exercise price be \$250, the life of the option be seven periods, and the annual risk-free rate equal 10 percent, we have the parameters of Exhibit 7.6. There are eight end states. The number of up movements ranges from zero to seven. Given an exercise price of \$250, the option is in the money only for the three uppermost states where n , the number of up movements, is 5, 6, or 7. Therefore, the value of the border state, state a , is 5. The risk-neutral probability is $p = (1.1 - .667)/(1.5 - .667) = .52$. The complementary binomial probability is the cumulative probability (based on risk-neutral probabilities) of finishing in-the-money, namely 26 percent. This is the probability that the exercise price will be paid. Therefore, the value of the second term in the binomial formula is

$$X(1+r_f)^{-T} B(n \geq a | T, p) = 250(1.10)^{-7} (.260668) = \$33.44$$

The first term in the binomial option pricing model is the current value of the underlying risky asset, $V_0 = \$100$, multiplied by another complementary binomial probability that is equal to one over the hedge ratio of options to the underlying that is necessary to form a riskless portfolio consisting of one unit of the underlying and m call options. To estimate the complementary probability to be used in the first term, we let

$$p' = \left[\frac{u}{(1+r_f)} \right] p$$

Exhibit 7.6 Seven-period binomial example.

Parameters: $V_0 = \$100$
 $u = 1.5, d = 1/1.5 = .667$
 $r_f = 10\%$

and

$$1 - p' = \left[\frac{d}{(1+r_f)} \right] (1-p)$$

We then can reduce the probability function in the first term as follows:

$$p^n (1-p)^{T-n} \frac{u^n d^{T-n}}{(1+r_f)^T} = \left[\frac{u}{(1+r_f)} p \right]^n \left[\frac{d}{(1+r_f)} (1-p) \right]^{T-n} = (p')^n (1-p')^{T-n}$$

Having made this transition, the binomial model for pricing a European call option (with a multiplicative stochastic process) can be summarized as follows:

$$C_0 = V_0 B(n \geq a | T, p') - X(1+r_f) B(n \geq a | T, p)$$

where

$$p = \frac{(1+r_f) - d}{u - d}$$

$$p' = \left[\frac{u}{1+r_f} \right] p$$

$a \equiv$ The smallest nonnegative integer greater than $\ln(X/V_0 d^a) / \ln(u/d)$
 $B(n \geq a | T, p) =$ The complementary binomial probability that $n \geq a$

Now we can finish the numerical example in Exhibit 7.6 by calculating the complementary binomial probability in the first term of the equation:

$$p' = \left[\frac{u}{1+r_f} \right] p = \left(\frac{1.5}{1.1} \right) .52 = .7091$$

and

$$1 - p' = \left[\frac{d}{(1+r_f)} \right] (1-p) = \left(\frac{.667}{1.1} \right) (1-.52) = .2909$$

The last column in Exhibit 7.6 shows the distribution of probabilities in the seventh time period. The value of the complementary binomial probability $B(n \geq 6 | 7, .7091)$ is .6676. Therefore, the value of the option, using a binomial approach for 7 time periods is

$$C_0 = V_0 B(n \geq a | T, p) - X(1+r_f)^{-T} B(n \geq a | T, p) = \$100(.6676) - \$250(1.1)^{-7} (.2606) = \$66.75 - \$33.44 = \$33.32$$

In the next section, we divide each annual time period into an infinite number of subintervals and show that the result equals the Black-Scholes formula.

THE LIMIT OF THE BINOMIAL OPTION PRICING MODEL IS THE BLACK-SCHOLES FORMULA

The binomial formula can be extended to a continuous time form by dividing its life, T years, into more and more subintervals, n , until n approaches infinity. Both models are written below for the purpose of comparison. First, the Black-Scholes model:

$$C_0 = V_0 N(d_1) - Xe^{-r_f T} N(d_2)$$

where

$$d_1 = \frac{\ln\left(\frac{V_0}{X}\right) + r_f T}{\sigma \sqrt{T}} + \frac{1}{2} \sigma \sqrt{T}$$

$$d_2 = d_1 - \sigma \sqrt{T}$$

And then the binomial model:

$$C_0 = V_0 B(n \geq a | T, p) - X(1+r_f)^{-T} B(n \geq a | T, p')$$

where

$$p = \frac{(1+r_f) - d}{u - d}$$

$$p' = \frac{u}{1+r_f}$$

follows:

y^{T-a}

European
American

$n(u/d) \geq a$

calculation
of the

The correspondence between discrete and continuous compounding of the risk-free rate is fairly straightforward. If we define r_f as the annual rate of return and j as the rate that is compounded n times in interval T , defined as the number of years to maturity then

$$\lim_{n \rightarrow \infty} \left(1 + \frac{j}{n/T}\right)^{nT} = e^j = (1 + r_f)$$

The Black-Scholes model. The call option price is given by

Cox, Ross, and Rubinstein (1979) derive a relationship that allows us to convert between the up and down movements in a binomial lattice and the annual instantaneous standard deviation of the rate of return on the underlying risky asset. Their results are

$$u = e^{\sigma\sqrt{T/n}}$$

$$d = e^{-\sigma\sqrt{T/n}}$$

Next we estimate the normal distribution of the underlying asset price.

Next, if we compare the binomial and Black-Scholes models, we need to compare the cumulative normal probability terms with the complementary binomial probability terms. The terms converge in the limit, as the number of lattice nodes per time period becomes large. Mathematically,

$$B(n \geq a | T, p') \rightarrow N(d_1)$$

$$B(n \geq a | T, p) \rightarrow N(d_2)$$

Thus, in the limit, the binomial model approaches the Black-Scholes model. We will demonstrate this result in the next section as we build an Excel spreadsheet using the binomial model, and allow the number of steps per year to become larger and larger. However, first we find the value of the same call option using the Black-Scholes formula as applied to the seven-period example in Exhibit 7.6. First, we need to find the standard deviation, σ , that corresponds to the up and down movements in our binomial tree. Our example has 7 years ($T=7$) and seven subintervals ($n=7$), therefore,

Finally, substitute the value of d_1 and d_2 into the Black-Scholes formula to find the call option price.

$$u = e^{\sigma\sqrt{\pi n}}$$

$$\ln(u) = \sigma\sqrt{\frac{T}{n}} = \sigma\sqrt{7+7}$$

$$\sigma = \ln(u) = \ln(1.5) = .4055$$

The Black-Scholes formula calls for a continuously compounded risk-free rate. The conversion is

$$1 + r_f = e^j$$

$$\ln(1.1) = j$$

$$j = .0953$$

Next we estimate the unit normal values, d_1 and d_2 , as well as the cumulative normal densities $N(d_1)$ and $N(d_2)$:

$$d_1 = \frac{\ln\left(\frac{V}{X}\right) + r_f T}{\sigma\sqrt{T}} + \frac{1}{2}\sigma\sqrt{T}$$

$$= \frac{\ln\left(\frac{100}{250}\right) + .0953(7)}{.4055\sqrt{7}} + \frac{1}{2}(.4055\sqrt{7})$$

$$= \frac{-.9163 + .6672}{.4055(2.646)} + .5(.53638)$$

$$= \frac{-.2491}{1.0728} + .53638 = .3042$$

$$N(d_1) = .5 - .1195 = .6195$$

$$d_2 = d_1 - \sigma\sqrt{T} = .3042 - .4055\sqrt{7} = -.7686$$

$$N(d_2) = .5 - .27894 = .22106$$

Finally, substituting these values into the Black-Scholes model, we find the value of the option:

$$C_0 = VN(d_1) - Xe^{-rT}N(d_2) = 100(.61950) - 250e^{-.08(7)}(.22106) = 61.95 - 250(.5132)(.22106) = 61.95 - 28.36 = 33.59$$

The value obtained using the binomial model was \$33.32, an error of only seven cents, or 0.2 percent. In the next section, we show that by increasing the number of periods per year we can reduce the error to zero.

BUILDING A SPREADSHEET MODEL OF A BINOMIAL TREE (EVENT TREE)

Now let's build a binomial tree on an Excel spreadsheet. There will be three sections to the spreadsheet. Input data and model parameters calculated from it compose the first section. We need to know the current value of the underlying (the present value of the project without flexibility), the exercise price, the life of the option in years, the annual risk-free rate, and the number of steps per year. From these, we calculate the up and down movements per step, the risk-free rate per step, and the risk-neutral probabilities (which, strictly speaking, are not needed for the event tree). Exhibit 7.7 provides some values for these parameters that we will use in a numerical example.

Exhibit 7.7 Input and calculated parameters.

| Input Parameters | | Calculated Parameters |
|---------------------------------|--------|---|
| Present value of the underlying | \$100 | up $u = \exp(\sigma\sqrt{T}) = \exp(.4055)\sqrt{1/1} = 1.5$ |
| Exercise price | \$250 | down $d = 1/u = .6667$ |
| Life of the option (in years) | 7 | |
| Annual risk-free rate | 0.10 | risk-neutral prob. $= (1 + r_f - d)/(u - d) = 0.52$ |
| Standard deviation of return | 40.55% | down state risk-neutral prob. $1 - p = 0.48$ |
| Number of steps per year | 1 | |

st
N
E
th
N
qt
ca

see
bui
cell
I11
up
cop
the
B12

Exhi

| | |
|----|--|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |
| 12 | |
| 13 | |
| 14 | |
| 15 | |
| 16 | |
| 17 | |
| 18 | |
| 19 | |

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

COLOR OR BLACK AND WHITE

UNREADABLE TEXT OR DRAWINGS

SKEWED/SIANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GREY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

An Assessment of Pricing Mechanisms for the Internet—A Regulatory Imperative

Mitrabarun Sarkar

Presented at MIT Workshop on Internet Economics March 1995

1 Introduction

This paper argues that however much of an anathema the notion of regulating the Internet may be, there is a strong need to start putting the appropriate regulatory structures in place as the commercialized Internet moves incrementally towards a usage-based pricing system. Various factors such as new bandwidth-hungry applications; the massification of the net; the concerted entry of the telephone, cable, and software companies; and the proliferation of electronic commerce all imply unimaginable potential growth rates for the Internet and a resultant scarcity of bandwidth, thus making it imperative to put a pricing system in place that would effectively ration scarce bandwidth.

As has been argued by many, a usage-based pricing system seems to be an innovative way to effectively ration scarce bandwidth. In this context, this paper examines the Precedence and the Smart Market models of Internet pricing. We note that (a) the perceived homogeneity of the Internet's load, and (b) the threat of market-power abuse through artificial creation of a high network load by those who control the bottleneck facilities, remain the fundamental weaknesses of usage-based pricing. However, given that usage-based pricing is inevitable, and that the Smart Market mechanism does present an innovative and a potential solution, it is important to consider the appropriate safeguards that need to be put in place. In this context, the paper argues that a usage based, free market pricing system needs to be combined with some form of regulatory oversight to protect against anti-competitive actions by the firms controlling the bottleneck facilities and to ensure non-discriminatory access to emerging networks.

2 The Different Dimensions of Growth

The Internet, which has hitherto been restricted as a resource for high level researchers and academics, is "expanding to encompass an untold number of users from the business, lower-level government, education, and residential sectors" (Bemier, 1994, p. 40). Studies done by Merit Network Inc. (1) indicate that the Internet has grown from 217 networks in July 1988 to 32,370 networks in May 1994. The number of hosts have increased from 1,000 to over two million over the same period, with about 640,000 of these located at educational sites, 520,000 at commercial sites, 220,000 at governmental sites, and the remaining 700,000 at non-US locations. Traffic over the NSFNET backbone increased by 10 times in three years, from 1.268 billion bytes in March 1991 to 12.187 billion bytes in May 1994. The traffic history of packets sent over the NSFNET shows similar exponential growth trends. As against 152 million packets in July 1988, 60,205 million packets of information were sent over the system in May 1994; an increase of almost 400 times. (2)

These stunning growth figures are just a precursor to the boom in Internet traffic that is expected to take place in the near future. As will be laid out in this paper, a set of factors in combination are threatening to dwarf even these exponential growth rates in the near future.

3 The Causal Model of Internet Congestion

As illustrated in the chart, a set of forces working together are threatening to create unprecedented levels of congestion on the Internet. It is argued that three main factors—incompatibility of the newer applications with the Internet's architecture, massification of the Internet, and privatization and concomitant commercialization of the Internet—are responsible for an inherent change in the Internet's dynamics, thus mandating a reexamination of the economic system that surrounds the Internet.

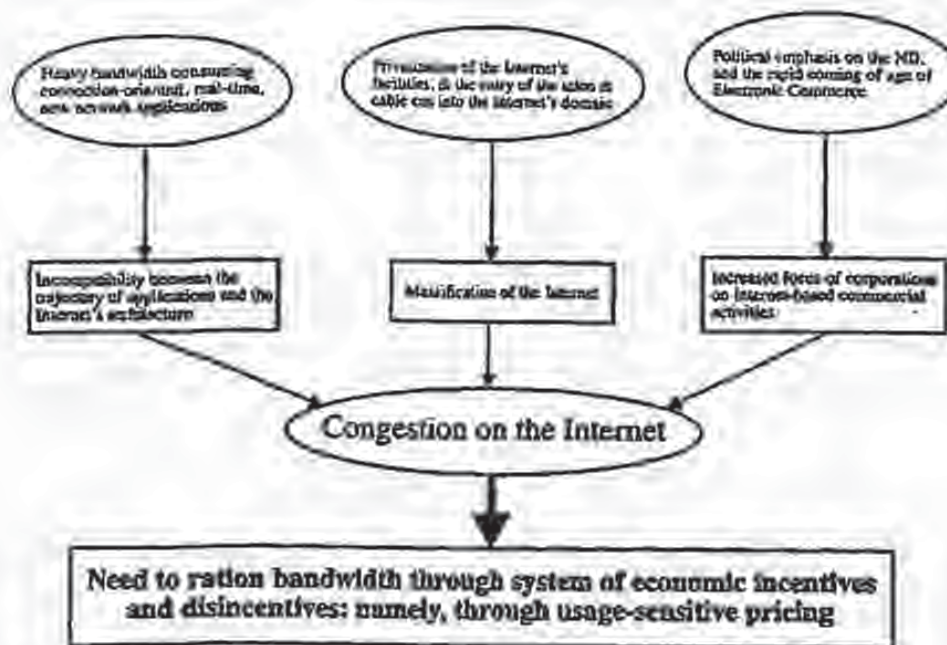


Figure 1

3.1 Incompatibility Issues

New network applications are all tending to require heavy bandwidth in near-real time. As Bohn et al. note, "one may argue that the impact of the new, specifically real-time, applications will be disastrous: their high bandwidth, duration requirements are so fundamentally at odds with the Internet architecture, that attempting to adapt the Internet service model to their needs may be a sure way to doom the infrastructure" (p. 3).

Their technical characteristics and, consequently, their demand on the network are very different from the more conventional, traditional electronic communication and data transfer applications for which the Internet has been designed. (3) While conventional electronic communication is typically spread across a large number of users, each with small network resource requirements, newer applications such as those with real-time video and audio require data transfers involving a continuous bit stream for an extended period of time, along with network guarantees regarding end-to-end reliability. Even though the data-carrying capacity of the networks is constantly being enhanced through upgrades in transmission capacity and switching technology, current developments in communication software, especially those related to multimedia, are creating network applications that can consume as much bandwidth as network providers can supply (Bohn, Braun, Claffy, & Wolff, 1994).

Multimedia Netscape applications, Internet fax, and Internet radio are becoming large users of resources (Love, 1994). Russell (1993) reports that while only 2.4 kbps are required for communication of compressed sound, 3840 kbps are required for CD quality stereo sound. Real-time video needs bandwidth ranging from 288 kbps to 2000 kbps, while studio quality non-real time video could require up to 4000 Kbps. HDTV requirements range from 60,000 to 120,000 Kbps. (4) Bohn et al. (1994) report that many videoconferencing applications require 125 kbps to 1 Mbps. Although compression techniques are being developed, the requirements are still substantial. CUSErMe, developed at Cornell University uses compression, yet its requirements are in the region of 100 kbps.

In essence, the trend is towards applications that are, first, heavy bandwidth consumers and second, require near real-time transmission—both characteristics that are essentially incompatible with the inherent architecture of the Internet.

3.2 Privatization, Commercialization, and Massification

Simultaneously, we are witnessing a privatization of the Internet's facilities, increasing commercialization of the net, and a political agenda promoting the rapid deployment of the NII. All these are resulting in a massification of the Internet, as it becomes easier to get "wired" in. The bottom line implication is that the demand for bandwidth is possibly rising beyond current levels of supply.

Prior to 1991, the net's physical infrastructure was government-owned and operated. On December 23, 1992, the NSF announced that it will cease funding the ANS TS backbone in the near future. The Clinton Administration's thrust on private-sector investment in the NII implies that very soon, possibly by 1996, the Internet's facilities will be largely privatized. In 1994, the NSF announced that the developing architecture of the Internet would utilize four new Network Access Points (NAPS), and the contracts for operating them were awarded to Ameritech, PacBell, MFS, and Sprint. In addition, MCI has been selected to operate the Internet's new very high speed backbone (vBNS).

The traditional telecommunication companies operating in a nearly saturated and increasingly competitive domestic market, are turning their focus towards advanced data services, a market where the "number of data relationships is growing at more than four times the number of voice relationships" (Campbell, 1994, p. 28). Spurred on by the promise of the NII, a variety of communication companies are getting into the act. "[T]elephone companies, cable companies, information service companies, television networks, film studios, and major and software vendors are all maneuvering to ensure that they are positioned to profit from the NII in general and the Internet in particular" (Business Editors, 1994).

Of all these players, the telephone, software, and cable companies are in a position to strongly affect one critical aspect of market accessibility. User-friendly software, enhanced services, and marketing skills are together likely to have a dual effect: one, allow computer literate users who have been to date outside the periphery of the net the opportunity to connect, and two, drive the development of user-friendly tools of navigation, which would have a multiplier effect on both network usage and the number of people who would be able to navigate through the Internet effectively and access desired information bases productively.

Bernier (1994) reports that the telephone and the cable companies have already rolled out their plans for the Internet. In March 1994, AT&T announced a national InterSpan frame relay service and Internet Connectivity options, both dial-up methods for accessing the Internet. MCI offers access over its frame relay services. Sprint, which offers a nationwide Internet access service along with providing international Internet connections, is now offering ATM access to the net. Several Bell regional companies are getting into the act. US West offers end users access to two Internet providers via its frame relay services. Pacific Bell in collaboration with InterNex Information Services, now offers Internet connections, while Ameritech has won a contract to be one of the four Network Access Providers. They plan to offer Internet protocol pipes over their frame relay, switched multi-megabit data service. Many cable operators are also getting into the market. Continental Cablevision and Jones Intercable are using cable modems hooked onto their coaxial lines to bring broadband Internet connections to businesses and homes. Continental, a Boston-based cable company, launched a service in March in collaboration with Performance Systems International, the national Internet access providers, to bring high bandwidth service to residences and businesses in Boston. (5)

The bottom line implication is that the number of Internet users is going to increase manifold, as opportunities to interconnect with the network become ubiquitous through the efforts of the telephone, software, and cable companies, and as user-friendliness and utility of the applications develop further.

4 Implications & Key Issues

The implication of these forces--the incompatibility of the new bandwidth hungry applications, infusion of new users, and the privatized and commercialized nature of the Internet--is that the demand on network resources will increase exponentially, and will possibly be much more than the supply of bandwidth. As network resources become scarcer and as the system is driven towards a free-market model, resource rationing through a change in the pricing system is inevitable.

The key issue is that the pricing mechanism should be able to (a) preserve the inherent discursive nature of the net, (b) send the right signals to the marketplace, and also (c) be flexible and adaptive to changes brought about through technology, political initiatives, and software development.

4.1 Pricing Alternatives

The major fear in some quarters is that the present system of flat-rate, predictable pricing for a fixed bandwidth connection will be replaced by some form of vendor preferred, usage-based metered pricing. Users feel that the Internet should continue

to function primarily as a vast, on-line public library from where they can retrieve virtually any kind of information at minimal costs.

According to some, a transition to metered usage would make the NII "like a Tokyo taxi, so that for every passenger who takes a ride on the national data superhighway, the first click of the meter will induce severe economic pain and the pain will increase with each passing minute" (Judith Rosell, International Data Corporation's Research Director quoted in *Business Editors*, 1994).

Consumer advocacy groups opposing metered pricing usage of the Internet (6) feel that the NSF should create a consumer advisory board to help set pricing and other policies for the network to ensure that the free-flow of information and democratic discourse through Internet listserver and fileservers sites is preserved and enhanced. In addition to the fear that a popular discussion would have to pay enormous amounts to send messages to its members, it is feared that usage based pricing would introduce a wide range of problems regarding the use of ftp, gopher, and mosaic servers, since the providers of the "free" information would be liable to pay, at a metered rate, the costs of sending the data to those who request for it. This would have a negative effect on such information sites, and would eliminate many such sources of free information.

In essence, the argument is that usage based pricing would imply severe economic disincentives to both users and providers of "free" information, and would therefore destroy the essentially democratic nature of the Internet.

4.2 The Arguments against Flat-rate Pricing

The paper argues that flat-rate pricing in the current context of the Internet is likely to run into severe problems. Paradoxical as it may sound, the continuance of flat rate pricing is likely to severely impair the current discursive nature of the Internet.

The basic role of a pricing mechanism is to lead to an optimal allocation of scarce resources, and to give proper signals for future investments. The mechanism in place should lead to the optimization of social benefits by ensuring that scarce resources are utilized in such a manner as to maximize productivity in ways society thinks fit. As Mitchell (1989) notes, "in a market economy, prices are the primary instrument for allocating scarce resources to their highest valued uses and promoting efficient production of goods and services" (p. 195). One critical issue however is the basis on which an appropriate pricing scheme can be designed.

Given that the marginal cost of sending an additional packet of information over the network is virtually zero once the transmission and switching infrastructures are in place, marginal cost pricing in its simplistic form is inapplicable. Cost-based return on investment (ROI) pricing is both not feasible, given the multiplicity of providers who would have to chip in to bring about an end-to-end service, and inefficient, given the chronic problem of allocating joint costs. (7) A "what the market can bear" policy would be likely to have unforeseen implications, especially if the markets are not competitive in each and every segment of the network.

The principle that is most likely to be effective in this scenario is a modified version of the marginal cost approach, where the social costs imposed by the scarcity of bandwidth-- the bottleneck resource--is taken into consideration. Bandwidth being the speed at which data is transmitted through its networks, its scarcity implies delays due to network congestion. This then is the social cost that needs to be incorporated into any efficient pricing scheme.

4.3 The Costs of Congestion

The packet-switching technology of the TCP/IP protocol embedded in the Internet has an essential vulnerability to congestion. A single user, overloading a sub-regional line that connects to the regional level network, can overload several nodes and trunks, and cause delays or even data loss due to cell or frame discarding for other users. The specific manner in which the problem manifests itself depends on the protocols used, and on whether the network is simply delaying or actually discarding the information (Campbell, 1994). Since backbone services are currently allocated on the basis of randomization and first-come-first-served principle, users now pay the costs of congestion through delays and lost packets (Varian & MacKie-Mason, 1994). (8) The problem is likely to become even worse as Power PCs such as a \$2000 Macintosh AV combined with a \$500 camcorder would enable an undergraduate to send real-time video to friends on another continent, by pumping out up to 1 megabyte of data per second onto the Internet, thus tying up a T1 line (Bohn et al., Love).

The cost of congestion on the Internet is therefore a tangible problem, and not merely the pessimistic outpourings of a band of dystopians. Some have argued that it does not matter if users fill up their leased line, and even less the manner in which they do so (Terney, *telecomreg*, 4 May 1994, 18:42:09). However, the Internet is not designed to allow just users to fill their

(taxes at the same time. Also, as new applications such as desktop videoconferencing and new transport services such as virtual circuit resource reservation come in, it will become more and more necessary for the network to provide dedicated and guaranteed resources for these applications to operate effectively (England, *telecomreg*, 7 May, 1994 08:04:26). In the Internet system, which is essentially designed for connectionless network services, the requirement of bandwidth reservation implies that an incompatible class of service needs to be provided over it, thus necessitating costs in developing added functionality to its edges (Pecker), and in decreasing its overall efficiency.

In essence, the changing nature of network traffic implies a social cost, largely due to this inherent incompatibility between new applications and the Internet architecture. There is a social cost imposed by those who are making unlimited use of the newer bandwidth-hungry, incompatible applications. This cost is being borne by others in the form of delays and data dropouts while making use of the more traditional applications such as email, ftp, and gopher. (9) The flat-rate pricing mechanism is therefore inefficient in sending out corrective signals to minimize social costs and as a resource allocator since it can hardly be argued that the social benefits of a democratic discourse are less beneficial to society than an undergraduate sending out real-time video to his friends. (10)

There is a potential danger here. Continuance of the current pricing system may result in a situation where the new applications drive out traditional uses. The inherent bias of flat-rate pricing, whereby heavy users are subsidized by light users, is a threat to the more traditional forms of net usage as applications requiring heavy bandwidth are coming of age. It is however clear that a new form of pricing scheme needs to be developed in order to ensure that the net retains part of its original character as it evolves into a more potent and futuristic medium of communication.

4.4 The Pricing Options

At the far end of the spectrum is pure usage-based pricing. Given the shortfalls of the flat-rate based scheme, it seems certain that there will eventually be "prices for Internet usage, and the only real uncertainty will be which pricing system is used" (Love).

4.4.1 The Telephone Pricing Model

One form of usage based pricing would be to use the system of posted prices as in telephony. One way to do this would be to adopt the telephone model of computing interLATA prices, where the cost of Internet usage is based on the distance between the sender and the receiver, and on the number of nodes through which data need to travel before they reach their destination. This however would be difficult to implement given the inherent nature of the connectionless net technology, which is based on redundancy and reliability, where packets are routed by a dynamic process through an algorithm that balances load on the network, while giving each packet alternative routes should some links fail (Varian & MacKie-Mason, 1993, p. 3). The associated accounting problems are also enormous. In addition, the sender would prefer that packets are routed through a minimum number of nodes in order to minimize costs, while the algorithm in the Internet would base its calculations on the concept of redundancy and reliability, and not necessarily on the fewest links or the lowest costs.

The telephone model of pricing is not likely to work for another reason. Posted prices are not flexible enough to indicate the state of congestion of the network at any given moment (Varian & MacKie-Mason, 1993, p. 19). As we have seen earlier, congestion in the network can peak from an average load very quickly depending on the kind of application being used. Also, time-of-day pricing means that unused capacity at any given moment cannot be made available at a lower price whereby it would be beneficial to some other users. Conversely, at moments of congestion, the network stands to lose revenue because users who are willing to pay higher amounts than posted rates are being crowded out of the network through the randomized first-in-first-out (FIFO) process of network resource allocation.

In essence, the system of posted fixed prices implies multiple problems: while it does not allow for revenue maximization under the "market can bear" philosophy or lead to optimal capacity utilization, it also does not address the social costs of congestion because it cannot allow for prioritization of packets. It is thus clear that the answer to the Internet's pricing problem does not lie at either ends of the pricing spectrum defined by flat-rate pricing and pure usage based pricing, but possibly in an innovative approach.

4.4.2 Innovative Pricing Models

Two innovative pricing schemes have been suggested recently. Bolin et al. have proposed the "Precedence" model, while Varian & MacKie-Mason have developed the "Smart Market" mechanism.

4.4.2.1 The Precedence Model

<http://www.press.umich.edu/jep/works/SarkAssess.html>

3/12/01

The Precedence model proposes "a strategy for the existing Internet, not to support new real-time multi-media applications, but rather to shield ... the existing environment from applications and users whose behavior conflicts with the nature of resource sharing" (Bohn et al., p. 4). The authors propose that criteria be set to determine the priority of different applications, which will then be reflected in the IP precedence field of the different data packets. Packets would receive network priority based on their precedence numbers. In the event of congestion, rather than rely on the current randomized decision, the Precedence model presents a logical basis for deciding which packets to send first and which to hold up or drop. While noting that their proposed system is vulnerable to users tinkering with precedence fields, the authors feel that this approach would "gear the community toward the use of multiple service levels, which ... (is) the essential architectural objective" (p. 10).

However, this model has some inherent weaknesses. Given that the Precedence model rests on priority allocation of packets, the central issue is how these priorities will be set and who will set them. There seems to be an inherent assumption of an increased governmental role in regulating content, and as Varian and MacKie-Mason point out, "Soviet experience shows that allowing bureaucrats to decide whether work shoes or designer jeans are more valuable is a deeply flawed mechanism" (1994, p. 16).

The system would also require continuous updating of the priority schemes as newer products and applications become available. Real time video may be assigned a lower priority than ftp, but it is possible that the video transfer of data is concerned with an emergent medical situation. Application-based priority will be limiting, and it would not be possible to define each and every usage situation in a dynamic environment.

Also, the model relies heavily on the altruism of net users, and the correct reporting and non-tinkering with precedence fields by computer-savvy netters. The continuing survival of such a system is at odds with current social trends.

4.4.2 The Smart Market Mechanism

Proposing the Smart Market mechanism as a possible model to price Internet usage, Varian & MacKie-Mason (1994) suggest a dynamic bidding system whereby the price of sending a packet varies minute-by-minute to reflect the current degree of network congestion. Each packet would have a "bid" field in its header wherein the user would indicate how much he is willing to pay. Packets with higher bids would gain access to the network sooner than those with lower bids, in the event of congestion. The authors acknowledge that this mechanism is preliminary and tentative and is only one approach to implementing efficient congestion control; moreover, it would only ensure relative priority without being an absolute promise of service.

The Smart Market mechanism has great theoretical potential as a basis for implementing usage-based pricing. By charging for priority routing during times of congestion, traffic that does not claim priority status, such as a large Internet mailing list or a listserve conference, would travel for free during off-peak hours. During congestion, users would bid for access and routers would give priority to packets with the highest bids. A great deal of consensus will be required along the network for smooth functioning and to ensure that priority packets are not held up.

Users will be billed the lowest price acceptable under the routing "auction," and not necessarily the price that they have indicated as their bid. A user would thus pay the lower amount between his bid and the bid of the marginal user, which will be necessarily lower than the bids of all admitted packets. As a result, the Varian and MacKie-Mason model ensures that while everyone would have the incentive to reveal his or her true willingness to pay, there are systematic incentives to conserve an scarce bandwidth while simultaneously allowing effectively free services to continue.

5 Discussion: Building a Case for Regulation

We argue that although the dynamic bidding mechanism is very attractive as a theoretical basis for pricing usage, it renders the system wide open to potential abuse by those who control the system bottlenecks. A case is therefore made for establishing some form of regulatory oversight to ensure against anti-competitive activities and abuse of market power. In essence, this paper argues that a usage-based pricing scheme needs to be combined with some form of regulatory oversight that aims at making the access of emerging networks to the Internet open and nondiscriminatory, and that the firms which control the bottleneck facilities in the emerging structure do not indulge in anti-competitive behavior. (11)

Interestingly, in the Internet debate, we seem to have lost sight of the fact that dynamic pricing of network services has been advanced and debated earlier. The notion of dynamic rates for pricing network services as a mechanism to balance loads, limit congestion, and avoid the high costs of adding capacity, has been advanced in the past (Mitchell). Vickrey (1981) proposed that telephone networks could manage their congestion during peak-load times by alerting subscribers through a

higher pitched dialing tone and charging premium rates for calls made at those times. Mitchell notes that as the local networks of telephone systems evolve into broadband systems and become even more capital-intensive, the gains from allocating capacity dynamically on demand will be larger. Dynamic pricing would enable higher overall use of network capacity, while allowing price-sensitive users to access telephone services at lower prices on a dynamic and daily basis.

5.1 The Weakness of the Dynamic Bidding Model

The essential weakness of the Smart Market proposal as a stand-alone, free market pricing system that does not need any regulatory oversight for its proper implementation lies in its assumptions, summarized below.

5.1.1 Perceived Homogeneity

First, the model proposes to price the scarce network resource based on the perceived network load. *Prima facie*, it seems that a uniform load factor is presumed across all points of the network on which basis bandwidth is priced. However, this is simply not true. The Internet is not a homogeneous network. The load factor and the resultant level of congestion is going to be very different along the different nodes/switches/lines between the sender and the receiver.

It may be argued that the price of sending a message can be based on the most congested point of the network. However, the path that a packet will take cannot be predicted with any degree of certainty. It is thus close to impossible to base pricing on an algorithm related to the network load at the most congested point of the network along the path that the packets have to traverse in order to be able to reach their destination.

Also, network load is unpredictable, and is prone to sudden peaks and troughs. It is entirely possible that the load at a particular node changes rapidly and the bid is simply not good enough to receive priority from that node at that moment, even though it might have been so earlier. It may be argued that through consensus a system could evolve where "regional" congestion is calculable, and the price determined on the basis of an algorithm that considers all possible routings and all possible levels of network loads. However, given the diversity of the Internet and the multiple levels of players, this sounds extremely far-fetched and difficult to achieve without any neutral, oversight agency.

5.1.2 Manipulation of network load

Second, and more importantly, a pricing system based on network load opens itself up to potential abuse by those who control the facilities at the system bottlenecks. It may be argued that any system would be vulnerable to abuse, but the anonymity of data transferred along the Internet would make this system especially vulnerable: for example, unscrupulous firms in control of the various nodes would have both the incentive and ability to manipulate the network load to keep it artificially high so as to create an upward pressure on the price of network usage. Given that marginal costs are almost zero, the firm would attempt to maximize revenue. It can do this by tracking network usage and artificially keeping the network load at a point where overall revenue realization is maximized.

The system is therefore open to abuse by bottleneck-controlling firms who peg the network load at high levels in order to maximize revenue, thereby manipulating the price of network usage upwards. For the system to operate fairly and efficiently, there would either have to be no motivation for exploitation of market power, or a strict system of controls against abuse.

5.2 Internet Pricing: A Case for Regulation

These two issues—the perceived homogeneity and the possibility of manipulation—are the fundamental reasons why the Market mechanism, or any variation of it, needs to be combined with an institutional form that is responsible for (a) consensus-building, and (b) ensuring against manipulation, anti-competitive behavior, and abuse of market power. Given the experience of the telecommunication industries, it should be amply clear that there is an essential contradiction in free market operations. The greater the degree of freedom, the greater becomes the role for regulation. (12) Taking the example of the telephone industry, it should be clear that potential bottlenecks and potential for abuse need to be considered well in advance so that necessary safeguards may be put in place.

It is important to address the control of bottlenecks and their role in influencing the pricing mechanism. Although an oversight agency could, hypothetically, ensure that the consumer surplus (13) generated is not collected as excess profits by the firms and is returned to consumers (MacKie-Mason, 1994 (14)), it is more desirable to design a system wherein the transfer of excess funds does not happen in the first place. While it is true that competition is the best form of regulation, the privatization of the Internet's facilities and the emergence of the NAPs indicate that the owners of the underlying trunks and

access paths (the Regional Bell Operating Companies, the Inter Exchange Carriers, and the CAPs) are likely to have more market power than any private organization has had over the Internet to date.

Whether one envisions Internet carriage emerging as a competitive industry or one that is effectively oligopolistic, there seems to be a role for regulatory agencies. There is a need to regulate pricing and control anti-competitive behavior in the event that the industry is less than competitive. On the other hand, even if the system is highly competitive, the dynamics of network pricing need to be implemented by some form of nonprofit consortium or by a public agency to ensure consumer protection on the one hand, and coordination and consensus among the different service providers on the other. In the of such consensus building activities and an imperfect market situation, dynamic pricing is likely to have a chaotic effect where the cost of accounting and regulatory oversight is extremely high. This might have an undesirable effect on the implementation of such a scheme in the first place.

Some may argue that in the event a purely competitive situation emerges, then it does not matter what form of pricing scheme emerges (Bohn, 1994 (15)). But this overlooks the fact that every pricing schemes has its own inherent bias and different levels and kinds of associated social benefits.

An added factor that needs to be assessed is law technology is expected to develop over time. Similar to pricing schemes, every technology also has its own bias. Since technological development is likely to be unbalanced, and breakthroughs can be expected to be sporadic both in terms of time and space, the pricing schemes that are implemented need to be accordingly tailored to reflect or obviate the effects of technological imbalances.

For example, transmission technology, which is dependent on fiber-optics, is slated to develop much faster than switching technology, which is currently electronic based. Should the expectation be that switching technology will develop quickly and fiber-optic technology implemented, the fear of congestion at the nodes will no longer be a valid one. The bottleneck will then change back to the transmission lines, not in terms of the physical capacity of the fiber optic trunk lines, but in the costs associated with overlaying all user lines, especially the last loop that connects the customers premises to the nearest switch.

In all likelihood, the market is going to be transformed in an incremental manner. Initially, some form of usage-based pricing, possibly dynamic pricing, may be combined with flat-rate pricing. For applications that require resource reservation, usage-based pricing would be necessary to control their proliferation and to ensure network performance. For more traditional forms of net usage, such as email, flat-rate access would continue to be the norm. In other words, the pricing system that is likely to evolve would move the industry towards multiple service levels. While it would be difficult to predict the exact form of pricing that will emerge, it seems clear that there will be a role for oversight agencies and regulators as the Internet evolves.

References

- Bernier, P. (1994). Opportunities abound on the Internet. *Telephony*, 226(13).
- Bohn, R. (20:35:25, 2 June 1994). Future Internet pricing. Posting on telecomreg@relay.adp.wisc.edu.
- Bohn, R., Braun, H.-W., Claffy, K. C., & Wolff, S. (1994). Mitigating the coming Internet crunch: Multiple service levels via Precedence. Tech rep., UCSD, San Diego Supercomputer Center, and NSF. Available at <http://ftp.sdsc.edu/pub/sdsc/air/papers/precedence.ps.Z>.
- Business Editors. (March 11, 1994). Competition, controversy ahead in era of Internet commercialization. *Business Week*.
- Cocchi, R., Shenker, S., Estrin, D., & Zhang, L. (1993). Pricing in computer networks: Motivation, formulation, and example. Tech rep., USC, Department of Computer Science, Hughes Airport Company, and Palo Alto Research Center. Available via Web from <http://gopher.econ.berk.umich.edu>.
- Campbell, A. (April 4, 1994). Distributed nesting: Avoiding the Domino effect. *Telephony*, 226(14).
- England, K. (08:04:26, 7 May 1994). Future Internet pricing. Posting on telecomreg@relay.adp.wisc.edu.
- Love, J. (00:02:55, 4 May 1994). Notes on Professor Hal Varian's April 21 talk on Internet economics. Posting on telecomreg@relay.adp.wisc.edu.

- MacKie-Mason, J. K. (13:37:03, 2 June 1994). Future Internet pricing. Posting on telecomreg@relay.adp.wisc.edu.
- Mitchell, B. M. (1989). Pricing local exchange services: A futuristic view. In *Perspectives on the telephone industry: The challenge of the future*. Edited by James H. Allaman & Richard D. Emmerson. Harper & Row: New York.
- Pecker, C. A. (1990). To connect or not to connect: Local exchange carriers consider connection oriented or connectionless network services. *Telephony*, 218(24).
- Russell, J. D. (1993). Multimedia networking requirements. In *Asynchronous Transfer Mode*. Edited by Yannis Viniotis & Raif O. Onvural. Plenum: New York.
- Tenney, G. (18:42:09, 4 May 1994). Future Internet pricing. Posting on telecomreg@relay.adp.wisc.edu.
- Varian, H., & MacKie-Mason, J. K. (1991). Pricing the Internet. Tech rep., University of Michigan, Department of Economics. Available via Web from <http://gopher.econ.is.umich.edu>.
- Varian, H., & MacKie-Mason, J. K. (1992). Economics of the Internet. Tech rep., University of Michigan, Department of Economics. Available via Web from <http://gopher.econ.is.umich.edu>.
- Wenders, J. T. (1989). Deregulating the Local Exchange. In *Perspectives on the telephone industry: The challenge of the future*. Edited by James H. Allaman & Richard D. Emmerson. Harper & Row: New York.
- Vickrey, W. (1981). Local telephone costs and the design of rate structures: An innovative view. Mimeo.

Author Information

Mirabaron Sarkar (sarkar@tc.msu.edu) is a Research Associate with the Institute of Public Utilities, The Eli Broad School of Management, Michigan State University, East Lansing, MI. Tel: (517) 355 8004.

Notes

(1) Traffic statistics are available from Merit's ftp site at [nic.merit.edu](ftp://nic.merit.edu).

(2) Varian and MacKie-Mason note that the actual growth has been faster. Internet usage is underestimated by the Merit figures, which do not incorporate data related to alternative backbone routes where the traffic is estimated to have been growing much faster.

(3) For example, real-time video is closer to a connection oriented network service (CONS) than it is to packet-switched connectionless network services. It does not exhibit the same stochastic burstiness that is characteristic of more conventional applications such as email. Russell (1993) notes that one way of distinguishing the kind of applications is to think of them as being either "conversational" or "distributive" (p. 190). Conversational applications are interactive where delays are critical to the natural flow of communication, and where a few hundred milliseconds can make a difference. Against this, in distributive applications, delays are not so critical. The newer applications are more skewed towards conversational than distributive.

(4) For a detailed overview of bandwidth requirements of different emerging applications, see "Multimedia networking performance requirements" by James D. Russell in *Asynchronous Transfer Mode Networks*, edited by Y. Viniotis & Raif O. Onvural, Plenum Press: New York, 1993.

(5) For a more detailed discussion of the telcos and cable companies involvement in the Internet, see Paula Bernier's "Opportunities abound on the Internet" in *Telephony*, vol. 226 (13), March 28, 1994.

(6) TAP-INFO is an Internet Distribution List provided for by a Washington-based organization, Taxpayers Assets projects, an organization founded by Ralph Nader. This letter, which was posted on various conferences across the Internet, requested a signature campaign addressed to Steve Wolf, Director of Networking and Communications for the NSF.

(7) For a detailed and well argued thesis of the difficulty in allocating joint costs in the telephone industry, see John T.

Wenders "Deregulating the Local Exchange" in *Perspectives on the Telephone Industry: The challenge of the Future*, edited by James H. Alleman & Richard D. Emmerson, Harper & Row, New York, 1989.

(8) They also report that the Internet has experienced severe congestion in 1987, and during the weeks of November 9 and 1992, when some packet audio/visual broadcasts caused severe delay problems, especially at heavily-used gateways to the NSFNET backbone and in several mid-level networks. A posting by William Manning on the telecomreg list on 4 May, 1994, at 20:50:46, reports that Rice University had to shut down their campus feed because some students were playing around and feeding live video signals into the Net, thus saturating the link, and making it unusable for other users on the ring. Varian & MacKie-Mason also report that they found delays varied widely across times of day, but followed no obvious pattern.

(9) One is tempted to include Mosaic and Netscape as a traditional application. However, the newer forms of multimedia applications over Mosaic and Netscape are tending to skew it as an application base that is that is at loggerheads with the net environment.

(10) It can also be argued that the real-time transmission of a heart surgery is more beneficial than an academic browser, and this is where the essential difficulty in assigning social values based on application software rather than specific uses come in. This point will be elaborated later.

(11) In the emerging architecture, the Network Access Providers will play a crucial role. The four NAPs, as mentioned earlier, are all telephone companies, with the exception of MFS which is a Competitive Access Provider (CAP). Historically, the telephone industry is replete with stories of monopoly abuse through the control of bottleneck facilities. It would be wise to realize that the inheritance of years of management styles cannot be shed aside very easily.

(12) The form and focus of regulation may change however.

(13) Consumer surplus in this case would be the excess bottleneck facilities.

(14) Posted on telecomreg on 2 June 1994.

(15) In response to my posting on telecomreg where I invited assessments of pricing mechanisms in the context of the systemic bottlenecks that are likely to emerge.

The Journal of Electronic Publishing
May, 1996 Volume 2, Issue 1
ISSN 1080-2711 <http://www.press.umich.edu/jep/works/SarkAssess.html>

[Front Page](#) | [About JEP](#) | [Backlist](#) | jep-info@umich.edu | [Search](#)

Pricing Network Usage: A Market for Bandwidth or Market for Communication?

David W. Crawford

Presented at MIT Workshop on Internet Economics March 1995

Abstract

[1] A congestion pricing scheme will generate revenue only if demand for bandwidth at zero price exceeds the bandwidth capacity. The recipient of congestion pricing revenue has an incentive to cause congestion in order to collect more revenue. Congestion can be caused by withholding capacity, which on the Internet, can be achieved (a) by strategically not building capacity, or (b) by hiding capacity from routers by deliberate non-advertisement of routes or by route blocking, or (c) by self dealing whereby the owner of capacity buys back a portion of her own capacity. Such a strategy of withholding capacity is analogous to the monopolist's strategy of choosing an output quantity smaller than that which corresponds to marginal cost intersecting the consumers' demand curve. There are several means to discourage the monopolistic inefficiencies due to the withholding of capacity: (a) by making congestion pricing a revenue neutral process by giving displaced users or their proxies the congestion fees, or (b) by making users joint owners of the bandwidth resource and thus joint claimants to the congestion revenue, or (c) by assessing both an access fee and a congestion fee (i.e., a two part tariff), or (d) by having competition for bandwidth provision.

[2] Incidence and liability for communication (network usage) costs are two distinct issues. The liability for communication costs (obligation to collect and submit the communication cost) may be imposed by the network owner on senders (sellers of information) and/or on receivers (buyers of information). Different liability allocations will result in different compliance (accounting, collection, and verification) costs. The liability should be imposed so as to minimize such compliance costs.

The incidence of the communication cost (the manner in which the communication cost is shared between buyer and seller) is not a design choice; it is endogenous and depends only on the preferences of network users.

[3] The question of how the market for communication (e.g., bandwidth) and the market for information (e.g., files) are linked is addressed by exploring analogies with other network environments.

1. Introduction and Outline

This paper examines proposed congestion pricing schemes allocating traffic on the Internet (such as Varian, 1994a, or Cocchi et al., 1992). In some cases, it is suitable to consider the task to be allocation of communication resources, i.e. a market for bandwidth. In other cases, it is beneficial to consider the task to be simultaneous allocation of both rights to information which can be sent over the Internet and the resources to be used for transmission, i.e. a joint market for information and for bandwidth. I will call this combination of information and bandwidth, communication. The formulation as a market for bandwidth ignores what it is that users want to send through the Internet; bandwidth is the only good considered, and can be considered solely from a sender's perspective. Both the formulation as a joint market for information and bandwidth and the formulation as a market for bandwidth alone addresses the possibility that both the sender and the receiver have a preference for the receiver receiving information.

The Internet and its predecessors (the Department of Defense's ARPAnet and the NSF's NSFNET) were funded by Federal government agencies, namely the Department of Defense and the National Science Foundation; individual users have not been charged for their use of networks, and have not generally been aware of the impact of their use on network performance. The number of people on the Internet is reported to have grown at a rate of 10 percent per month since 1990 when Commercial Internet Exchanges (CIX) were first connected to the Internet to allow commercial traffic. Rapid growth in the number of users, the proliferation of online graphic images, and especially the one button click-to-download interfaces are factors that are increasing the demand for transmission capacity hence increasing the opportunity cost of misallocating transmission capacity. The phasing out of Federal government funding of Internet operation in the United States necessitates some form of alternative funding, such as revenue from fee-for-service operation.

The motivation for imposing a pricing scheme is to give users knowledge about the value of what they do to other people, and an interest to not so as to reduce harm done to others. It is assumed that the system which grants users the power to cause congestion also provides users the power to reduce congestion and thereby avoid needless or inefficient harm. A generous

user who is willing to use a system after hours needs to know when after hours actually occurs. A less socially benevolent user, if offered a discount for after hours usage, may reschedule her use, not out of charity or of concern for the public good, but because it is in her interest to save money. Finally, a user must have sufficient power over the system so that after having decided to save money by using resources when they are cheap, the actions taken have that result. A user who submits her contributions to a mailing list at night will not have any benevolent impact if her software accumulates mail until 9 am and then transmits her messages.

A potential pitfall of introducing a pricing scheme is that it is not only the behavior of the consumers that may be affected, but also the behavior of the providers. Profit seeking providers will have as much knowledge, interest, and power in the system as any consumer.

This paper has three objectives. The first objective is to characterize congestion pricing as part of an optimal pricing scheme for network usage. The charge to users can in principle be based on any observable characteristic of or behavior by the user. Suitable behavioral characteristics on which to base a pricing scheme include (a) access; (b) capacity; (c) usage, and (d) priority of service. Observable non-behavioral characteristics include factors such as whether the user is a non-profit or for-profit institution, and the age of an individual user. Non-behavioral characteristics such as these could be used in setting prices, for example, by giving discounts to senior citizens or to nonprofit institutions. Somewhat equivalently, lump sums or rebates could be given to particular classes of consumers, who would then face the same price as everyone else in a uniform price market. Such schemes of non-behavior based price discrimination will not be considered in the present paper.

The access and capacity charges do not depend on if or how much the user uses the system, so these two charges can be combined into one lump sum charge for each user called the fixed charge, π . The usage and the priority charges depend on how and how much the user uses the system, and can be combined into one charge called the variable charge, p . Together, the fixed charge, π , and the variable charge, p , are a two-part tariff. If only one part of a multi-part tariff, the usage charge, is considered in isolation, an incentive appears to set the remaining part higher. For example, if p was reduced to 0 as a simplification of the analysis, the optimal value of π becomes larger. Therefore we model both the fixed charge and the variable charge simultaneously.

Secondly, the question of incidence and liability for communication (network usage) costs are two distinct issues. The liability for communication costs (obligation to collect and submit the communication cost) may be imposed by the network owner on senders (sellers of information) and/or on receivers (buyers of information). Different liability allocations will result in different compliance (accounting, collection, and verification) costs. The liability should be imposed so as to minimize such compliance costs. Third, and lastly, many people see analogies between the Internet and the interstate highway system, as suggested by the nickname, "the Information Superhighway," and as demonstrated by the use of extended metaphors such as on-ramps, road kill and speed bumps. Fiber optic links are called pipes; and analysis of the Internet lends itself to many analogies with other network resources. The specific characteristics of various networks that make them similar or dissimilar to the Internet is explored.

2. The Multi-Part Tariff: Access, Capacity, Usage, and Congestion

The short run costs of operating the Internet backbone are all either sunk because they are due to past decisions or are fixed because they do not depend on the quantity of information sent. Here the short run is defined as the duration of time from present until just before new capital goods can be bought and installed. Such sunk and fixed costs include the construction and configuration of lines, switches, and routers, or the leasing of such assets. Once such costs have been incurred, the cost to the owner of these assets of providing an additional unit of bandwidth is zero, as long as the total bandwidth used is between zero and the capacity of the system. Additional usage, beyond the capacity of the present system, is impossible during the short run because we adopt a literal meaning for the term "capacity" and because of how we define the short run.

A congestion pricing scheme will generate congestion revenue only if there is congestion, i. e. if demand for bandwidth at zero price exceeds the bandwidth capacity. In Figure 1, for the smaller supply, the price for which quantity demanded is equal to quantity supplied is positive; but for the larger supply, a zero price allows all demand to be met. If the only revenue generated by a communication resource is that due to congestion pricing, the owner of the resource has a strong incentive to increase her revenue by causing congestion by, for example, withholding capacity. In Figure 2, the gain in revenue due to a higher per unit price more than offsets the loss in revenue due to fewer units of bandwidth sold; thus the supplier will keep reducing the quantity of bandwidth offered to the market until reaching the quantity where marginal revenue equals marginal cost (or zero). At this point the revenue gain due to a higher price per unit is just equal to the revenue loss due to selling one fewer unit. See Figure 3.

Figure 1: Zero Price without Congestion
D. W. Crawford 1995 March

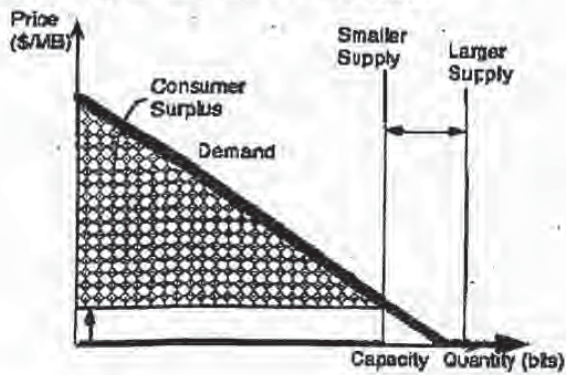


Figure 1.

Figure 2: Reduced Capacity Increases Price and Revenue
D. W. Crawford 1995 March

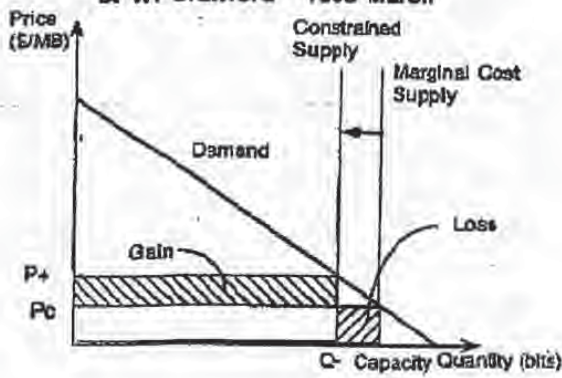


Figure 2.

Figure 3: Monopolistic Solution by Constraining Supply
D. W. Crawford 1995 March

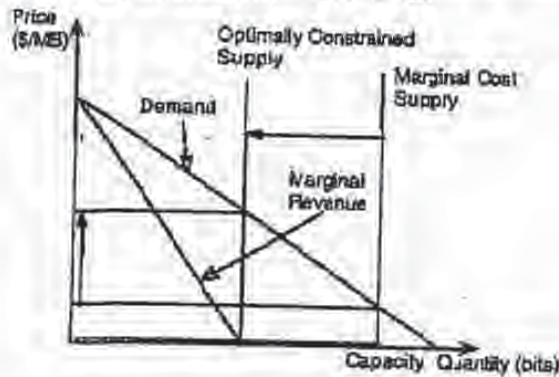


Figure 3

On the Internet, withholding capacity can be achieved by strategically not building capacity—by hiding capacity from routers. Analogously, one could cause congestion in a road network by hiring a few cars and drivers and having them feign breakdowns in strategic locations. On the Internet, we may cause congestion by what we may call demand pseudo augmentation whereby the apparent demand is increased by some form of supplier self-dealing. The optimal increase in demand shown in Figure 4 results in the same quantity legitimately consumed as does the optimal decrease in supply shown in Figure 3. By contrast, one could cause congestion in a road network by hiring many cars and drivers. But unlike cars, the packets that travel on the Internet are essentially free to generate and to dispose of. The demand could be augmented legitimately by providing access to more users or greater advertising of the benefits of Internet use. The pseudo-augmentation is due to the supplier of the bandwidth, or her collaborator, buying bandwidth solely to drive up the price. The collaborator would be refunded the entire cost of units purchased, so there is no net cost to the collaborator. Such a long run scheme would work easily on the Internet since it is costless to generate and request transmission of huge files (or many packets) and costless to discard these huge files (or many packets) upon receipt. In the financial world, self dealing whereby the owner of securities buys back a portion of her own holdings in order to manipulate the apparent market price is generally illegal. Such a scheme for raising the price up by pseudo-augmenting demand would not work in most other contexts, because there is a real cost of generating the articles sold or transmitted, and there is a further cost of then storing or disposing of them after their arrival at their destination.

Figure 4: Monopolistic Solution by Augmenting Demand
D. W. Crawford 1995 March

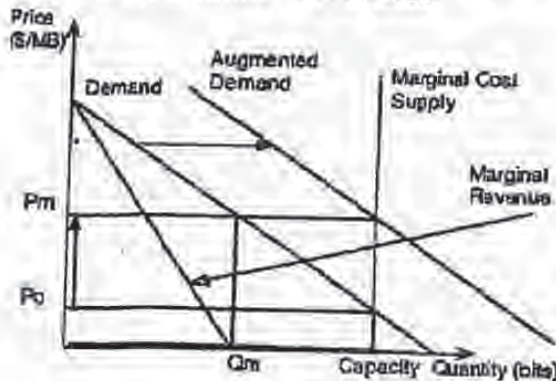


Figure 1.

Of the various strategies to reduce the quantity actually delivered to consumers in the market, the strategy of under investing in capital by under building capacity is the most attractive steady state solution, because presumably the smallest system is the cheapest system to build and yet it yields the same revenue as the other strategies. However, the notion of steady state in the Internet or computer industry is not appealing because both demand and technology continue to advance rapidly.

The strategy to build capacity and mask it out is appealing, because it accommodates growth in demand, and as less capacity is masked out, the supplier can claim credit for innovation and efficiency. Such a scenario is similar to that of an environmental engineer, who faced with a mandate to reduce emissions by half, declares, "This is the benchmark setting period - let's run dirty today". The strategy of pseudo-augmenting demand is less appealing, because the growth of total official quantity consumed will be under reported, and will hide the growth of the bandwidth providing company. Note that it is redundant to withhold capacity that has not been built.

There are several means to discourage the monopolistic inefficiencies due to the withholding of capacity:

(a) Revenue Neutral Congestion Pricing

Rather than allowing the network owner to keep congestion pricing revenue, the revenue could be given to displaced users. This is called a revenue neutral process because the revenue is collected from and given to the users, so the network owner is unaffected. This process is similar to the practice of compensating passengers who are bumped from an overbooked airplane: it would be identical if the non-bumped passengers were taxed to pay for the bumping compensation. If the ticket prices were set with the possibility of bumping compensation in mind, then the situations are perfectly analogous. Such a system needs to block further entry by consumers once it is recognized that the system is overbooked or congested. The revenue neutral congestion pricing rule removes the interest the network owner has in having network congestion occur.

(b) Unifying the Network

A system of managing a public good is for all the users to form a cooperative. The revenue from operation is divided among the users according to some agreed upon formula. Such an institution has been used extensively for managing oil reserves and aquifers with multiple well owners drawing from the same source [Libecap, 1989]. The unified network curtails the incentive to cause congestion because it is the same agents who both sufferer of congestion and are claimants to congestion pricing revenue.

(c) Multi-Part Tariff

The charge to users can in principle be based on any observable characteristic of or behavior by the user. Suitable behavioral characteristics on which to base prices include:

- access (whether the user is in fact connected to the system);
- capacity (the maximum rate at which a user can move information through the system, whether or not the user actually has used the capacity—essentially this is a standby charge for having the option to use available capacity);
- usage (a charge for the actual quantity of information sent through the system); and
- priority (a charge for displacing other users in the event of congestion).

Observable non-behavioral characteristics include whether the user is a non-profit or for-profit institution, or the age of an individual user. Non-behavioral characteristics such as these could be used in setting prices, for example, by giving discounts to senior citizens or to non-profit institutions. Somewhat equivalently, lump sum or rebates could be given to particular classes of consumers, who would then face a uniform price market. Such schemes of price discrimination will not be considered in the present paper.

The access and capacity charges do not depend on if or how much the user uses the system, so these two charges can be combined into one lump sum charge for every user, called the fixed charge, π . The use and the priority charges depend on how and how much the user uses the system, so these charges are variable. The usage and priority charges can be combined into one charge, called the variable charge, p . Together, the fixed charge, π , and the variable charge, p , are a two-part tariff. The optimal solution for the network owner is to set π equal to the consumer's surplus (See Figure 1), and to set p equal to the marginal cost. The marginal cost is equal to the highest value that any displaced user put upon not being displaced. In an

economically efficient allocation, the highest value that any displaced user put upon not being displaced is bounded by the lowest value a non-displaced user put on not being displaced. If there is no congestion, no user is displaced, and the marginal cost is zero. If there is congestion, and the buyers bid for usage, the marginal cost is equal to the highest rejected bid. If there is no congestion, no bids are rejected and the marginal cost is zero. The two part tariff so implemented is efficient because it provides the same quantity of the good as a competitive market would. The strategy of using a two-part tariff is normatively appealing because users pay a fixed fee based on their scale, so large sites pay more than small sites, and the variable fees vary with usage; however once packets are admitted to the system, each packet is routed alike, and all originator sites are treated alike.

The difficulty with the two part tariff approach lies in the fact that all consumers do not have the same individual demands, and thus have different consumer's surpluses. This difficulty could be overcome if the supplier could identify consumers with high demand and justify charging them a higher price and prevent resale by consumers given low prices to consumers given high prices. Since the proposed system has elicited bids for service, those bidding relatively high amounts can be presumed to be those with a high demand. The fact that such consumers have less chance of having their service interrupted helps to justify charging them a higher fee [Wilson, 1989]. If low bidding customers engage in resale, they will require larger capacity connections, and may need to bid higher in order to obtain the additional bandwidth. In doing so, they will have revealed themselves to have the higher demand of those to whom they would resell. Clearly, the opportunities for arbitrage in such a system are rather limited. If only one part, the variable charge, is considered in isolation, there appears an incentive for the supplier to withhold capacity. Therefore both the access charge and the congestion charge should be modeled simultaneously.

(d) Competition for Bandwidth Provision

Assuming compatibility and interoperability problems could be overcome, having multiple suppliers would compete away the monopolistic profits. If one supplier withheld bandwidth, another would be willing to provide it.

3. Incidence and Liability for Transmission Costs

The cost of communication (network usage, transportation of information), T , if any, can be modeled as a difference between the price the buyer pays for the information, P_b , and the price the seller receives for the information, P_s , so

$$P_b - P_s = T$$

The liability refers to the obligation to submit T to the transport provider. The incidence of a tax refers to the change in prices from a datum in a tax free market where the price for everybody was P . The buyers may see their price increase by $(P_b - P)$ and the sellers see their price decrease by $(P - P_s)$ upon imposition of a tax T .

Seller incidence IS refers to the portion of the tax paid by the seller:

$$IS = \frac{P - P_s}{T} = \frac{P - P_s}{P_b - P_s}$$

Buyer incidence IB refers to the portion of the tax paid by the buyer:

$$IB = \frac{P_b - P}{T} = \frac{P_b - P}{P_b - P_s}$$

Note that $IS + IB = 1$ is an identity:

$$IS + IB = \frac{P - P_s}{P_b - P_s} + \frac{P_b - P}{P_b - P_s} = \frac{(P - P_s) + (P_b - P)}{P_b - P_s} = \frac{P_b - P_s}{P_b - P_s} = 1$$

Collecting a sales tax in a retail industry is analogous to collecting a communication fee. In the retail industry, where buyers greatly outnumber sellers, and sellers are less mobile than buyers, it is presumed more efficient to hold sellers liable for the tax; this division of labor reduces the number of agents to be monitored for compliance and evasion.

In the Internet context, providers of files (e. g., ftp archives or www sites) already assume the costs for disk space, access and

capacity costs, and file maintenance. In some cases, such as files offered to provide technical support or advertising, the provider would be willing to incur the additional cost of transportation. In other cases, such as the distribution of shareware or non-commercial documents, the consumer would be willing to pay an additional cost. In either case, the file is made available and the buyer pays P_t and the seller keeps P_s . Implementing this system as a seller liable system would be easy, since the seller is the sender of the files; this may require (depending on incidence) having the seller collect a charge from the buyer. Implementing this system as a buyer liable system would require a charge back accounting system, in which the file sent by the seller has its transportation cost billed to by the buyer. The buyer-labile system has a greater security related obstacle in verifying that the buyers actually requested the files they receive and for which they are liable for transportation costs. An explicit hybrid liability scheme is also possible. In the hybrid liability scheme, the buyer and seller agree to some allocation of the transmission costs. For example, the buyer may agree to pay one dollar and the seller agree to pay the remainder of the transmission charge. Any system that bills the receiver for transmission cost will be easier to implement if the receiver is already paying for the content. It is assumed that there will be more cases of receivers paying senders to send files than senders paying receivers to receive files, thus most file transfer transactions would be file senders collecting money from file receivers. In these cases, it seems suitable for the sender to collect additional money to cover the receiver's incidence of transmission cost. Assuming that most file transactions are of the paying to receive mode and not the paying to send mode, a sender liable system seems likely to minimize the transactions costs. A COD or postage due type of system is not likely feasible, because of the storage requirement needed from the time the message is sent to the time the potential recipient is informed of incoming information and announces a willingness to pay or not.

4. How are networks similar or different?

A network is a set of nodes and arcs; each arc links two nodes. The use or function of a network is to allow some object to be sent from one node to another node. An arc may be directional, which implies that the sending is possible in only one direction. There may be more than one arc linking two nodes. The object transported may be water, oil or gas in the case of pipeline networks; or planes, trains and automobiles in the cases of airline, rail, and road networks, respectively. The planes, trains and automobiles hierarchically include people and freight as objects transported. In the case of information networks, such as computer data or telephone networks, the object transported is a bundle of information. A postal system may be considered a network; objects sent via mail may be considered information. In a commodity network (oil, gas, water, or electricity), the objects transmitted are generic and perfectly interchangeable. In an information network (mail, phone, computer data), the objects sent may be individualized and not interchangeable.

Example 1. Water transport network technology

- input: x = water at node A at time t_1
- output: y = water at node B at time t_2
- production function: $f(x, t) = y$

Note that in the water network example above, both the input and the output are time stamped. If $t_1 < t_2$ then the flow is from A to B. Generally network flows are reversible, so it is important to keep track of the direction of flows and the time at which an object is at a particular node. A factor common to all types of networks is that their capacity to produce is not storable, so capacity unused today cannot be saved for use tomorrow. Note that the storage of capacity of a network to transmit is distinct from the storage of objects transported over the network. So for example, if a milkman takes one day off and does not use his capacity to deliver milk for a day, his capacity to deliver milk is not stored and accumulated, giving him double capacity on the following day. However, the undelivered milk may be stored.

The possible uses of a network literally maps from departure space (where you start) to arrival space (hopefully where you want to go). The example above was an example of a transportation activity. The network can formally be expressed as the set of all possible transportation activities. For example, a postal network can be represented as a mapping from and to the space generated by the Cartesian product of all possible pieces of mail, all possible locations of mail, and all possible instants of time. Of course, this may not be the most parsimonious representation. For a communication network, we may be able to think of discrete pieces of information represented by flashes of light or voltage fluctuations on a wire, as mail trucks on a road or as packages inside the mail truck. Though computers can send data over phone lines by using modems, the term 'phone network' and 'computer data network' are not synonymous. The cost of operating a network typically depends on the amount of traffic it bears; the Internet is an exception. This phenomenon of more users causing greater operation cost is a negative externality. In the case of increased connectivity, having more users is a positive externality because more people are reachable.

Comparison of Networks

(a) Net Flow vs. Total Flow

The commodity networks do share a common property that one unit transferred from node B to node A is a perfect substitute for a unit that already was at node A. Non-commodity transportation networks (planes, trains, and automobiles) do not share this perfect substitution regardless of origin property. In communication, each unit of information has a source node (author) and receiver node (reader). Receiving mail or phone calls intended for another node is typically useless (unless it's cash in the mail) both for the sender and recipient. In communication, there are intermediate cases such as broadcasting, in which watching the State of the Union Address delivered on station X is a perfect substitute for watching the State of the Union Address delivered on station Y. *Table 1. Network Type vs. Characteristics*

| Network Type | Characteristic | | | | |
|--------------|-------------------|------------------------|-----------------|----------|---------------------|
| | Store and Forward | Net Flow or Total Flow | Frictional loss | Self | Measure of Capacity |
| Mail | yes | total | possible | no | letters/day |
| electricity | no | net | yes | yes | power (MW) |
| data | maybe | total | maybe | NA | bits per second |
| telephone | no | total | no | NA | calls |
| road | yes | total | possible | yes/NA | trucks per hour |
| water | yes | net | yes | no | kg per second |
| gas/oil | yes | net | yes | possible | kg per second |

In commodity flow networks (electricity, oil, gas, water), only net transfers between two nodes during a period or net transfer rates at a time matter. In information networks (data, mail), the total number of objects transferred between nodes matters. Compare the following three cases:

Example 2. Suppose we are currently pumping 50 units of water from node A to node B. The net transfer between nodes is 50 units from node A to node B.

Example 3. Suppose we are currently pumping 80 units of water from node A to node B and simultaneously pumping 30 units of water through the same pipe from node B to node A. The net transfer between nodes is 50 units from node A to node B.

Both of these examples (2 and 3) describe the same net flow of water. Example 3 may appear to be an inefficient use of the network, but since our consideration will be in terms of net flows, and the second case is identical to the first case in terms of net flow, the second case is as efficient as the first case.

(b) Frictional losses

In a pipeline network, such as one containing water, gas, or oil, flow is induced by increasing pressure at source nodes and/or decreasing pressure at sink nodes. In electric networks, flow is induced by increasing voltage at source nodes and/or decreasing voltage at sink nodes. Gas and oil networks have frictional losses, and pumps may be used to overcome such losses, but it is not necessarily gas used to power pumps in a gas network to overcome friction or oil powered pumps used in an oil network. An electric network has losses that are analogous to friction: the resistance/impedance of the wires. In an electric network it is the electricity itself that is used up to overcome this resistance. The electricity used up in an electric network is like milk drunk by a milkman who drinks more milk the longer and more tiring his route. A water network arc thus has a property known as conservation of mass, where water going in one end comes out the other. But an electric network has in kind losses, so what comes out at one end is less than what went in at the other end. These in kind losses make modeling the electric network more difficult than modeling a network that conserves mass. Communication networks are externally powered. For example, the mailman provides the energy to sort and move mail; the mail itself is not energized. But we may think of the bandwidth used to carry header data as frictional loss encountered when sending a data payload.

(c) Store and Forward

Above it was stated that all networks share a property that their capacity is not storable. However, the good transmitted on a network may be storable. For instance, a mailbox is a node in a mail network. The mailbox sends (is emptied) once or twice a

day, but may receive incoming mail hundreds of times per day. Between events of being emptied, the mailbox is storing mail. Nodes on gas, water, or oil may have reservoirs for storing product between two other nodes. Many data networks have a store and forward architecture. However, electricity itself is not storable, so nodes in an electric network cannot be used for storage. As a low level protocol, Internet does not store and forward, but applications such as Usenet do store and forward.

(d) Measuring Capacity

Gas and oil may be measured by mass, number of molecules, or volume at some pressure and temperature, or energy content at some pressure and temperature. Electricity is measured in terms of energy.

Quantifying communication is more problematic than quantifying electricity or water. Suppose you wish to tell someone which horse you think will win a race against seven other horses. You might transmit the DNA genetic code of the winning horse; that would be a lot of information. If the horses have proper and unique English names, you may transmit the name of the horse, 'Sir Ed, 3rd'. If the horses have numbers, you may transmit '1'. That is very little information, but in this context, '1' is just as sufficient to identify the horse as is providing the complete genetic code. In this example, we need to indicate one of eight possible states of the world, since there are eight horses. If we start with a set of eight horses and make three binary decisions, we will have uniquely identified a particular horse. If each horse has a unique indicator, then by making three binary decisions, we will have uniquely identified a particular indicator, and by the uniqueness of the indicator, we will have identified a particular horse. The lesson here is that we can measure information as the number of binary decisions needed to get from some set of possible states of the world that are common knowledge to the knowledge that one particular state of the world is true. In the eight horse race, the amount of information needed to identify a particular horse is three binary decisions, or three bits.

To write a letter on a computer, we commonly use an extension of the roman alphabet called ASCII, which has 128 characters (a,...,z, A,...,Z, 0,...,9, and punctuation), or a PostScript alphabet which may have up to 220 characters. Newer alphabets are much larger: Apple Computer's QuickDraw GX alphabet has 65,000 possible characters [Arnold]. An ancient computer might have used an alphabet of 38 characters (A,...,Z, 0,...,9,...) and therefore needs 6 bits per character of English ($38 < 2^6 = 64$). A modern computer which is using display PostScript with a character set of 220 needs 8 bits per character ($220 < 2^8 = 256$). These examples show why saving the same content as different file types may result in different file sizes. The trend towards much larger symbol sets allows much more richly formatted text, but at a cost of longer files. A more detailed discussion of measuring information can be found in [Cover].

This analysis is germane to Internet pricing, because utilized systems (see Section 2b) such as America Online have been designed to send graphical icons once and save them locally; then subsequent invocations to the icon need pass only a cryptic abbreviated reference to the icon, not the icon itself. However, the user who has stored the icon gets to see the icon, and not the cryptic reference.

The World Wide Web system is not organized to store icons with common identifiers, but does have a system called Hyper Text Markup Language (HTML) that allows for very abbreviated formatting commands to be sent, such as emphasis which sends the word emphasis with information that the recipient's system should emphasize the word using boldface, or italics, as determined by the recipient's system. HTML does not tell the recipient's system how to render boldface or italic text; that is already known to the local system.

Conclusion

For analysis of the incidence of transmission costs on senders and receivers of information, it is best to consider the task to be allocation of both bandwidth and rights in information. For analysis of congestion pricing, the content can be ignored, but the access and capacity charges must be considered jointly with the usage and priority charges.

References

- Arnold, Kandy. "GX will provide printing power", MacWeek, 1994 August 15.
- Bellamy, John. Digital Telephony. New York: John Wiley and Sons, 1991. Bergseth, F. R. and S. S. Venkata. Introduction to Electric Energy Devices, Englewood Cliffs, New Jersey, 1987. 370 pp.
- Cocchi, R., Estrin, D., Shanker, S., and Zhang, L. "A study of priority pricing in multiple service class networks". In

Proceedings of Sigcomm '91. (1991). Available from: <ftp://parcftp.xerox.com/pub/net-research/pricing1.ps.Z>

Cocchi, R., Estrin, D., Shenker, S., and Zhang, L. "Pricing in computer networks: Motivation, formulation, and example". Technical Report, University of Southern California. (1992).

Cover, Thomas M. and Joy A. Thomas. *Elements of Information Theory*. New York: John Wiley and Sons, Inc. 1991.

Fudenberg, Drew and Jean Tirole. *Game Theory*. Cambridge, Mass.; MIT Press, 1992.

Kahn, Robert E. "The Role of the Government in the Evolution of the Internet", *ACM Communications*, Vol. 37, No. 8 (1994), pp 15-19.

Laffont, Jean-Jacques and Jean Tirole. *A Theory of Incentives in Procurement and Regulation*. Cambridge, MA: MIT Press, 1993.

Libecap, Gary D. *Contracting for Property Rights*. Cambridge [England]; New York: Cambridge University Press, 1989.

MacKie-Mason, J. K., and Varian, H. (1993). "Some Economics of the Internet". Technical Report, University of Michigan.

MacKie-Mason, J. K., and Varian, H. (1994a). "Pricing the Internet". In Kahin, B., and Keller, J. (Eds.), *Public Access to the Internet*. Unknown.

MacKie-Mason, J. K., and Varian, H., (1994b) "Economic FAQs About the Internet", *Journal of Economic Perspectives*, (Fall, 1994) anonymous ftp, gopher, or World Wide Web at <gopher.econ.lsa.umich.edu>. Version: April 4, 1994. [Ed note: this link no longer active. Try accessing the *Journal of Electronic Publishing* version at: <http://www.press.umich.edu/jep/works/FAQs.html>.]

Mas-Colell, Andreu. *The Theory of General Equilibrium: A Differentiable Approach*. Cambridge University Press, 1985.

Rassenti, Stephen, S. S. Reynolds, V. L. Smith. "Cotenancy and competition in a an experimental auction market for natural gas pipeline networks". *Economic Theory*, 3, (1993), pp. ??? ???.

Wilson, R. "Efficient and Competitive Rationing", *Econometrica* 57 (1989) pp. 1-40.

Acknowledgments

I would like to thank Stephen J. Rassenti, Vernon L. Smith, John Hawkinson, Dale O. Stahl and participants in the experimental economics workshop at the University of Arizona for useful comments and suggestions. Remaining misconceptions and errors are the fault of the author.

Author Information

David W. Crawford (david@arizona.edu) is a doctoral student in the Department of Economics at the University of Arizona. He can be reached at: McClelland Hall 401; University of Arizona; Tucson, AZ 85721; 520-621-6224.

The Journal of Electronic Publishing
 May, 1996 Volume 2, Issue 1
 ISSN 1080-2711 <http://www.press.umich.edu/jep/works/CrawMarket.html>

[Front Page](#) | [About JEP](#) | [Backlist](#) | jep-info@umich.edu | [Search](#)

<http://www.press.umich.edu/jep/works/CrawMarket.html>

3/12/01

Equilibrium Allocation and Pricing of Variable Resources among User-Suppliers (1998) (Correct) (2 citations)

Steven H. Low

cc.mtu.edu/infotrio...equilibrium1.ps
Cached: PS.gz PS PDF Image Update

From: cc.mtu.edu/staff/sample_papers
Home: S.Low (2) HPSearch

ResearchIndex Home Bookmark Context Related Track Related Site Documents
Highlight on Homepage

Rate this article: 1 2 3 4 5 (best)
Comment on this article

Abstract: We propose a novel model of resource sharing schemes that provide each user with a fixed minimum and a random extra amount of bandwidth and buffer. Allocations and prices are adjusted to adapt to resource availability and user demands. At equilibrium, if it exists, all users optimize their utility and resource demand equals supply, i.e., the marginal increase in user utility due to higher return on variable resources is balanced by the marginal decrease in utility due to their variability. We show how an equilibrium might be approached using a simple price adjustment rule that does not require any knowledge on the part of the network about user utilities. We further show that at equilibrium every user holds strictly positive amounts of variable bandwidth and variable buffer, and in the... (Correct Abstract)

Context of citations to this paper: More

...practice and a source that desires both fixed and variable bandwidth would subscribe to ABR with a minimum cell rate guarantee. We show in [24], [25] that at equilibrium, where all sources are at their optimality and demand equals supply, every source desires a strictly positive...

...n, yn) are restricted to be nonnegative. A variant of NI where the nonnegativity constraint on (xn, yn) is removed is treated in [12]. It models users (resellers) who can both buy and sell bandwidth and buffers among themselves through the network. The nonnegativity...

Cited by: More

Equilibrium Bandwidth and Buffer Allocations for Elastic Traffic - Steven H. Low (2000) (Correct)
Optimization Flow Control, I: Basic Algorithm and Convergence - Steven Low (1999) (Correct)

Active bibliography (related documents): More All

- 0.3: Increasing cones, recession cones and global cones - Paulo Klinger Monteiro (Correct)
- 0.4: Optimization Flow Control with On-line Measurement - Steven Low Dept (Correct)
- 0.4: The Cost of Quality in Networks of Aggregate Traffic - N. G. Duffield, S.H. Low (1998) (Correct)

Users who viewed this document also viewed: More All

- 0.1: An Optimization Approach to ABR Control - David Lapsley Steven (1998) (Correct)
- 0.1: Random Early Marking - Sanjeeva Athuraliyi, Steven. (2000) (Correct)
- 0.1: Optimization Flow Control with Newton-Like Algorithm - Sanjeeva Athuraliyi And (1999) (Correct)

Related documents from co-citation: More All

- Doc 2: D.G. Luenberger (1984). *Linear and Nonlinear Programming*, Second Edition, AddisonWesley
- Doc 2: Sanjeeva Athuraliyi, David Lapsley, and Steven Low. *An Enhanced Random Early Marking Algorithm for Internet Flow Control*. Submitted for publication, 1999.
- Doc 2: D.P. Bertsekas and J.N. Tsitsiklis, *Parallel and Distributed Computation* (PrenticeHall, Englewood Cliffs, 1989).

Bibtex entry: (Correct)

Steven H. Low. Equilibrium allocation and pricing of variable resources among user-suppliers. *Performance Evaluation*, 24(4), December 1998. More

```

@article { low98equilibrium,
  author = "Steven H. Low",
  title = "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers",
  journal = "Performance Evaluation",
  volume = "24",
  number = "4",
  pages = "207-223",
  year = "1998",
  url = "citeseer.nj.nec.com/low98equilibrium.html"
}

```

Citations made in this document:

BEST AVAILABLE COPY

- Doc. Context [1] Dimitri P. Bertsekas. *Necessary and sufficient conditions for existence of an optimal portfolio*. *Journal of Economic Theory*, 8:235-247, 1974.
- Doc. Context [2] A. K. Choudhury and E. L. Hahn. *Dynamic queue length thresholds for shared-memory packet switches*. *IEEE/ACM Transactions on Networking*, 6(2):130-140, April 1998.
- Doc. Context [3] R. Cicchi, D. Estrin, S. Shenker, and L. Zhang. *Pricing in computer networks: Motivation, formulation and example*. *IEEE/ACM Transactions on Networking*, 1(6):614-627, 1993.
- Doc. Context [4] Costas Courcoubetis, Vasilios A. Siris, and George D. Stamoulis. *Integration of pricing and flow control for ABR services in ATM networks*. *Proceedings of Globecom'96*, November 1996.
- Doc. Context [5] N. Duffield and S. Low. *The cost of quality in networks of aggregate traffic*. In *IEEE Infocom'98*, San Francisco, CA, March 1998.
- Doc. Context [6] A. Elwalid, D. Mitra, and R. Wentworth. *A new approach for allocating buffer and bandwidth in heterogeneous, regulated traffic in an atm node*. *IEEE Journal on Selected Areas in Communications*, 13(6):1115-1127, August 1995.
- Doc. Context [7] S. J. Golestani. *A self-clocked fair queueing scheme in high speed applications*. In *Proceedings of Infocom'94*, pages 636-646, 1994.
- Doc. Context [8] Jerry R. Green. *Temporary general equilibrium in a sequential trading model with spot and futures transactions*. *Econometrica*, 41(6):1103-1123, November 1973.
- Doc. Context [9] Oliver D. Hart. *On the existence of equilibrium in a securities model*. *Journal of Economic Theory*, 9:293-311, 1974.
- Doc. Context [10] Robert A. Farrow. *Finance Theory*. Prentice-Hall, Englewood Cliffs, N.J., 1988.
- Doc. Context [11] F. P. Kelly. *Charging and accounting for bursty connections*. In L. W. McKnight and J. P. Bailey, editors, *Internet Economics*. MIT Press, 1996.
- Doc. Context [12] Frank P. Kelly, Aman Maitloo, and David Tan. *Rate control for communication networks: Shallow prices, proportional fairness and stability*. *Journal of Operations Research Society*, 49(3):237-252, March 1998.
- Doc. Context [13] John Lintner. *The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets*. *Review of Economics and Statistics*, 47:13-37, 1965.
- Doc. Context [14] S. Low and P. Varaiya. *A new approach to service provisioning in ATM networks*. *IEEE/ACM Transactions on Networking*, 1(5):547-553, October 1993. For an updated version see <http://www.ee.mu.nz/~staff/low/research.html>.
- Doc. Context [15] S. H. Low and P. P. Varaiya. *Burst reducing servers in ATM networks*. *Queueing Systems*, 20:61-84, 1995.
- Doc. Context [16] Steven H. Low. *Equilibrium allocation of variable resources for elastic traffics*. In *Proceedings of INFOCOM'98*, San Francisco, CA, USA, March 1998. 20.
- Doc. Context [17] Jeffrey K. MacKie-Mason and Hal R. Varian. *Pricing congestible network resources*. *IEEE Journal on Selected Areas in Communications*, 13(7):1141-1149, 1995.
- Doc. Context [18] Debasis Mitra and Ilze Ziedins. *Virtual partitioning by dynamic priorities: fair and efficient resource-sharing by several services*. In B. Plattner, editor, *Lecture Notes in Computer Science (Proc. Intl. Zurich Sem. Digital Comm.)*. Springer, 1996.
- Doc. Context [19] J. Mossin. *Equilibrium in a capital asset market*. *Econometrica*, 34:768-783, 1965.
- Doc. Context [20] J. Murphy, L. Murphy, and E. C. Posner. *Distributed pricing for embedded ATM networks*. In J. Labelle and J. W. Roberts, editors, *Proceedings of the 14th International Teletraffic Congress*. Elsevier Science, 1994.

- Doc Context [21] Ben Noble and James W. Daniel. *Applied Linear Algebra*, 3rd Ed. Prentice-Hall, 1988.
- Doc Context [22] A. K. Parekh and R. G. Gallager. *A generalized processor sharing approach to flow control in integrated services networks - the single node case*. IEEE/ACM Transactions on Networking, 1(3):344-357, June 1993.
- Doc Context [23] F. L. Presti, Z. Zhang, J. Kurose, and D. Towsley. *Source time scale and optimal buffer/bandwidth trade-off for regulated traffic in an atm node*. In Proceedings of Infocom'97, April 1997.
- Doc Context [24] R. T. Rockafellar. *Convex Analysis*. Princeton University Press, N.J., 1970.
- Doc Context [25] S. Sathaye. *Traffic Management Specification v 4.0*. ATM Forum Traffic Management Group, October 1996.
- Doc Context [26] W. F. Sharpe. *Capital asset prices: A theory of market equilibrium under conditions of risk*. Journal of Finance, 19:425-442, 1964.
- Doc Context [27] Scott Shenker. *Fundamental design issues for the future internet*. IEEE Journal on Selected Areas in Communications, 13(7):1176-1188, 1995.
- Doc Context [28] D. Stiliadis and A. Varma. *Rate-proportional servers: a design methodology for fair queueing algorithms*. IEEE/ACM Transactions on Networking, 6(2):164-174, April 1998.
- Doc Context [29] Hal R. Varian. *Microeconomic Analysis*, Third Ed. W. W. Norton & Company Inc., 1992.
- Doc Context [30] M. Vidyasagar. *Nonlinear Systems Analysis*. Prentice Hall, 2nd edition, 1993.
- Doc Context [31] Jean Walrand and Pravin Varaiya. *High-Performance Communication Networks*. Morgan Kaufmann Publisher, San Francisco, CA, 1996.
- Doc Context [32] H. Zhang. *Service disciplines for guaranteed performance service in packet-switching networks*. Proceedings of the IEEE, 83, October 1995.
- Doc Context [33] L. Zhang, S. E. Deering, D. Estrin, S. Shenker, and D. Zappia. *RSVP: A new Resource reSerVation Protocol*. IEEE Network, 7(5):8-18, September 1993.
- Documents on the same site (http://www.ee.mu.az.au/staff/low/research/sample_papers.html): More
The Cost of Quality in Networks of Aggregate Traffic - N. G. Duffield, S.H. Low (1998)
A New Approach to Service Provisioning in ATM Networks - Steven H. Low, Pravin P. Varaiya (1993)
Optimization Flow Control, I: Basic Algorithm and Convergence - Steven Low (1999)
- Sample documents with summaries: Summarize this document
Undulant-Block Elimination and Integer-Preserving Matrix... - David Wise
A Note on the Relation Between Two Convergence Acceleration... - Paul Levrie, Adhemar...
Imprecise Observations of Mobile Robots Specified by a Modal... - Mathijs De Weert, Frank ...
- ResearchIndex - researchindex.org - NEC Research Institute 1997-2001

Assuring Ownership Rights for Digital Images

Germano Caronni

Computer Engineering and Networks Laboratory
Swiss Federal Institute of Technology Zurich
E-Mail: caronni@tik.ethz.ch

Abstract

The use of digital data has become more and more commercialized. This is especially true for digital images, where proofs of origin and of content integrity are an important issue. This paper describes a problem related to 'proof of origin' and proposes a possible solution to it. After a discussion of the solution, possible extensions and related areas of work are addressed.

1 The Problem

Until now, digital data which was disseminated had no 'unique' features. Everybody received an identical copy of the data. Thus, if one of the copies was illegally distributed, it was impossible to determine the initiator of the unauthorized distribution. Typical effects are software piracy, the unauthorized distribution of vector fonts for printers and the distribution of certain digital images, such as art collections and satellite data. The same holds true for the distribution of confidential texts or images.

All possible kinds of digital data, such as computer software, fonts, texts, images and sound suffer from this problem. Only digital data in form of images¹ will be discussed here. Although related solutions for other types of digital data might be found, they have not yet been considered and would exceed the limits of this paper. A possible solution for formatted text may be found in [9] or [16].

A distributor of digital images of commercial or confidential nature usually is interested in detecting the source of illegal copies of his data. To do this, he has to provide each recipient with a different copy of his data. A process called **tagging** will be described, which includes hidden information in images, and thus makes distributed instances of an image different from each other. 'Hidden' here means that the inclusion of the data into the image causes quality degradation which is not perceivable by human eyes, and a receiver of the processed image is not able to detect or remove the included tags. As soon as the distributor of the original image

¹ Only digital (or digitized) images are considered, which contain a certain amount of noise, or variance in brightness. Thus images of 'Roger Rabbit' may not be acceptable, but a copy of Tizians 'Pietà' is.

somehow receives an illegal copy of it, he should be able to identify the original receiver of this particular image with high probability, even if the image suffered from some loss of quality.

Naturally, the distributor has to decide if the cost (time and effort) of tagging is adequate to achieve the intended results. If the distributed images have a short lifetime and are spread to a large audience, as with Reuters news images, tagging might be less adequate than in an art catalogue. At the same time, secure means for distribution and storage of tagged images have to be used, e.g. by applying commonly known cryptographic techniques, such as DES[11] or IDEA[12] for storage and additionally RSA[10] for transmission. Otherwise, a tagged image might be stolen from a legal customer, causing him to be accused for illegally spreading this image.

2 Requirements for successful tagging of images

The fundamental solution to the problem of detecting the distribution path of each image is to provide each recipient of an image with a different copy. The difference in the distributed images will allow the distributor to identify a certain recipient, by determining to whom he has given this instance of the original image.

As soon as a recipient, from now on dubbed *enemy*, wants to illegally spread his image, he will use countermeasures like the addition of noise, stretching of the image in one axis, or any other change which does not destroy the semantics of the image. This makes it more difficult for the distributor to identify him and has to be taken into account when looking for solutions to the following requirements.

- A tag² introduced into an image should have maximal information content to allow a good differentiation between different recipients.
- The tag should destroy as small as possible an amount of original information in the image. This guarantees high acceptance of the modified image by the recipient.
- The distributor should be able to easily separate the tags from the original image to allow detection of tags when an illegal copy of an image returns to him.
- There should be no possibility to separate the tags from an image without having access to the original untagged image.
- Removing or hiding the tags in the image should imply a maximum loss of quality in the image.

Some of these requirements work against each other, so a balance has to be found in order to get an optimal result. This balance depends on the actual needs of the distributor, and is influenced by e.g. the number of recipients or the fact if the distributor wants to recognize printed copies of the image.

3 Technical Approach

The issue of tagging images was partitioned into interdependent problems. Possible solutions to these problems are examined in the following sections. The approach presented here is partially based on heuristics, as formal models and methods have yet to be defined. To do this, information theoretical and statistical arguments have to be combined and discussed together. No tightly related work has been found. Although [18] pursues the same goals as this paper, the chosen approach is strongly related to DCT compression of an image, and has not been considered further. Loosely connected previous and related work is referenced.

² The sum of hidden information introduced into the image is named tag.

3.1 Information that Constitutes the Tags

To allow the distributor to differentiate between multiple instances of the same image, information has to be included into them. In its most abstract form, this information is a sequence of bits. Experiments have shown that, using the method presented in section 3.2, an image usually contains some hundred tag bits. Depending on the expected strategies of the enemies, different usage and interpretation of these bits should be chosen. Under the assumption that enemies do not cooperate (see section 3.3), the tag bits may provide maximum difference between different image instances. Principles applied to the construction of error correcting codes [1] (ECC) can be used to construct highly individual tag sequences. Under other circumstances, random bit sequences [3] may be used. They are easier to construct than ECCs, and give a better possibility to detect groups of cooperating enemies (see section 3.3).

3.2 Integrating the Tags into the Image

A mechanism has to be found to integrate the above defined tag bits into the image in a non-localizable manner. The distributor may not simply append the tags to the image, or place them in well-defined locations of the image, as an enemy might then just remove the tags, without suffering a loss of quality.

The idea of hiding information in an image to provide means of transferring the information without detection by an enemy is not new [2][3]. For example, a bitsequence could be directly integrated into the image by setting the least significant bit of the color values of a pixel to the value of one bit in the sequence. Nevertheless, currently known mechanisms are not fault tolerant, even slight distortion of the image makes the hidden information unrecoverable², as no redundancy is provided.

If the tagging procedure were to be executed by a human he could modify some picture elements manually, thus minimally changing the semantics of the image. By introducing these modified elements (such as additional leaves of a depicted tree, a change in a shadow or a shift in the position of the sun) depending on the chosen bit sequence, a corresponding tag sequence would be produced. A similar but automated method for tagging purposes could shift borders detected in the image, replace homogenous areas by slightly different shades or change line widths of lines detected in the image. These two approaches (the manual and automatic change of image semantics) were not examined further, but still remain interesting, as they represent a near-optimal fulfilment of the requirements stated in section 2.

The approach taken in this work modulates the brightness of chosen rectangles in the image to hide its tagging information. Independent modulation of RGB color values is not suitable, as greylevel images are deemed to be of quite good quality, and the transformation from color to greylevel causes an extremely high information loss. Figure 1 illustrates the method.



Figure 1: Example on rectangular tags

To the left, an unmodified section of the image is displayed. The section in the middle is

² The approach of image tagging might even be used to convey small amounts of information between communication partners in a unrecognizable and fault-tolerant way.

tagged with a modulation of 2% of the maximal brightness, allowing the recovery of most of the tags even after printing and rescanning the image. Finally, the section to the right is tagged with a modulation of 15%, giving the possibility to actually see the embedded rectangles.

Using rectangles introduces a high amount of redundancy for the tag information, allowing the detection of tags even after strong distortions of the image. Special considerations taken when placing the rectangles in the image cause them to disappear behind the 'natural' noise in the image. No rectangle is placed in a region which is too homogenous, or contains a sharp break, such as an edge. Homogenous regions have to be avoided to prevent enemies from extrapolating the state of the tag by analyzing the surroundings of the tag, edges have to be avoided to maintain image quality.

3.3 Recovering Tags from Distorted Images

To recover the tags from a distorted image, the possible actions of the enemies have to be considered. An enemy can try to work alone, having access to only one tagged image, or a group of enemies can work together, and devise strategies which use their differently tagged images to defeat the distributor.

An enemy who has access to only one tagged image is not able to detect the tags, as they are hidden behind the 'natural' noise in the image. He can distort the whole image or regions of it. This may be a change of contents, like adding noise, quantifying the colorspace of the image, applying dithering or a change in the form of the image such as stretching it, slightly rotating it, etc.

Unless this solitary enemy degrades the quality of the image by an amount which makes a future exploitation unlikely, the redundancy of the tags which were introduced by the distributor allows a good (> 90%) detection of the tag sequence. Methods to compensate for a change in form are known (e.g. [4],[5] and [6]), but have yet to be applied.

A group of enemies working together is able to initiate a much stronger attack by mixing or comparing their differently tagged images. This way, they can reduce the detectability of tags or even localize a certain amount of them. Estimates on the strength of such attacks may be found in section 5.2. To solve the problem of cooperating enemies in a better fashion, special tag sequences or even a different tagging method have to be developed. A possible approach to do this might be derived from [17].

After the tag sequence is retrieved by the distributor, it is compared with all generated tag sequences. The ones that are most similar represent the enemy or group of enemies who has distributed the image.

4 Realisation

In this section, the proposed simple tagging mechanism and the detection of tags shall be examined in greater detail, after discussing some preliminaries.

The tagging process introduces noise into an image, thus degrading its quality. This quality degradation (and the degradation that occurs when enemies apply countermeasures to a tagged image) has to be measured. This may be done by some humans, stating their subjective impression about the image. Preferring more objective data which may be collected in an automated way another approach has been taken. The correlation coefficient between original and modified image is measured. This coefficient is calculated on the brightness of each corresponding pixel in the two images ($b_o(x, y)$ for the original and $b_m(x, y)$ for the modified image respectively). It is defined as:

$$R = \frac{V_{om}}{V_o V_m}$$

$$v_{om} = \frac{1}{(X \cdot Y) - 1} \sum_{x=1}^X \sum_{y=1}^Y (b_o(x, y) - m_o)(b_m(x, y) - m_m)$$

is the covariance between original and modified image, where m_o and m_m represent the mean brightness of either one. v_o and v_m are the variances of the two images, v_o is defined as

$$v_o^2 = \frac{1}{(X \cdot Y) - 1} \sum_{x=1}^X \sum_{y=1}^Y (b_o(x, y) - m_o)^2$$

When comparing two identical pictures, $|R|$ will have the value of 1, the more differences the pictures show, the more $|R|$ will decrease towards 0. This method for comparing images can only be applied to images having the same size, which sometimes might require the preprocessing of images.

4.1 How to Integrate the Tags

In this tentative realisation of the tagging mechanism, the bitsequence which constitutes the tags is generated by a simple random number generator [14]. For more serious applications better generators have to be chosen to disallow attacks based on this information.

Tags are represented by rectangles which get modulated onto an image. The more geometrical deformation of the image is expected, the bigger a tag should be. They have a fixed size of $2 \cdot 2$ up to $2n \cdot 2n$, ($n < \min(X, Y) / 2$) pixels, which is chosen at program start. Tags of 4×4 up to 16×16 pixels have been examined in [8] and in section 5 of this paper. In a first step, all locations in the image where a tag could possibly be placed are identified by calculating the variance of regions of size $n \cdot n$ in the image and comparing it against a upper and a lower limit. These limits were empirically defined. After having located all possible positions, some of these positions are randomly chosen; keyed by a so called **group identification** and a probability for each possible position to be actually used. Care is taken to provide each rectangle with a border of n unmodulated pixels. This is needed for a later detection of the tags. At the same time, the direction in which a future tag may get modulated (brighter/darker) is randomly chosen.

The location and possible modulation of tags in an image is the same for all customers who receive this image, as long as the group identification is the same for all customers. To differentiate between customers, a *serial number* is used, again keying a random generator. The thus generated bitsequence triggers the actual modulation of the tags, and is at the same time used to add some noise (currently 0.5% of the maximal brightness) to each pixel of the image. The activation of a tag alters the brightness of a corresponding rectangle in the image by e.g. 1%. Again these values are hardcoded. Figure 2 illustrates the different modulations which are superimposed on top of the original image.

Actual data on some examples (number of tags and correlation coefficient) may be found in section 5. Adapting the variance in brightness to the actual variance of the local region might lead to a noticeable increase in tag detection by the distributor, and will be subject to further study.

As tag rectangles are placed only in regions with a minimal variance, it is expected that the 'additional' information added by the tag disappears behind the image noise. Tags introduced in an image usually are not visible to a careful observer.

4.2 Recovering the Tags

The algorithm which recovers the tags is designed to exploit the fact that image distortion introduced by an enemy or e.g. lossy compression algorithm usually are not localized exactly on the effective tag rectangles. Distortion is expected to equally spread on the rectangles (or

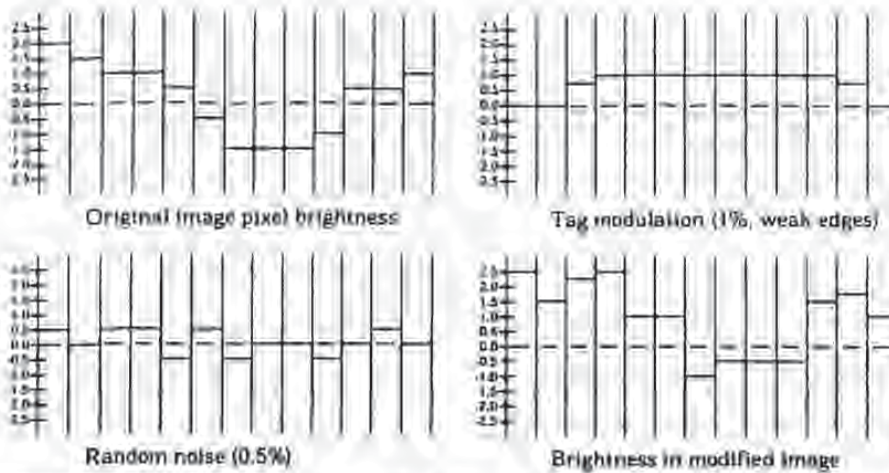


Figure 2: Modulation of an image by tagging information

part of them) and their unmodified surroundings. It is a precondition that the image to be processed has the same size as the original image, and that geometrical distortions (like rotation) have been eliminated from it.

In a first step, the brightness of each pixel in the received image is subtracted from the original one. Now, having knowledge of possible tag positions, the algorithm tries to recover the original modulation of the rectangle, thus identifying the state of the corresponding bit in the tag sequence. Around the original tag with size $2n \times 2n$ an unmodified region of size n should exist. After the subtraction, the mean brightness of the border region should be 0. The actual value is calculated, and the so won offset used to correct the mean value for the brightness in the tag rectangle. This is done separately for each quarter of the tag rectangle, allowing a future balancing of the four mean values extracted from the rectangle on a nonlinear base. Currently, just the arithmetic mean of the four values is taken and compared with a threshold. If the mean value is higher than $1/2$ of the modulation strength of the rectangle, the corresponding tag bit is taken as '1' in the other case as '0'.

After this has been done for each tag rectangle in the image, the distributor is now in possession of a recovered tag sequence. By comparing it with the stored tag sequences of all customers the enemy may be identified. If a group of enemies shall be detected, groups of different tag sequences have to be generated, and just the bits in each sequence which are equal to all customers in the assumed group have to be checked.

5 Evaluation

To substantiate some of the claims in this paper, data has been collected. The main purpose of this data is to show the detectability of tags in distorted images on the one hand, and on the other hand give some hints on how strong the quality degradation of the images in the course of tagging actually is.

5.1 Tagging and Quality Loss

Depending on the size and the 'noisiness' of the image, and on the tag size, a different number of tags can be placed in the image. Table 1 enumerates the number of tags which was measured on a variety of randomly collected pictures. At the same time values of $|R|$ are dis-

played, giving a hint on quality loss introduced by the tagging process.

| Image | #Tags 4x4 | #Tags 8x8 | #Tags 12x12 | #Tags 16x16 | [R] 4x4 | [R] 8x8 | [R] 12x12 | [R] 16x16 | [R] Ref. $\pm 1\%$ Noise |
|-------------------|--------------|--------------|----------------|----------------|----------|----------|-----------|-----------|-----------------------------|
| bud (640x480) | 690 | 477 | 254 | 150 | .9986551 | .9998131 | .9997596 | .9997647 | .9989916 |
| airlin (512x512) | 1593 | 606 | 282 | 156 | .9991024 | .9995785 | .9998635 | .9996585 | .9994244 |
| pic3 (562x800) | 814 | 445 | 250 | 204 | .9990525 | .9998270 | .9997997 | .9997749 | .9988591 |
| yellow (1152x779) | 1209 | 1075 | 683 | 435 | .9995562 | .9994302 | .9993338 | .9992625 | .9964358 |
| lake (812x512) | 1530 | 608 | 209 | 175 | .9999128 | .9998015 | .9998394 | .9998352 | .9993030 |

Table 1: Number of tags and value of correlation coefficient (tagging with 1.2%)

5.2 Countermeasures

As stated in section 3.3 enemies might apply different kinds of modifications to a tagged image to make it harder for the distributor to recover the tag sequence. The list of possible modifications and attacks on tagged images in this paper represents in no way an exhaustive overview, nor does it prove anything. It just gives a hint on the possibilities of the enemy⁴.

A group of enemies working together is able to initiate a strong attack. They may simply mix their images, giving each pixel of their 'output' image the value of the mean of all the corresponding pixels in the different images. This way, they can reduce the detectability of some of the tag bits by flattening the profile of the corresponding tag rectangles. Additionally they may compare their images, thus detecting differently modulated tags (see figure 3).



Figure 3: The detection of differing tags by enemies (20 tags detected)

They are then capable of falsifying their tag sequence. Assuming a randomly constructed bit sequence as identifier for each customer, N enemies may detect a fraction of $1 - 2^{1-N}$ of all tags. As long as the number of enemies is small, the distributor may still identify them by checking the bits they were not able to detect; if the number of enemies gets larger ($2^N \geq \text{Number of Tags}$) it is impossible to detect them.

A solitary enemy is not able to gain any information on the tags in the image. Thus his possible attacks are of two distinct classes:

1. Modification of image geometry

The enemy may slightly rotate, shrink, stretch, shift, etc. the whole image, or parts of it. This causes the locations of tags to be shifted, making it difficult for the distributor to (automatically) check the tags.

Just to give an example, some images have been shrunk by 50%. About 2/3 of all tags were still detectable, while $|R|$ dropped to about 0.85 and the images were subjectively severely degraded. The main problem here is to undo the geometrical distortion introduced by an enemy to allow the subsequent detection of tags. The application of [6] will at least partially solve this problem.

⁴ Usually it is very difficult for the designer of a cryptography or protection related algorithm to prove the strength of his algorithm, or assess all possible methods to counter it.

2. Modification of image content

The goal of content modification is to 'remove' the tags from the image, or at least distort the brightness of tag rectangles as much as possible, thus disallowing the distributor to successfully recover the bit sequence hidden in them. Image content modification comprises many possibilities. The following mechanisms have been employed to gain some data.

- Noise has been randomly added to the tagged image. The noise has been added to the brightness of each pixel, changing it by $\pm 2\%$, respectively $\pm 4\%$ of its maximal value.
- The JPEG lossy image compression algorithm [15] has been employed on the tagged images. The quality of the image was reduced to 75% and 30% respectively, where a quality of 30% represents a rather degraded picture.
- The colorspace of the tagged image has been reduced to 32 colors. At the same time dithering with Floyd-Steinberg error diffusion has been employed. The output of this step is in the range of a very sophisticated color printer.

Table 2 depicts the quality loss experienced when employing above methods on the original images (col: number of colors in the original image):

| | Noise 2% | Noise 4% | JPEG 075 | JPEG 030 | FSQUANT 32 |
|-----------------|----------|----------|----------|----------|------------|
| bud 16x16x16 | 9969303 | 9879267 | 9941969 | 9749611 | 9900836 |
| zurim 16x16x16 | 9983960 | 9935527 | 9971828 | 9918425 | 9949042 |
| pic3 16x16x16 | 9968435 | 9875711 | 9984049 | 9965293 | 9725430 |
| ystone 16x16x16 | 9961947 | 9624366 | 9959885 | 9912676 | 9983207 |
| leka 16x16x16 | 9980696 | 9923478 | 9971820 | 9942864 | 9911633 |

Table 2: Quality degradation after distortion of original images

A very special kind of modification is the repeated tagging of an already tagged image. Some trials assuming the knowledge of the tagging algorithm and all its parameters except the group identification and the original picture have shown a quality degradation of about 0.0002 per tagging iteration, and a loss of 3-4% of the original tags per iteration. After about the fifth iteration the images subjectively become more and more distorted.

5.3 Success in Recovering the Tags

Having produced a variety of tagged images (tagged with different tag sizes and differing strength of tag rectangle modulation) the content distortions mentioned above have been applied. Afterwards the tag sequences were recovered and compared with the originally introduced tags. Table 3 enumerates the percentage of tags that were successfully detected in each case for different tag sizes and tag modulation strengths.

Using a modulation strength of 2% and a tag size of 16x16 pixels, it was possible to recover 75% of the tags from enlarged, (color-)printed and rescanned images.

6 Summary and Future Work

A new and interesting problem has been presented, and some basic approaches for a solution have been discussed. Although there is still a lot of work to do, the results are promising. Additional efforts on both the theoretical and the practical side need to be done on at least the following points:

- Explore other forms of tagging and modulation of tags, including 'Adaptive Tagging'
- Explore hierarchical distribution paths for the images (multiple tagging?).
- Apply 'tagging' to sound (Tagging text has in the meantime been done by [9])
- Prove the nondetectability of tags introduced into images.

| | | Noise 2% | | | | Noise 4% | | | | JPEG Q75 | | | | JPEG Q30 | | | | FSQUANT 32 | | | |
|--------|------|----------|-----|-------|-------|----------|-----|-------|-------|----------|-----|-------|-------|----------|-----|-------|-------|------------|-----|-------|-------|
| | | 4x4 | 8x8 | 12x12 | 16x16 | 4x4 | 8x8 | 12x12 | 16x16 | 4x4 | 8x8 | 12x12 | 16x16 | 4x4 | 8x8 | 12x12 | 16x16 | 4x4 | 8x8 | 12x12 | 16x16 |
| bud | 1,0% | 81 | 98 | 99 | 100 | 68 | 83 | 90 | 99 | 82 | 99 | 100 | 100 | 83 | 83 | 93 | 100 | 76 | 91 | 94 | 98 |
| | 1,2% | 84 | 98 | 100 | 100 | 70 | 85 | 93 | 99 | 85 | 100 | 100 | 100 | 85 | 86 | 96 | 100 | 72 | 91 | 94 | 99 |
| | 1,4% | 86 | 99 | 100 | 100 | 73 | 90 | 97 | 100 | 88 | 100 | 100 | 100 | 88 | 92 | 99 | 100 | 82 | 96 | 95 | 98 |
| jurim | 1,0% | 81 | 98 | 100 | 100 | 68 | 87 | 93 | 97 | 82 | 99 | 100 | 100 | 85 | 83 | 96 | 98 | 75 | 90 | 92 | 94 |
| | 1,2% | 85 | 99 | 100 | 100 | 70 | 89 | 96 | 99 | 86 | 100 | 100 | 100 | 86 | 87 | 98 | 99 | 76 | 93 | 94 | 94 |
| | 1,4% | 88 | 100 | 100 | 100 | 73 | 92 | 98 | 100 | 89 | 100 | 100 | 100 | 89 | 90 | 99 | 100 | 81 | 95 | 95 | 96 |
| pk3 | 1,0% | 83 | 98 | 100 | 100 | 69 | 84 | 96 | 98 | 83 | 99 | 99 | 100 | 86 | 85 | 96 | 99 | 88 | 84 | 86 | 92 |
| | 1,2% | 85 | 99 | 100 | 100 | 71 | 86 | 96 | 99 | 84 | 99 | 100 | 100 | 86 | 89 | 96 | 100 | 71 | 84 | 88 | 94 |
| | 1,4% | 88 | 100 | 100 | 100 | 74 | 91 | 99 | 99 | 88 | 100 | 100 | 100 | 88 | 94 | 99 | 100 | 76 | 89 | 94 | 94 |
| ystone | 1,0% | 82 | 97 | 99 | 100 | 68 | 83 | 94 | 98 | 85 | 99 | 100 | 100 | 87 | 89 | 96 | 99 | 72 | 86 | 87 | 90 |
| | 1,2% | 85 | 98 | 100 | 100 | 70 | 86 | 95 | 99 | 85 | 100 | 100 | 100 | 88 | 91 | 98 | 100 | 76 | 88 | 88 | 90 |
| | 1,4% | 89 | 99 | 100 | 100 | 73 | 90 | 98 | 100 | 89 | 100 | 100 | 100 | 71 | 94 | 99 | 100 | 79 | 90 | 90 | 92 |
| lake | 1,0% | 80 | 98 | 99 | 100 | 67 | 88 | 94 | 98 | 83 | 99 | 100 | 100 | 86 | 88 | 96 | 99 | 69 | 85 | 88 | 94 |
| | 1,2% | 83 | 99 | 100 | 100 | 69 | 90 | 96 | 100 | 86 | 99 | 100 | 100 | 89 | 89 | 98 | 99 | 71 | 87 | 90 | 93 |
| | 1,4% | 87 | 100 | 100 | 100 | 72 | 94 | 98 | 100 | 89 | 100 | 100 | 100 | 71 | 93 | 99 | 100 | 73 | 89 | 92 | 94 |

Table 3: Measured success in detecting tags (in percent)

- Define probability limits for detecting enemies after receiving distorted images.
- Explore other geometrical shapes or overlapping shapes to carry tag information. Is spread spectrum technology applicable to the process of tagging?
- Adapt the 'decomposition of deformation' [6] to the analysis of tagged images.
- Develop better tag sequences for groups of enemies.
- Do extensive tests on different types of images.
- Find alternative methods to measure quality degradation of images.
- Analyze tagging in connection with confidential data and for steganographic purposes.
- Classify different possible types of tagging mechanisms, depending on the kind of document which is to be tagged.
- Study this approach in relation to the detection of covert channels [7].

Acknowledgements

The author would like to thank Bernhard Plattner and Ueli Maurer for their encouragement and support, which made this work possible.

References

- [1] Shu Lin, Daniel J. Costello Jr., "Error Control Coding: Fundamentals and Applications". Prentice Hall, 1983.
- [2] D. Kahn, "The Codebreakers", Macmillan, New York, 1967, pp. 523.
- [3] Friedrich Bauer, "Kryptologie: Methoden und Maximen". Springer-Verlag Berlin, 1993, pp. 5-20.
- [4] A.W. Gruen, "Adaptive Least Squares Correlation: A powerful image matching technique", Report Number 115 of the Institute for Geodesy and Photogrammetry, ETH Zürich, 1986.
- [5] William K. Pratt, "Correlation Techniques of Image Registration", IEEE Transactions on aerospace and electronic systems, vol AES-10, no 3, May 1974.

- [6] Fred L. Bookstein, "Principal Warps: Thin-Plate Splines and the Decomposition of Deformation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 6, June 1989, pp. 345-365.
- [7] National Computer Security Center, "A Guide to Understanding Covert Channel Analysis of Trusted Systems", (NCSC-TG-030), NCSC, National Security Agency, INFOSEC Awareness Division, Ft. George G. Meade, MD 20755-6000.
- [8] Germano Caronni, "Ermitteln unauthorisierter Verteiler von maschinenlesbaren Daten", in german only, Computer Engineering and Networks Laboratory, Swiss Federal Institute of Technology, August 1993.
- [9] J. Brassil, S. Low, N. Maxemchuk, L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", *Proceedings of Infocom '94*, pp. 1278-1287, June 1994.
- [10] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *CACM*, vol. 21, no. 2, pp. 120-127, Feb. 1987.
- [11] "Data Encryption Standard (DES)", NBS-FIPS Publication 46, National Technical Information Service, Springfield, VA, April 1977.
- [12] Xuejia Lai, "Detailed Description and a Software Implementation of the IPES Cipher", Institute for Signal and Information Processing, ETH Zürich, 1991.
- [13] M. Blum, S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits", *SIAM J. Comput.*, vol. 13, no. 4, pp. 850-864, Nov. 1984.
- [14] Stephen K. Park, Keith W. Miller, "Random Number Generators: Good Ones are Hard to Find", *CACM*, vol. 31, no. 10, pp. 1192-1201, Oct. 1988.
- [15] Gregory K. Wallace, "The JPEG Still Picture Compression Standard", *CACM* vol. 34, no. 4, pp. 30-44, Apr. 1991.
- [16] J. T. Brassil, S. Low, N. F. Maxemchuk, L. O'Gorman, "Hiding Information in Document Images", Submitted to IEEE Symposium on Security and Privacy 1995.
- [17] Dan Boneh, James Shaw, "Collusion-Secure Fingerprinting for Digital Data", Technical Report at Princeton University (<http://ftp.cs.princeton.edu/reports/1994/468.pdf>), October 1994.
- [18] K. Tanaka, Y. Nakamura, K. Matsui, "Embedding secret information into a dithered multilevel image", *Proceedings of the 1990 IEEE Military Communications Conference*, pp. 216-220, September 1990.

A WWW SERVICE TO EMBED AND PROVE DIGITAL COPYRIGHT WATERMARKS

Jian Zhao

Fraunhofer Institute for Computer Graphics
Wilhelminenstr. 7, 64283 Darmstadt
GERMANY
Email: zhao@igd.fbg.de

ABSTRACT

This paper describes a digital watermarking service which allows the publisher and information provider to mark and identify their copyrighted materials through the World Wide Web (WWW). First a general copyright watermarking scheme is proposed to aim at identifying the ownership and distribution path of multimedia works. Then a class of digital watermarking methods for images, videos and structured texts is outlined. Finally the implementation of this watermarking scheme in the WWW is described.

Keywords: Copyright Protection, Digital Watermarking, World Wide Web, Multimedia.

1 INTRODUCTION

The intrinsic characteristics of digital media (such as ease of replication, ease of transmission and multiple use, plasticity, identical copying, compactness and nonlinearity) have caused the problems associated with the enforcement of intellectual property rights [1, 2, 3]. One of the major solutions to the problems is based on *usage control scheme*, i.e. each usage such as printing, viewing or playing of the copyright protected material is controlled by authorized "rendering" hardware, firmware or programs. This scheme has been recommended by the working group on intellectual property rights in the USA's National Information Infrastructure [4]. A similar scheme, called CITED model, has even been experimentally implemented in CITED [5] and COPICAT [6] projects funded by the European Commission.

Although such restrictive use scheme may become the predominant transaction in some applications such as video-on-demand, it seems unlikely that it will be the single universal

solution. For example, P. Samuelson has criticized the scheme and concluded in some fields, e.g. in digital libraries, that the usage-based scheme is inappropriate [7]. The reason is two-fold: first tolerating some leakage may be in the long run of the interest of publishers. Second it may deter learning and deep scholarship for educational and research work. Furthermore, this scheme may also cause legal and implementation problems. To implement such a use-control scheme, all user's rendering devices (e.g. for printing, displaying) and their production must be licensed and authorized. This prerequisite is difficult to meet without a harmonic standard, a moderate user acceptability, and corresponding legislation measures. Therefore, it is unlikely that as a universal solution this use-control scheme will be widely put into practice in near future.

Rather than attempt to restrict and control copying or use of copyrighted materials, another solution could be to allow unlimited copying or use, and afterwards to provide evidence of any misbehavior. This solution is based on digital copyright watermarking technique [8, 9, 10, 11, 12], which secretly embeds robust marks into a material to designate its copyrights-related information such as the origin, owner, content, use, or destinations. We believe that this technique on the one hand can provide evidence for copyright infringements after the event, on the other hand, it may serve as a kind of deterrent to illicit copying and dissemination of copyrighted materials, therefore, to decrease their occurrences in advance. In addition, the watermarking technique is not contrary to the usage-control scheme: it is just complementary to the usage-control scheme by providing another defence against misbehavior on the copyrighted materials that may escaped from the controlled domain of the usage-control scheme.

To make the unauthorized copying and distribution evidential and provable, the copyright watermarking technique must meet the following requirements. First the embedded watermarks must be perpetual invisible, undetectable, unremovable and unalterable. Second it must be resistant against any processing and attack that do not effect the quality of the material. These requirements have been discussed in [3, 12].

To use digital watermarking, the copyright holders, especially small publishers and individual artists, expect a trusted body providing services

- to watermark and register copyrighted works,
- to provide copyrights and related information (such author, price) of a registered work,
- to verify the rights in the works, or
- to provide evidences of illegal copying and use.

The increasingly availability of computers, high-speed networks, and electronic-commerce technology make the electronic service possible. The aim of the watermarking server pres-

ented in the paper is to automate these services through network means. This server first allows work owners in the network to watermark and verify their works without having watermarking softwares, second allows consumers to obtain copyright information of any registered (watermarked) work. Besides the watermarking service, such a server may provide more functionalities for facilitating electronic copyright transaction and clearance.

This paper presents a design of such a watermarking server and an implementation in the World Wide Web. We will first describe a general and flexible copyright watermarking scheme aiming to identify the ownership and distribution path of the copyrighted material. Then we briefly describe a variety of watermarking methods which are used to provide the watermarking services and have been developed in the SysCoP (System for Copyright Protection) [12]. Finally, an implementation of the watermarking server in the World Wide Web is described.

2 A COPYRIGHT WATERMARKING SCHEME

In this section, we propose a three-phase copyright watermarking scheme. This scheme is based on a belief in private control of copyrights only by respective owners, and in flexibility and freedom of copyright protection and management. All keys for reading watermarks and the original copy of the work are controlled by its copyright holder. We believe that any "key escrow" or "escrow of the original" is not the interest of complex and dynamic digital marketplace. The watermarking server in this scheme is a trusted assistant to provide flexible watermarking services. The owner can ask the server to watermark his works, or can watermark by himself locally and register the watermarking on the server, or even does not contact the server.

This scheme addresses two important identifications associated with copyrights in the work: the owner and the distribution. In addition, it proposes to embed a public watermark into the work to indicate its copyright notice.

Public watermark

Similar to a traditional copyright notice or indication, a public watermark is readable publicly, and may be displayed or performed by the rendering device (image viewer, audio or video player). More information such as price or contact address may further facilitate end users to receive or purchase a particular permission from the copyright holder. Unlike the watermarks for identifying the owner or recipient, the public watermark is not secure, but can help the end user who wants to know if a multimedia material is copyrighted and more (e.g. the rights of use, contact address), thus to decrease copyright infringements resulting from ignorance or carelessness of the users.

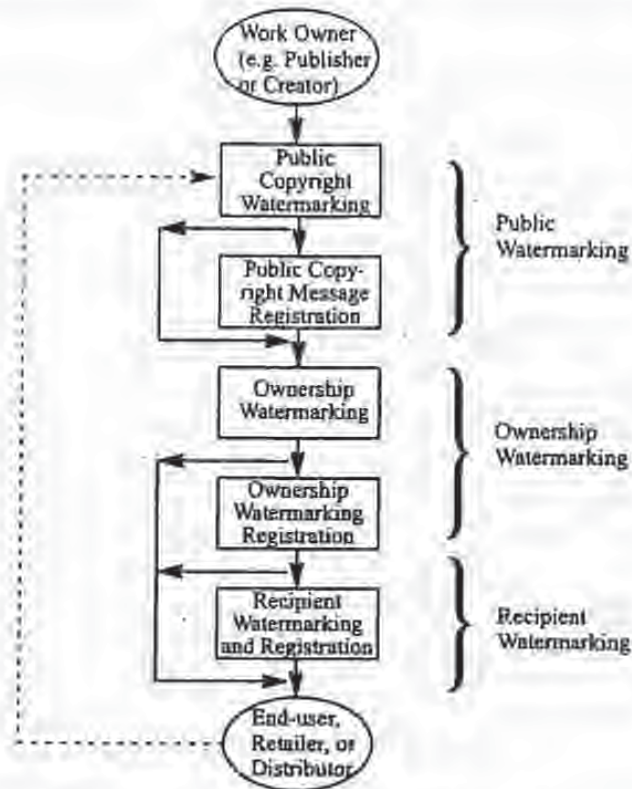


Figure 1. A digital copyright watermarking scheme

Ownership watermarking

This phase is concerned with the ownership watermarking and registration of the copyrighted material. The copyright holders have three optional ways to watermark their works:

- to send the work to the server for watermarking and registration,
- to watermark the work locally and then register this watermarking to the server, or
- to watermark and register the work locally.

More involvement of the watermarking server, more service can be provided to work holders and customers. In the first case, the server can not only provide copyright information, but can also solve some copyright disputes. In the last case the server only plays a role to read watermark from a work regardless of its authenticity. Section 4 will discuss watermark verification in details.

Recipient watermarking

This phase is optional – it embeds a unique identifier of a recipient into the material that will be delivered to the purchaser. It is likely to carry out this watermarking locally in information provider's site because of the large number of customers. A local codebook can be maintained to keep the mapping between customers' information and their unique identifiers. This recipient watermarking enables us to identify who made illicit copying and distribution.

When the recipients (i.e. purchasers) of the watermarked work are non-end-users (e.g. retailers or distributors), they may apply the second phase "recipient watermarking" again for their redistributions. Furthermore, when they buy the reproduction or derivation rights in the work from the original owner to produce or derive new materials, they have to perform the first phase "ownership watermarking" to protect their rights they bought in the new materials. Such a "multiple" ownerships and recipients chain implies another important requirement of digital watermarking: hierarchical watermarking, i.e. a multimedia data can be marked more than one times such that all watermarks are extractable if the quality of the data is not degraded yet.

3 WATERMARKING METHODS

The basic principle of watermarking methods is to add copyright information into the original data by modifying it in a way that the modifications are perpetual invisible and robust. It is obvious that the watermarking methods may depend on the media type and perhaps also content feature of multimedia documents. The watermarking server presented in this paper employs the methods developed in SysCoP [12]. Currently, three watermarking methods have been developed in SysCoP supporting three important media, namely, still images, motion images and structured text image. All methods share a framework for watermark-embedding or for watermark-retrieval process. Each process is composed of two steps. The first step is to generate a pseudo random position sequence for selecting blocks where the code is embedded, using extracted features of the multimedia data together with a user-supplied secret key as the seeds. The second step simply embeds or retrieves the code into or from the blocks specified in the position sequence using different watermarking methods. Each of these watermarking methods will be outlined below.

Frequency Hopping

The frequency-hopping watermarking method embeds a watermark bit through holding specific relationships between three randomly-selected quantized elements with a moderate variance level in the middle frequency ranges. The relationships among them compose B patterns (combinations), which are divided into three groups: "1" patterns and "0" patterns

representing "1"- or "0"-bit of embedded watermark respectively, and the *invalid patterns*. If too big modifications are needed to hold a desired valid pattern representing a bit, this block is invalid. In this case, the relationships among the three elements of the selected location set are modified to any of the invalid patterns, or are stored as part of the secret key to "tell" the watermark-retrieval process that this block is invalid. The criterion for invalid blocks is the maximum difference between any two elements of a selected set in order to reach the desired valid pattern.

By dividing the elements that have moderate variance level in a block into several zones, we can support *hierarchical digital watermarking*, i.e. multiple copyright watermarks can be embedded in different zones, and each of them can be separately extracted later. To increase the robustness of the watermarks, the same watermark can be redundantly embedded into one data more than one times.

Black/White Ratio-based Switching

This method was designed to embed robust watermarks into binary images (i.e. black/white images). A bit is embedded into a randomly selected block in the following way: a "1"-bit is embedded into the block if the ratio of black to white is in a range (T_1), and a "0"-bit is embedded into the block if the ratio is in another range (T_2). A sequence of randomly selected blocks is modified by switching whites to blacks or vice versa until falling into the ranges. When too much switching is needed, the selected block is invalid and is modified into any invalid range which is outside T_1 and T_2 . A "buffer" λ is introduced between T_1 , T_2 and the invalid ranges, representing the robustness degree against image processing of watermarked images, i.e. the number of bits that can be altered after image processing without damage of embedded bits.

Line & Word Shifting

This method was developed in AT&T Bell Laboratories [8] and can be used to watermark the text format file (e.g. in Postscript format) or black-white document images. A bit is embedded into a text document by shifting slightly a line down or up, and/or a word in a line left or right. We have implemented a simple version of this method. First we only support a specific format of text document, namely, the Window-Word produced Postscript file. Second we do not use the first and last lines of paragraph, and a line or a word in a line where a bit is embedded is always accompanied by two unmodified lines (one above and one below) or two unmodified words (one left and one right).

4 COPYRIGHT WATERMARK VERIFICATION

The aim of the copyright verification is to claim the ownership and/or identify the original purchaser of a watermarked work. This aim consists of three tasks:

- To construct the embedded codes using the secret key that was used in the watermarking embedding process,
- To prove that a watermark retrieved from a material is the same one that was embedded, and
- To determine which watermarking is earlier than another one.

The first task can be accomplished using a watermarking server or a local watermarking retrieval program. Several approaches have been proposed to prove the authenticity of the watermark, and to determine the watermarking time. They will be described below.

Error Correction

The first approach is to embed an error-correction code, in addition to the information provider's or purchaser's identifier, into the material. The advantage of this approach is that neither additional information nor the involvement of third party is needed in solving copyright disputes. However, trust and reliability of this approach are restricted on the capability of the error-correction method.

Watermark Certificate

The third copyright verification approach is to use a certificate issued by the watermarking server. When a document is registered and marked in a server, the server issues a certificate stamped with its digital signature. In addition, this certificate is encrypted using the requester's public key and therefore can only be decrypted by the requester. The certificate may contain most same information (holder, registration time, embedded watermark, etc.) that are also stored in the server's database. Thus, many copyright disputes may be solved by parties involved according to the rules described above.

Use of a Watermarking Server

In the second approach, a watermarking server takes over the verification task using the original watermarks stored in its database. The automatic verification process at the server consists of three steps, as shown in Figure 2:

- (1) Retrieve the embedded code using the user-supplied secret key and the multimedia data to be verified.
- (2) Retrieve the watermark from the server's database according to the unique document identification (DID).
- (3) Compare two watermarks that are retrieved from the multimedia data and the database, respectively. If the match accuracy is greater than a criteria percentage T (e.g. 85%), the verification succeeds, otherwise fails.

To determine a watermark is earlier than another, both watermarked works are usually needed. We assume that the similarity between two works is judged by human experts – they determine whether a work is derived from the other (i.e. infringes copyrights in the deriving work). Assume that the two similar works in a copyright dispute are $d1$ and $d2$ held by the person $p1$ and $p2$, respectively. If $p1$ is able to read his/her valid watermark both from $d1$ and $d2$, he/she is supposed to be the "original" owner of the work.

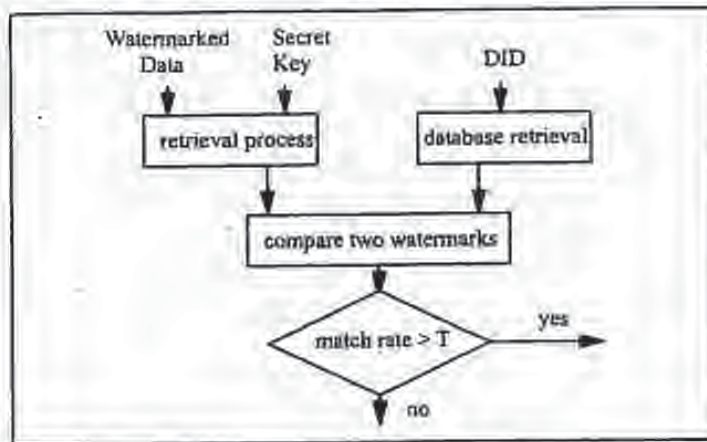


Figure 2. Copyright verification by the Watermarking Server

A watermarking server may also use watermarking time to determine which watermark is "original" if both watermerkings were performed by a server. If both $d1$ and $d2$ have been marked and registered by $p1$ and $p2$ in watermarking servers, the registration time of $d1$ and $d2$ is the decisive factor in solving the dispute: the earlier register shall hold the ownership of $d1$ and $d2$.

5 IMPLEMENTATION IN THE WWW

As increasingly expansion and development of the World Wide Web, on the one hand, copyright problem has become one of major barriers in the commercial use of the WWW publishing [13]: without appropriate copyright protection and revenue technologies, the WWW will and can only stay for advertisement purpose in the field of commercial electronic publishing or for disseminating "gray literature" (technical reports and other materials that have not yet been published formally). On the other hand, the WWW provides an excellent means for a wide range of WWW users to perform copyright transactions and for copyright holders and agents to offer electronic services such as clearance, licensing, as well as watermarking and registration. This section describes an implementation of a watermarking

server in the World Wide Web. It accepts the requests from WWW users for copyright watermarking and verification of their copyrighted materials.

The complete URL of the image (ppm, gif, tiff, jpeg):

The label to be embedded into the image (max. 8 characters):

Secret key (max. 9 digits):

Figure 3. Image watermark-embedding form

The complete URL of the image (ppm, gif, tiff, jpeg):

Secret key (max. 9 digits):

Document identifier (DID):

Figure 4. Image watermark-retrieval form

Technically, the WWW user's watermark-embedding or -retrieval requests (in a WWW client) are implemented as two HTML forms, which are shown in Figure 3 and 4, respectively. The complete URL of the multimedia data to be watermarked must be entered in the first field. The server accepts various image formats, including PPM (PGM, PBM), JPEG, GIF, TIFF. Since conversions between image formats do not damage watermarks, any conversion

toolkit (e.g. PBMPLUS or XV) can be used to convert other formats to an acceptable one before sending it to the server. MPEG-I and the Postscript data produced by Microsoft Window Word are the supported formats for video and structured text, respectively. Up to 8 characters can be entered as a watermark code to designate the copyright information such as owner's ID, purchaser's ID. In the last entry field a secret key must be given.

The "Submit" buttons in the forms activate gateway programs of a secure "httpd" server (Hypertext Transfer Protocol Daemon). The gateway programs communicate with the WWW server/browser using the standard CGI (Common Gateway Interface) [14], and perform the watermark embedding and extraction by calling SysCoP commands and functions. This WWW server together with these gateway programs forms a watermarking server.

The security and trust of the watermarking server mainly rely on a secure "httpd" (e.g. NCSA's s-httpd [15]) and a secure Web browser (e.g. NCSA's secure mosaic [16]). They support authentication, integrity and confidentiality between the service requesters and the watermarking server.

Embedding Watermarks

The watermark-embedding gateway program accomplishes a watermarking request in the following four steps. Figure 5 shows the whole process in respect of data flows between the watermarking server and the requester's WWW client and server.

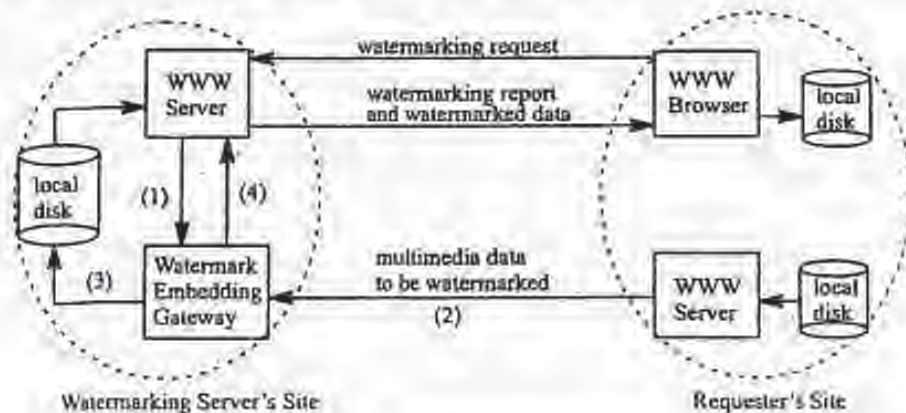


Figure 5. Watermark-embedding process

- (1) Get the request-form information using the CGI, including the complete URL (Uniform Resource Locator) of the data to be marked, a secret key, a watermark code to be em-

bedded into the data, and any (optional) additional copyright message (e.g. author, contact address, price, etc.).

- (2) Get the multimedia data to be marked according to its complete URL address.
- (3) Watermark-embedding transaction. First a unique document identification (DID) is assigned to the multimedia data. Then the gateway program calls the watermark-embedding command which takes the secret key, the watermark and the data as input parameters and produces a marked data file. In addition, this DID is also embedded into the data as the public watermark. Finally, it stores the DID, the embedded watermark, registration information (e.g. registration time, requester name), and the optional copyright message into a secure database.
- (4) Create a HTML page which will be shown on the requester's Web browser using CGI protocol. This page reports the status of the watermark-embedding process, shows the DID which has been assigned to uniquely identify the watermarking requester, and displays the marked multimedia data as an accessible icon. The requester click on this icon to get the watermarked data and store it into local disk.

Each watermark-embedding request is stored as a record into a secure database managed by a simple client-server DBMS on the watermarking server. As expansion of the number of watermarking servers, a federated, interoperable database management tool will be needed in the future for data exchange and integration between the databases at different servers. Each record consists of the following information:

- Unique Document Identifier (DID), which uniquely identifies the document in each watermark-embedding request.
- Registration and watermarking time.
- Requester's information, including user name, client address, etc.
- A checksum of the multimedia data.
- Information about watermarked document, including the type, format, and size of the document, and optionally a short description of the document content.
- Watermarking status, which represents the result of the embedding process (e.g. failure reasons).
- Embedded watermark, which is either supplied by the requester or generated by the system if it is not provided.
- Any copyright message which is optionally given the requester.

It is noted that the source and watermarked multimedia data, or the secret key supplied by the user for watermarking each multimedia data is not stored in the watermarking server. In the

current implementation, DID is a number incrementally assigned by the watermarking server – it should be a universal identification number (such as ISBN for books or ISRC for records) harmonized to international standards; The checksum of data could be replaced in the future by a hash value (e.g. produced with a MD5 algorithm) or more efficient feature digest in order to provide document authenticity and integrity service.

Retrieval of Watermarks

The watermark-retrieval gateway program reads a watermark, and verifies the ownership or recipient (if the watermark is secret) or reports the copyright information stored on the watermarking server (if this watermark is public). This process consists of four steps as illustrated in Figure 6:

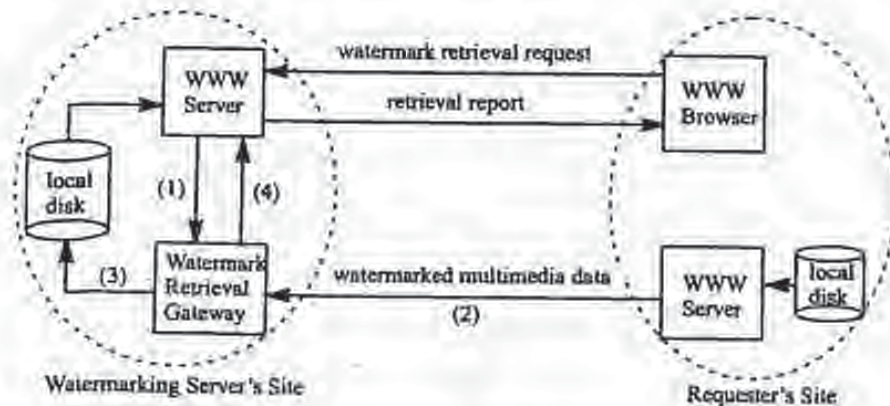


Figure 6. Watermark-retrieval process

- (1) Get the request-form information using the CGI, including the complete URL of the watermarked data, a secret key and a DID (only for retrieval of secret watermark).
- (2) Get the watermarked data according to its complete URL address.
- (3) If a secret key was given, retrieve a watermark using this key and performs copyright verification as described in Section 4 and illustrated in Figure 2; otherwise use the retrieved public watermark as a DID to search the database on the watermarking server to obtain corresponding copyright messages.
- (4) Create a HTML page, and show it on requester's Web browser using CGI protocol. This page displays the retrieved watermark, reports the status of the watermark-retrieval process, and shows the verification result (in case of retrieval of secret watermark), or public copyright message (in case of public watermark retrieval).

6 CONCLUSION

This paper presents a watermarking server providing multimedia copyright-watermarking and -verification services and an implementation in the World Wide Web. This WWW copyright watermarking server has been released to the whole WWW user since October 1995. Hundreds of requests and great attentions from a wide range of perspectives have been received since its operation. The URL of the server is <http://sagittarius.igd.fhg.de:64325>.

The present implementation of the watermarking server on the WWW is only at its very early phase. The further developments will go on in several directions:

The copyright watermarking scheme discussed in the paper only addresses part of the multimedia chain and actors involved. The static common functional model as well as the dynamic transactional model, which is being developed in the TALISMAN project [17] to cover the whole production and transaction chains of multimedia works, might be taken as a reference model for extensions.

We also plan to integrate and combine the watermarking server with a Copyright Clearance Center, which provides traditional copyright clearing and licensing services, for example, copyright query service (i.e. to determine what rights a user needs and who holds the rights), copyright negotiation and licensing in copyright transactions between the user and "copyright offices".

Though the technology for digital copyright watermarking is still in its early development and there is no legislation at present to accept its legal status, some activities have been under way [4, 18]. We believe that as the digital watermarking technology becomes mature and is widely used, it will obtain an important legal position in a court trial – perhaps just like fingerprint or blood group.

REFERENCES

- [1] Samuelson, P. (1991).
Legally Speaking: Digital Media and the Law.
Communications of the ACM, 34(10), October 1991, pp.23-28.
- [2] Kahin, B. (1994).
The strategic environment for protecting multimedia. IMA Intellectual Property Project Proceedings, vol. 1, no.1, 1994, pp.1-8.
- [3] Koch, E.; Rindfrey, J.; Zhao, J. (1994).
Copyright Protection for Multimedia Data. *Proceedings of the International Conference on Digital Media and Electronic Publishing* (6-8 December 1994, Leeds, UK).
- [4] Lehman, B. A. and Brown, R. H. (1995).
Intellectual Property and the National Information Infrastructure.
Section C, Part II, The Report of the Working Group on Intellectual Property Rights, September 1995.
- [5] Van Slype, G. (1994).
Natural language version of the generic CITED model. ESPRIT II CITED Project 5469, June 28, 1994.
- [6] COPICAT (1994).
Copyright Ownership Protection in Computer Assisted Training (COPICAT), Esprit Project 8195, Workpackage 2 (Requirements Analysis), Deliverable 1, June 2, 1994.
- [7] Samuelson, P. (1995).
Legally Speaking: Copyright and Digital Libraries.
Communications of the ACM, 38(3), April 1995.
- [8] Brassil, J.; Low, S.; Maxemchuk, N.; O'Gorman, L. (1994).
Electronic Marking and Identification Techniques to Discourage Document Copying. AT&T Bell Laboratories, Murray Hill, NJ, 1994.
- [9] Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. (1994). A digital watermark.
In: *Int. Conf. on Image Processing*, vol. 2, page 86-90, 1994.
- [10] Macq, B and Quisquater, J. J. (1995).
Cryptography for Digital TV Broadcasting.
In: *Proc. of the IEEE*, vol. 83, no. 6, 1995, pp. 944-957.
- [11] Cox, I.J.; Kilian, J.; Leighton, T.; Shamoon, T.
Secure Spread Spectrum Watermarking for Multimedia.
Princeton, NJ: NEC Research Institute, Technical Report 95-10, October 1995.
- [12] Zhao, J. and Koch, E. (1995).
Embedding Robust Labels Into Images For Copyright Protection.
In: *Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies* (Vienna, Austria, August 21-25, 1995).

In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Neuve, Belgium, May 1996

- [13] Norderhaug, T. and Oberding, J. M. (1995).
Designing a Web of Intellectual Property
In: Proc. of the Third International World-Wide Web Conference (10-14 April 1995, Darmstadt, Germany), pp.1037-1046.
- [14] CGI.
The Common Gateway Interface. See <http://hoohoo.ncsa.uiuc.edu/cgi/overview.html>.
- [15] Shttps.
The Secure NCSA https. See <http://www.commerce.net/software/Shttps>.
- [16] SMosaic.
The Secure NCSA Mosaic. See <http://www.commerce.net/software/SMosaic>.
- [17] TALISMAN. (1996).
Common Functional Model. Workpackage 1 of the TALISMAN project (EC ACTS AC019),
Deliverable 12, February 1996.
- [18] EC-COM(95)-382.
The Green Paper of Copyright and Related Rights in the Information Society.
Section 9, Part 2, Commission of the European Communities, COM(95) 382 final, Brussels, 19
July 1995.

Lecture Notes in
Computer Science

1174

Ross Anderson (Ed.)

Information Hiding

First International Workshop
Cambridge, U.K., May/June 1996
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Ross Anderson

Cambridge University, Computer Laboratory

Pembroke Street, Cambridge CB2 3QG, UK

E-mail: rja14@cl.cam.ac.uk

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information hiding : first international workshop, Cambridge, UK, May 30 - June 1, 1996 ; proceedings / Ross Anderson (ed.) - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996

(Lecture notes in computer science ; Vol. 1174)

ISBN 3-540-61996-8

NE: Anderson, Ross (Hrsg.); GT

CR Subject Classification (1991): E.3, K.6.5, D.4.6, E.4, C.2, I.1, K.4.1, K.5.1, H.4.3

ISSN 0302-9743

ISBN 3-540-61996-8 Springer-Verlag, Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10549111 06/3142-5 * 3 2 1 0 Printed on acid-free paper

Sometime in early 11 research communities do mostly unaware of each o

Firstly, recent moves other intellectual proper digital objects can be est — embedding hidden co in the event of a dispute. pictures or music, and yet technological challenge.

Secondly, a number o catons, digital cash, call for third parties to trace properties of everyday tr whether technological pro

Thirdly, computer sec over twenty years about c shared resource (such as i by modulating the system. The concern is that a vir a highly protected to a le of subliminal channels in attention of the crypto c interesting research.

Fourthly, there is steg of messages, often in othe out a message in Morse C in a letter home. This fel various governments' rece programs have appeared i to a digital picture.

Finally, a number of es have been developed over the military. These inclu use of highly directional i

These areas of study i the whole topic of inform

A suitable opportunity curity, Cryptology and C year at the Isaac Newton tee was put together, co

*r Multimedia Data,
Media and Electronic*

*Journal for Electronic
1994*

*Copyright Labelling,
Image Processing, News*

*to secretly embed a
proceedings, vol. 1, no:*

381-000-8

079061-0

Materials for the Class

Application, Springer-

*tion Using Iterated
as Center, San Diego*

Application, Chapter 1.

*tion Using Iterated
as Center, San Diego*

Course Notes

Application, Chapter 1.

Application, Chapter 1.

Echo Hiding

Daniel Gruhl, Anthony Lu, and Walter Bender

Massachusetts Institute of Technology Media Laboratory

Abstract. Homomorphic signal-processing techniques are used to place information imperceptibly into audio data streams by the introduction of synthetic resonances in the form of closely-spaced echoes. These echoes can be used to place digital identification tags directly into an audio signal with minimal objectionable degradation of the original signal.

1 Introduction

Echo hiding, a form of data hiding, is a method for embedding information into an audio signal. It seeks to do so in a robust fashion, while not perceptibly degrading the host signal (cover audio).¹ Echo hiding has applications in providing proof of the ownership, annotation, and assurance of content integrity. Therefore, the data (embedded text) should not be sensitive to removal by common transforms to the stego audio (encoded audio signal), such as filtering, re-sampling, block editing, or lossy data compression.

Hiding data in audio signals presents a variety of challenges, due in part to the wider dynamic and differential range of the human auditory system (HAS) as compared to the other senses. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thousand to one. Sensitivity to additive random noise is also acute. Perturbations in a sound file can be detected as low as one part in ten million (80dB below ambient level). However, there are some "holes" available in this perceptive range where data may be hidden. While the HAS has a large dynamic range, it often has a fairly small differential range. As a result, loud sounds tend to mask out quiet sounds. Additionally, while the HAS is sensitive to amplitude and relative phase, it is unable to perceive absolute phase. Finally, there are some environmental distortions so common as to be ignored by the listener in most cases.

A common approach to data hiding in audio (as well as in other media) is to introduce the data as noise. A drawback to this approach is that lossy data compression algorithms tend to remove most imperceptible artifacts, including

¹ At the Information Hiding Workshop held in Cambridge, England, the adjectives *cover*, *embedded*, and *stego* were chosen to describe the various signals used in data hiding. The term *cover* signal is used to describe the original signal in which the data is to be hidden. The information to be hidden in the *cover* signal is called the *embedded* signal. The *stego* signal contains both the *cover* signal and the *embedded* signal and is the final encoded signal. The word *signal* can be replaced by more descriptive terms such as audio, text, stills, video, etc.

typical low dB noise. Echo hiding introduces changes to the cover audio that are characteristic of environmental conditions rather than random noise, thus it is robust in light of many lossy data compression algorithms.

Like all good steganographic methods, echo hiding seeks to embed the data into a media stream with minimal degradation of the original media stream. By minimal degradation, we mean that the change in the cover audio is either imperceptible or simply dismissed by the listener as a common non-objectionable environmental distortion.

The particular distortion we are introducing is similar to resonances found in a room due to walls, furniture, etc. The difference between the stego audio and the cover audio is similar to the difference between listening to a compact disc on headphones and listening to it from speakers. With the headphones, we hear the sound as it was recorded. With the speakers, we hear the sound plus echoes caused by room acoustics. By correctly choosing the distortion we are introducing for echo hiding, we can make such distortions indistinguishable from those a room might introduce in the above speaker case.

Care must be taken when adding these resonances however. There is a point at which additional resonances severely distort the cover audio. We are able to adjust several parameters of the echoes giving us control over both the degree and type of resonance being introduced. With carefully selected parameter choices, the added resonances can be made imperceptible to the average human listener. Thus, we can exploit the limits of the HAS's discriminatory ability to hide data in an audio data stream.

3 Applications

Protection of intellectual property rights is one obvious application of any form of data hiding. Echo hiding can place a digital signature redundantly throughout an audio data stream. As a result, a reasonable level of hidden information is maintained even after operations such as extracting or editing. This information can be, but is not limited to, copyright information. With redundantly placed copyright information, unauthorized use of protected music becomes easy to demonstrate. Any clipped portion of the stego audio will contain a few copies of the digital signature (i.e. copyright information). Even "sound bites" distributed over the internet can be thus protected. Before placing an original sound bite on a web site, the creator can quickly run the Echo Hiding encoder. The creator can then periodically send out a web crawler that decodes all sound bites found, and reports if the given signature is in them. For such applications, detection and modification of the embedded text must be limited to only a select few. The embedded text is only for the benefit of the encoder and is of little use to the end user. We would like it to be immune to removal by unauthorized parties. With the correct parameters, echo hiding can place the data with a very low probability of unauthorized interception or removal.

Another application of audio data hiding is the inclusion of augmentation data. In most cases, this type of data is placed for the benefit of the end user. As

er audio that are noise, thus it is

embed the data l media stream. f audio is either in-objectable

esonances found the stego audio ng to a compact he headphones, hear the sound he distortion we indistinguishable

There is a point . We are able to h the degree and parameter choices, human listener. lity to hide data

on of any form of ntly throughout i information is This information andantly placed comes easy to i a few copies of tes" distributed final sound bite ler. The creator ind bites found, tions, detection select few. The little use to the horized parties. with a very low

f augmentation he end user. As

such, detection rules are more lenient. Since the data is there for the benefit of all, malicious tampering of the data is less likely. Echo hiding can be used to non-objectably hide data in these scenarios also. We can place the augmentation data directly into the cover audio in a binary format. One benefit of our technique is that annotations normally require additional channels for both transmission and storage. By hiding the annotations as echoes in the cover audio, the number of required channels can be reduced.

While the inclusion of augmentation data does not require strict control over detection by third parties, echo hiding provides a low interception rate as an option. The uses of augmentation data include closed-captioning (of radio signals and CD's, etc.) and caller-id type applications for telecommunications systems. With echo hiding, the sound signal could contain both the audio information and the closed-captioning. A decoder can then take that signal and output the audio or display the captioning.

More interesting examples are caller-id and secure phone lines. We can use echo-hiding techniques to place caller information during a phone call. A decoder on the receiving end can detect this information revealing who the caller is and displaying other supplemental data (i.e., client information, client history, location of caller, etc.). The information is attached to the caller's voice and is independent of the phone or phone service used. In contrast, current caller-id schemes only reveal the number of the device used to place the call. With echo hiding, it is possible to attach the information directly to the voice. As such, we have a form of voice identification and voice authentication. This can be useful in large conference calls when many people may try to talk, and identification of the current speaker is difficult due to low bandwidth. Phone calls that require a high degree of assurance of the identity of either party (e.g. oral contracts between an agent and employer) can also benefit from this application of echo hiding.

Echo hiding can also be useful to companies dealing with assuring that audio is played. For instance, when a radio station contracts to play a commercial, it can be difficult to know with certainty that the commercial is indeed being played as frequently as contractually agreed upon. Short of hiring someone to listen to the stations 24 hour a day, there is little they can do. Using echo hiding, we can place a "serial number" in the commercial. A computer can be set up to "listen" to the radio station, check for the identification number, and keep a tally of the number of times the commercial was played and how much of it was played (played in its entirety, cut off half way through, etc.). Echo hiding can also be useful when a radio station is multi-affiliated. Given similar commercials by two different companies, the radio station is by law required to play the tape given by each company in order to count for advertising by each company. This holds true even if the commercials are identical. By encoding each commercial using echo hiding techniques, the companies can keep track of which commercial is played. We can encode identical commercials with a different signature for each company.

Finally, tamper-proofing (prevention of unauthorized modification) can also be accomplished using echo hiding. A known string of digital identification tags can be placed throughout the entirety of the cover audio. The stego audio can easily be checked periodically for modified and/or missing tags revealing the authenticity of the signal in question.

3 Signal Representation

In order to maintain a high quality digital audio signal and to minimize degradation due to quantization of the cover audio, we use the 16-bit linearly quantized Audio Interchange File Format (AIFF). Sixteen-bit linear quantization introduces a negligible amount of signal distortion for our purposes, and AIFF files contain a superset of the information found in most currently popular sound file formats. Various temporal sampling rates have been used and tested, including 8 kHz, 10 kHz, 16 kHz, 22.05 kHz, and 44.1 kHz. Our methods are known to yield an acceptable embedded text recovery accuracy at these sampling rates.

Embedded text is placed into the cover audio using a binary representation. This allows the greatest flexibility with regards to the type of data the process can hide. Almost anything can be represented as a string of zeroes and ones. Therefore, we limit the encoding process to hiding only binary information.

4 Parameters

Echo Data Hiding places embedded text in the cover audio by introducing an "echo." Digital tags are defined using four major parameters of the echo: initial amplitude, decay rate, "zero" offset, and "one" offset (offset + delta) (Figure 1). As the offset (delay) between the original and the echo decreases, the two signals blend. At a certain point the human ear hears not an original signal and an echo, but rather a single distorted signal.²

The coder uses two delay times, one to represent a binary one ("one" offset) and another to represent a binary zero ("zero" offset). Both delay times are below the threshold that the human ear can resolve the echo and the cover audio as different sources. In addition to decreasing the delay time, we can also ensure that the distortion is not perceivable by setting the echo amplitude and the decay rate below the audible threshold of the human ear.

5 Encoding

The encoding process can be represented as a system that has one of two possible system functions. In the time domain, the system functions we use are discrete

² This point is hard to determine exactly. It depends on the quality of the original recording, the type of sound being echoed, and the listener. In general, we find that this fusion occurs around one thousandth of a second for most sounds and most listeners.

time exponential
impulses.

In this mean,
copy the cover a

We let the t
encoding a binary
encode a zero, P
encoded signal (t

The delay be
or system functi
with a delay of t
delay. In order t
smaller portions
bit by consideri
several bits) is t

In Figure 5,
labeled a, b, c,

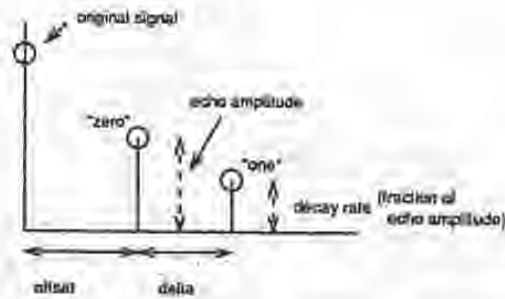


Fig. 1. Adjustable parameters

time exponentials (as depicted in Figure 2) differing only in the delay between impulses.

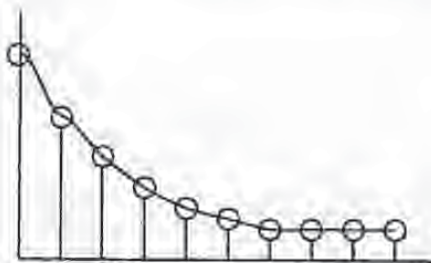


Fig. 2. Discrete time exponential

In this example, we chose system functions with only two impulses (one to copy the cover audio and one to create an echo) for simplicity.

We let the kernel shown in Figure 3(a) represent the system function for encoding a binary one, and we use the system function defined in Figure 3(b) to encode a zero. Processing a signal with either system function will result in an encoded signal (see example in Figure 11).

The delay between the cover audio and the echo is dependent on which kernel or system function we use in Figure 4. The "one" kernel (Figure 3(a)) is created with a delay of δ_1 seconds while the "zero" kernel (Figure 3(b)) has a δ_0 second delay. In order to encode more than one bit, the cover audio is "divided" into smaller portions. Each individual portion can then be echoed with the desired bit by considering each as an independent signal. The stego audio (containing several bits) is the recombination of all independently encoded signal portions.

In Figure 5, the example signal has been divided into seven equal portions labeled a, b, c, d, e, f, and g. We want portions a, c, d, and g to contain a

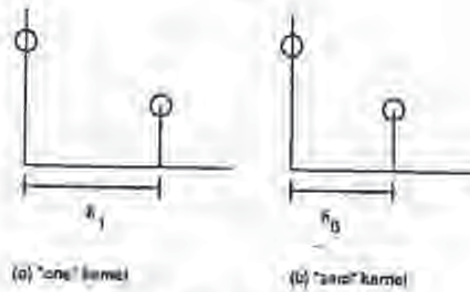


Fig. 3. Echo kernels

one. Therefore, we each of these ports system function. In a similar manner they have been individually processed and are recombined. We use something slightly different using each of the systems or all zeroes. The result

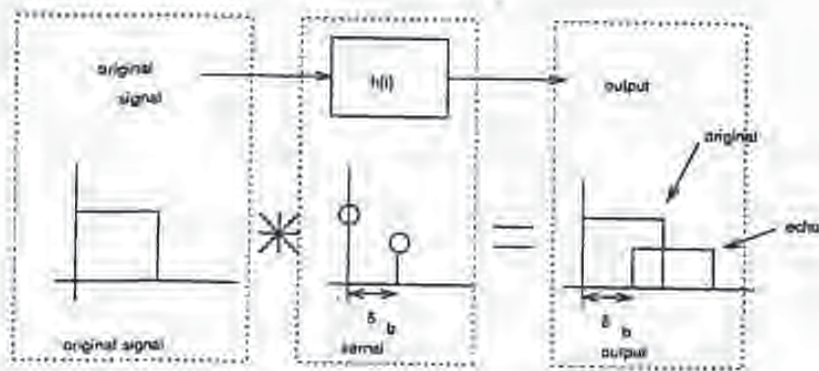


Fig. 4. Echoing example

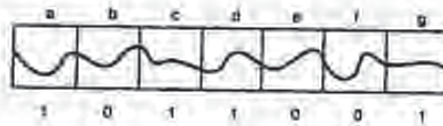
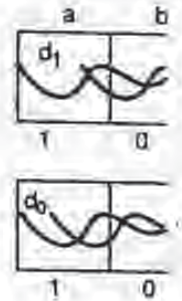


Fig. 5. Divide the cover audio into smaller portions to encode information

In order to combine the mixer signals and hide the information in different bits.

The "one" mixer signal is mixed with the original signals and scaled. Note that the "zero" and that the transmission of the two mixers between portions is the resonance of the system representing the

one. Therefore, we use the "one" kernel (Figure 3(a)) as the system function for each of these portions i.e. each is individually convolved with the appropriate system function. The zeroes encoded into sections b, e, and f are encoded in a similar manner using the "zero" kernel (Figure 3(b)). Once each section has been individually convolved with the appropriate system function, the results are recombined. While this is what happens conceptually, in practice we do something slightly different. Two echoed versions of the cover audio are created using each of the system functions. This is equivalent to encoding either all ones or all zeroes. The resulting signals are shown in Figure 6.

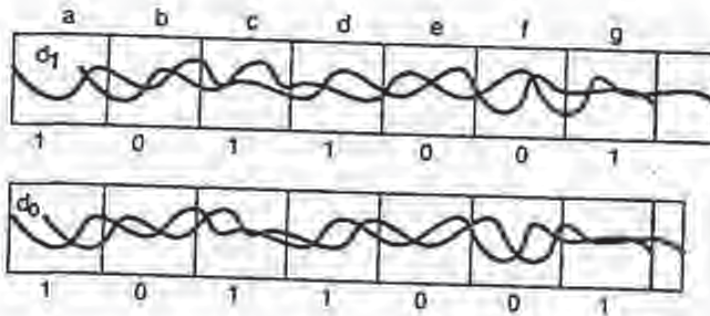


Fig. 6. First step in encoding process

In order to combine the two signals, two mixer signals (Figure 7) are created. The mixer signals are either one or zero (depending on the bit we would like to hide in that portion) or in a transition stage in-between sections containing different bits.

The "one" mixer signal is multiplied by the "one" echo signal while the "zero" mixer signal is multiplied by the "zero" echo signal. In other words, the echo signals are scaled by either 1 (encode the bit) or 0 (do not encode bit) or a number in-between 0 and 1 (transition region). Then the two results are added. Note that the "zero" mixer signal is the binary inverse of the "one" mixer signal and that the transitions within each signal are ramps. Therefore, the resulting sum of the two mixer signals is always unity. This gives us a smooth transition between portions encoded with different bits and prevents abrupt changes in the resonance of the stego audio, which would be noticeable. A block diagram representing the entire encoding process is illustrated in Figure 8.

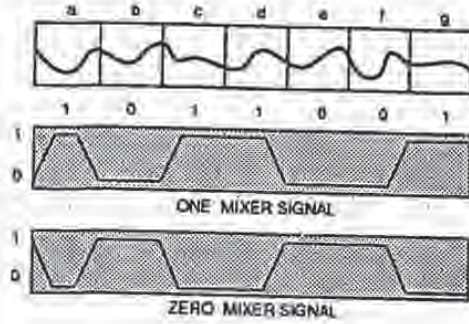


Fig. 7. Mixer Signals

6 Decoding

Information is embedded in one of two delay kernels as by an echo kernel with a δ_1 second delay. Extraction of between the echoes. In ord locations) of the autocorrela The following procedure is : a sample signal that is a ser by a set interval and have elsewhere (Figure 9).

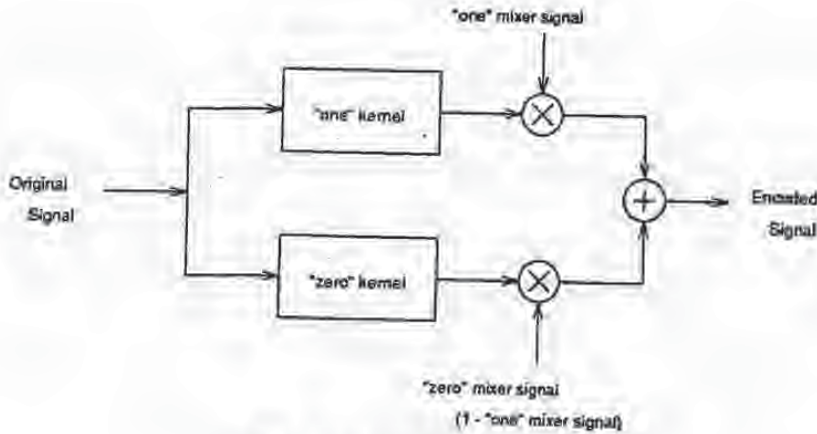


Fig. 8. Encoding process

Fig. 9. Extr

We echo the signal once The result is illustrated in I

Fig.

6 Decoding

Information is embedded into an audio stream by echoing the cover audio with one of two delay kernels as discussed in Section 5. A binary one is represented by an echo kernel with a δ_1 second delay. A binary zero is represented with a δ_0 second delay. Extraction of the embedded text involves the detection of spacing between the echoes. In order to do this, we examine the magnitude (at two locations) of the autocorrelation of the encoded signal's cepstrum (Appendix B). The following procedure is an example of the decoding process. We begin with a sample signal that is a series of impulses such that the impulses are separated by a set interval and have exponentially decaying amplitudes. The signal is zero elsewhere (Figure 9).

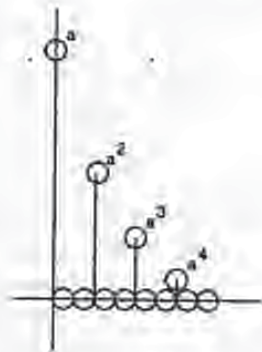


Fig. 9. Example signal: $x[n] = a^n u[n]$; $0 < a < 1$

Encoded
Signal

We echo the signal once with delay δ using the kernel depicted in Figure 10. The result is illustrated in Figure 11.

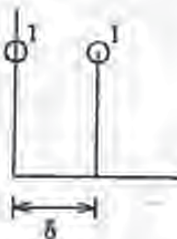


Fig. 10. Echo kernel used in example

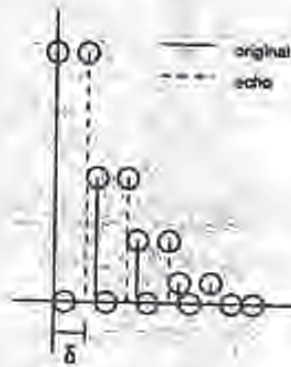


Fig. 11. Echoed version of the example signal

The next step is to find the cepstrum (Appendix A) of the echoed version. Taking the cepstrum "separates" the echoes from the original signal. The echoes are located in a periodic fashion dictated by the offset of the given hit. As a result, we know that the echoes are in one of two possible locations (with a little periodicity).

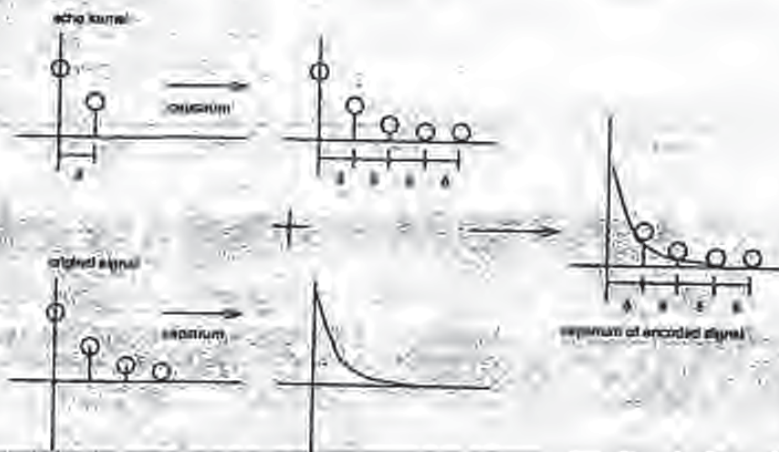
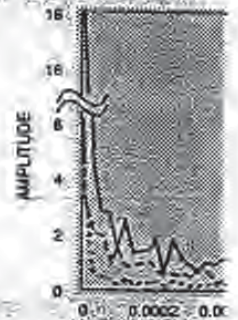
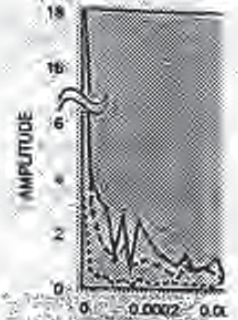


Fig. 12. Cepstrum of the echo-encoded signal

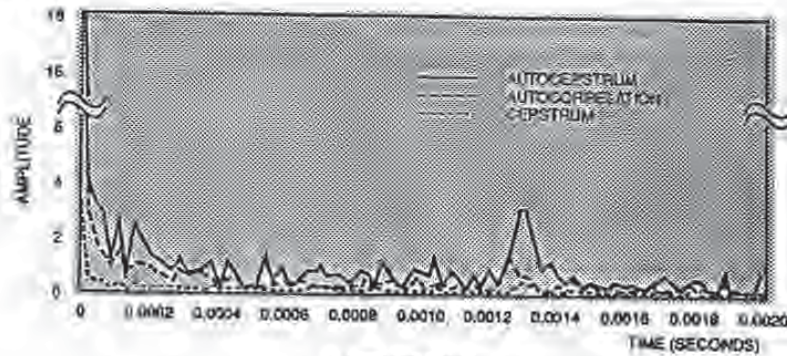
Unfortunately, the result of the cepstrum also "duplicates" the echo every δ seconds. In Figure 12, this is illustrated by the impulse train in the output.

Furthermore, the way relative to the cover is this problem is to take

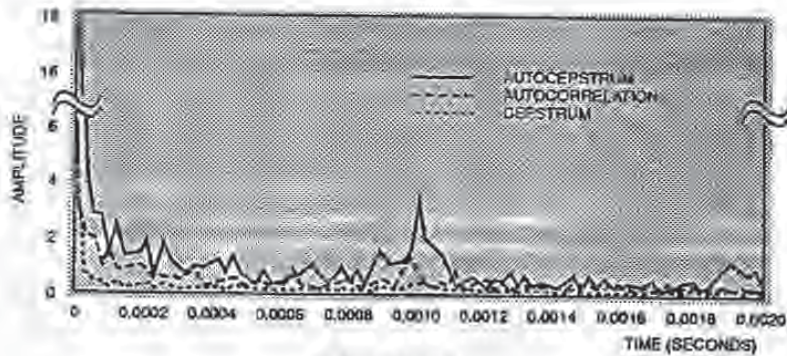


The autocorrelation. With the echoes spaced at either δ_1 or δ_0 in the at echo spacings of δ power at δ_0 and δ_1 in higher power level (se

Furthermore, the magnitude of the impulses representing the echoes are small relative to the cover audio. As such, they are difficult to detect. The solution to this problem is to take the autocorrelation of the cepstrum.



(A) ZERO (FIRST BIT)



(B) ONE (FIRST BIT)

Fig. 13. Result of autocorrelation

The autocorrelation gives us the power of the signal found at each delay. With the echoes spaced periodically every δ_1 or δ_0 , we will get a "power spike" at either δ_1 or δ_0 in the cepstrum. This spike is just the power (energy squared) at echo spacings of δ_1 or δ_0 . The decision rule for each bit is to examine the power at δ_0 and δ_1 in the cepstrum and choose whichever bit corresponds to a higher power level (see Figure 13).

ded version.
The echoes
in bit. As a
with a little



echo every
the output.

7 Results

Using the methods described, we can encode and decode information in the form of binary digits in an audio stream with minimal degradation at a data rate of about 16 bps.¹ By minimal degradation, we mean that the output of the encoding process is changed in such a way that the average human cannot hear any objectionable distortion in the stego audio. In most cases the addition of resonance gives the signal a slightly richer sound.

Using a series of sound clips provided by ABC Radio, we have obtained encouraging results. The sound clips cover a wide range of sound types including music, speech, a combination of both, and sporadic sound (music or speech separated by empty space or noise). We created a tool to test these clips over a wide range of parameter settings in order to characterize the echo hiding process. Running the characterizations on 20 sound clips of varying content and length, we discovered that the relative volume of the echo (decay rate) was the most important parameter with regards to the embedded text recovery rate. With 85% chosen as a minimally acceptable recovery rate (defined in Equation 1) all stego signals showed acceptable accuracy with a decay rate (relative volume of the echo compared to the original signal) between 0.3 and 0.85.

$$\text{recovery rate} = \frac{(\text{number of bits correctly decoded}) * 100}{\text{number of bits placed}} \quad (1)$$

At 0.5 and 0.6, few can resolve the echoes. While these results are encouraging, we would like to push the relative volume down even more. Between 0.3 and 0.4 even those with exceptional hearing have difficulty noticing a difference. We observed that in general the recovery rate was linearly related to the relative volume. However in certain cases, we observed deviations from this general rule, caused by the particular structure of the specific sound signal. Figures 14 through 17 illustrate the correlation (for three select files) between relative volume and embedded text recovery rate. The sound files chosen are representative of the entire set of sound clips. For the plots provided in this paper, the sample most amenable to encoding by Echo Hiding (a6, a segment of popular music), the sample least amenable to encoding (a1, a spoken news broadcast), and one mid-range sample (a14, spoken advertising copy) were used. In general, the more difficult samples are typically the ones with large "gaps" of silence (similar to a1, the example of unproduced spoken word) while those easiest to encode are those without such "gaps" (similar to example a6, the popular music clip).

Initially, we tested the process in a closed-loop environment (encoding and decoding from a sound file). The results are illustrated in Figure 14. All the files reached the 85% mark with relative volumes less than or equal to 0.6. a6 required a relative volume of only 0.3 to recover an acceptable number of bits. By 0.4, we were able to recover 100% of the hidden bits. a1 and a14 required a higher relative volume of 0.5 in order to achieve the 85% mark.

¹ This is dependent on sampling rate and the type of sound being encoded. 16bps is a typical value, but the number can range from 2bps-64bps.

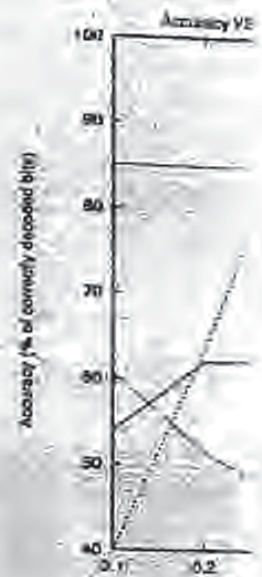


Fig. 14

We also tried encoding on an analog wire (with another machine (Fig. 0.9). Both a1 and a14 relative volumes, but approximately the same

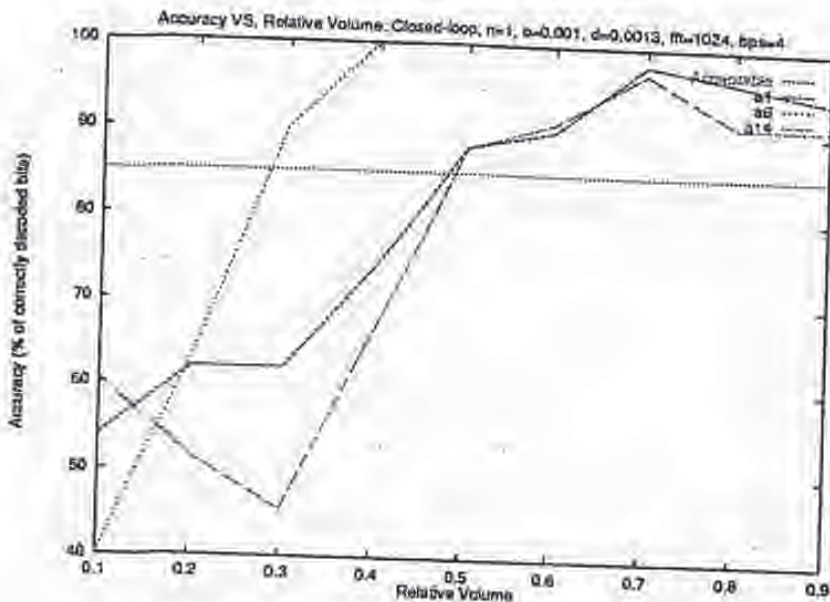


Fig. 14. Accuracy vs. relative volume: closed-loop

We also tried encoding on one machine, transmitting the sound file over an analog wire (with appropriate D/A and A/D conversions), and decoding on another machine (Figure 15): The required relative volume of a14 increased to 0.8. Both a1 and a14 experienced a noticeable decrease in accuracy at higher relative volumes, but an acceptable recovery rate could still be reached. a6 was approximately the same except that the 100% mark was not reached until 0.5.

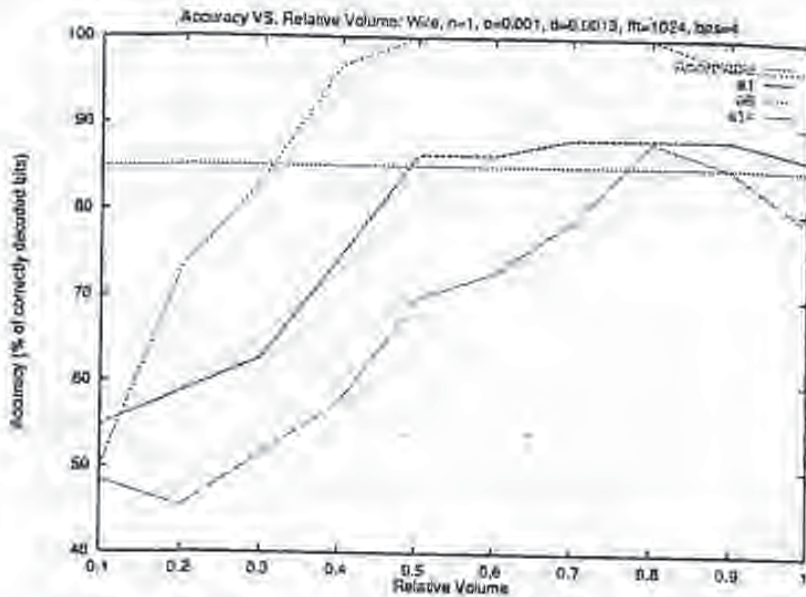


Fig. 15. Accuracy vs. relative volume: Analog wire

After testing an analog connection between two machines, we experimented with compression and decompression before decoding. We used two compression methods: MPEG (Figure 16) and SEDAT (Figure 17). The SEDAT compression was done with a test fixture provided by ABC Radio. In both cases, the recovery rate of a1 and a14 significantly decreased. a6 was only slightly effected by the compression and decompression.

The other parameters (number of echoes, offset, and delta), seemed to produce acceptable results regardless of their value. This does not, by any means, indicate that these parameters are useless. Instead, these parameters play a significant role in the perceivability of the synthetic resonances. These interactions are in some cases highly non-linear, and better models of them are an area of continuing research. As discussed earlier (Section 4), a smaller offset and delta result in an increased "blending" of the resonances with the cover audio mak-



Fig. 16. Accuracy

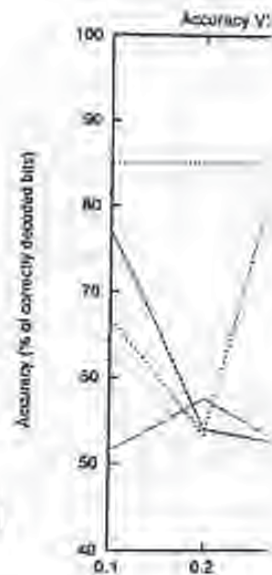


Fig. 17. Accuracy

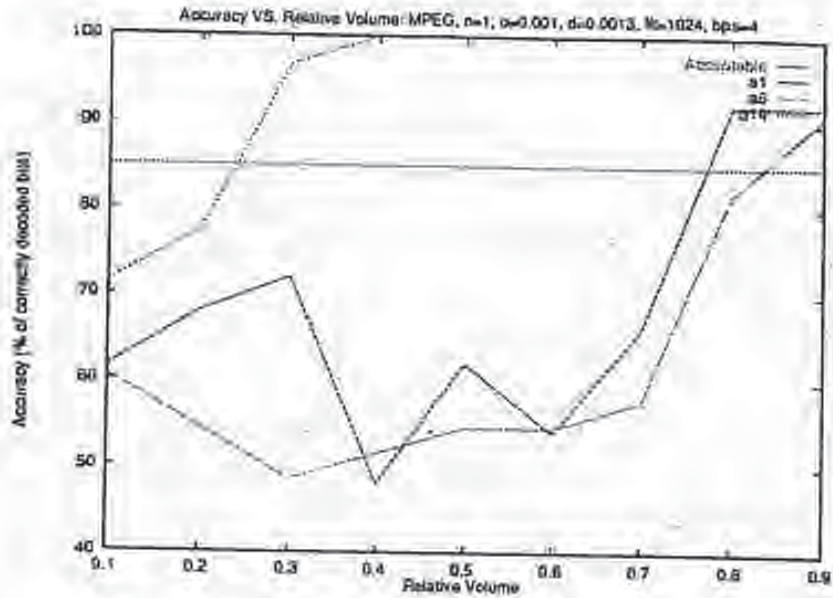


Fig. 16. Accuracy vs. relative volume: analog wire and MPEG

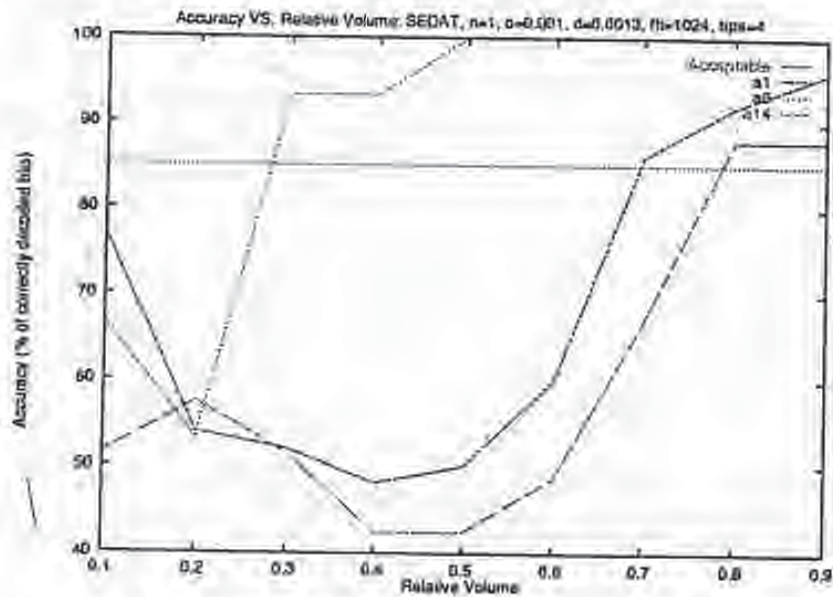


Fig. 17. Accuracy vs. Relative volume: analog wire and SEDAT

erimented
impression
impression
e recovery
ted by the

ed to pro-
oy means,
play a sig-
teractions
in area of
and delta
adio mak-

ing it increasingly difficult for the human observer to resolve the echo and the cover audio as two distinct signals. Offsets greater than 0.5 milliseconds produced acceptable recovery rates. The average listener cannot resolve the echoes with an offset of 0.001 seconds. Below a 0.5 millisecond offset, even the decoder had difficulty distinguishing the echo from the cover audio.

Extensive testing reveals that the two most important echo parameters are relative volume (decay rate) and offset. The relative volume controls the recovery rate. While the offset is the major factor in the perceptibility of the modifications.

The results illustrated in Figures 14 through 17 were obtained at sampling rates of 44.1 kHz (closed-loop) and 10 kHz (wire, MPEG, and SEDAT). Other sampling rates tested include 8 kHz, 16 kHz, and 22.05 kHz all yielding similar (but appropriately scaled) results.

As can be seen, echo hiding performs very well in situations where there is no additional degradation (such as that produced by D/A conversion, line noise or lossy encoding). In this respect, its performance is similar to many existing techniques. Its strength lies in its reasonable performance even in the much more challenging cases where such degradation is present.

At the present time, echo hiding works best on sound files without gaps of silence. This is unsurprising as it is difficult to analyze and recover echoes in regions of silence (such as inter-word pauses in speech). We are working on various thresholding techniques to try to avoid these difficulties by encoding only those areas where there is sound, and skipping areas of silence completely.

8 Future Work

Echo hiding can effectively place imperceivable information into an audio stream. Nevertheless, there is still room for improvement. We have been examining the use of different echoing kernels and their effect on recovery accuracy and echo perceptibility. In particular, we are actively researching both multi-echo kernels (adding another level of redundancy) and pre-echo kernels (echoing in negative time). With the old kernels, we are modifying the encoding process to be self-adaptive. Completion of these modifications will allow the encoding program to decide which parameters yield the highest recovery rate given the user's constraints on perceptibility and sound degradation. In addition, we will use echo hiding as a method for placing caller identification type information in real time over 8-bit, 8 kHz, analog phone lines.

9 References and Notes

1. W. Bender, D. Grubb, N. Morimoto, "Techniques for Data Hiding," Proc. of the SPIE, 2420/40, San Jose, CA., 1995.
2. W. Bender, D. Grubb, N. Morimoto, A. Lu, "Techniques for Data Hiding," To appear in IBM Systems Journal, Vol. 35, No. 3&4, 1996.
3. S. Baron, W. Wilson, "MPEG Overview," SMPTE Journal, pp 391-394, June 1994.

4. R. C. Dixon.
5. L. R. Rabin, Prentice-Hall, Inc.
6. A. V. Oppel, Prentice Hall, Inc.
7. Conversational Fixture.

Append

Much of the following is from the book *Discrete-Time Signal Processing* by Alan V. Oppenheim and Ronald W. Schaefer, 2nd Edition, Prentice-Hall, Inc., 1989.

A Cepstrum

Cepstral analysis is a technique for analyzing convolution operators. In convolution systems, the cepstrum consists of a cascade of all-pole filters. The cepstrum transform (\mathcal{F}), the inverse cepstrum transform (\mathcal{F}^{-1}), and



(F)

The operations in the frequency domain are performed in the time domain. In fact, we use the fast Fourier transform (FFT) to place us in the frequency domain, the inverse FFT to return us to the time domain, and the time-invariant (LTI) two functions. This is done using a slide rule simple addition by

the echo and the milliseconds resolve the echoes even the decoder

parameters are roles the recovery he modifications. ned at sampling SEDAT). Other yielding similar

is where there is ersion, line noise o many existing ven in the much

es without gaps d recover echoes are working on by encoding only completely.

an audio stream, a examining the uracy and echo uli-echo kernels oing in negative ocess to be self- ding program to the user's con- ve will use echo tion in real time

iding," Proc. of t Data Hiding," ial, pp 301-304,

4. R. C. Dixon, *Spread Spectrum Systems*, John Wiley & Sons, Inc., 1976.
5. L. R. Rabiner and R. W. Schaffer, *Digital Processing of Speech Signal*, Prentice-Hall, Inc., NJ, 1975.
6. A. V. Oppenheim and R. W. Schaffer, *Discrete-Time Signal Processing*, Prentice Hall, Inc., NJ, 1989.
7. Conversations with Scientific Atlanta regarding SEDAT Evaluation Test Fixture.

Appendix

Much of the following short tutorial was derived from Oppenheim and Schaffer's *Discrete-Time Signal Processing*. Please refer to the original text for a more complete discussion.

A Cepstrums

Cepstral analysis utilizes a form of a homomorphic system that converts the convolution operation to an addition operation. As with most homomorphic systems, the cepstrum can be decomposed into a canonical representation consisting of a cascade of three individual systems. These systems are the Fourier transform (\mathcal{F}), the complex logarithm (see Section C), and the inverse Fourier transform (\mathcal{F}^{-1}) as depicted in Figure 18.



Fig. 18. Canonical representation of a cepstrum

The operational conversion is the result of a basic mathematical property: The log of a product is the sum of the individual logs and multiplication in the frequency domain is identical to convolution in the time domain. To exploit this fact, we use the first system in the canonical representation of the cepstrum to place us in the frequency domain by taking the Fourier transform. In the frequency domain, the desired modifications are linear. The next system is a linear, time-invariant (LTI) system that takes the complex logarithm of the product of two functions. This simply becomes the sum of the logarithms. It is analogous to using a slide rule. In fact, the principle is the same. Multiplication becomes simple addition by first taking the logarithm. The final system puts us back in

the original (time) domain. In order to express the "conversion" mathematically, let's convolve two finite signals $x_1[n]$ and $x_2[n]$.

$$y[n] = x_1[n] * x_2[n] \tag{2}$$

After taking the Fourier transform of $y[n]$, we get:

$$Y(e^{j\Omega}) = X_1(e^{j\Omega})X_2(e^{j\Omega}) \tag{3}$$

Now, we take the complex log of $Y(e^{j\Omega})$

$$\log Y(e^{j\Omega}) = \log(X_1(e^{j\Omega})X_2(e^{j\Omega})) = \log X_1(e^{j\Omega}) + \log X_2(e^{j\Omega}) \tag{4}$$

Finally, we take the inverse Fourier transform.

$$\mathcal{F}^{-1}(\log Y(e^{j\Omega})) = \mathcal{F}^{-1}(\log X_1(e^{j\Omega})) + \mathcal{F}^{-1}(\log X_2(e^{j\Omega})) \tag{5}$$

By the definition of the cepstrum, this becomes (where $\tilde{x}[n]$ is the cepstrum of $x[n]$):

$$\tilde{y}[n] = \tilde{x}_1[n] + \tilde{x}_2[n] \tag{6}$$

Figure 19 illustrates the entire conversion process.

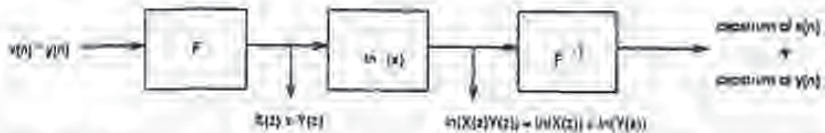


Fig. 19. Conversion of convolution in the time domain to the equivalent cepstral addition while still in the time domain

The inverse cepstrum is the reverse of the process described above and is depicted in Figure 20.



Fig. 20. Inverse cepstrum (canonical representation)

B Autocorrelat

Autocorrelation can i correlation of any fun

With a change of equation for the auto

Now let's rearrange that:

Recall that convol

There is a similar the "modified" autocor negation of time in th ically speaking, the a

If a signal is self-s) the autocorrelation of

In the frequency (b this becomes:

Using cepstrums, found by first taking The steps in this pro

Before we square wards, we take the in were finding the cepst frequency domain wh performs the operati



B Autocorrelation using cepstrums

Autocorrelation can be done while taking the cepstrum. Recall that the autocorrelation of any function $x[n]$ is defined as:

$$R_{xx}[n] = \sum_{m=-\infty}^{+\infty} x[n+m]x[m] \quad (7)$$

With a change of variable (letting $k=n+m$ and substituting $m=k-n$), the equation for the autocorrelation of a given function $x[n]$ becomes:

$$R_{xx} = \sum x[k]x[k-n] \quad (8)$$

Now let's rearrange the second term in the summation (the $x[k-n]$ term) so that:

$$R_{xx} = \sum x[k]x[-(n-k)] \quad (9)$$

Recall that convolution is defined as:

$$x[n] * h[n] = \sum_{k=-\infty}^{+\infty} x[k]h[n-k] \quad (10)$$

There is a similarity between the convolution equation (Equation 10) and the "modified" autocorrelation equation (Equation 9). The only difference is the negation of time in the second term of the autocorrelation equation. Mathematically speaking, the autocorrelation equation can be represented as:

$$R_{xx} = x[n] * x[-n] \quad (11)$$

If a signal is self-symmetric, $x[-n]$ is identical to $x[n]$ by definition. Therefore, the autocorrelation of a self-symmetric signal becomes:

$$R_{xx} = x[n] * x[n] \quad (12)$$

In the frequency domain (i.e. after taking the fourier transform of the inputs), this becomes:

$$S_{xx}(e^{j\Omega}) = (X(e^{j\Omega}))^2 \quad (13)$$

Using cepstrums, the autocorrelation of a self-symmetric function can be found by first taking the cepstrum of the function and then squaring the result. The steps in this process are depicted in Figure 21 and Figure 22.

Before we square the cepstrum, we first take the fourier transform. Afterwards, we take the inverse fourier transform. The reason is the same as when we were finding the cepstrum (Appendix A). The fourier transform places us in the frequency domain where modifications are linear. A linear system (x^2) actually performs the operation. Finally, the inverse fourier places us back in the time

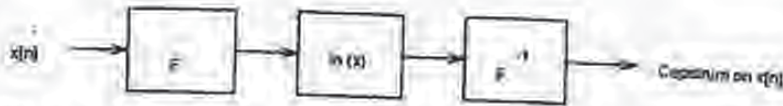


Fig. 21. The first step in finding the Cepstral Autocorrelation is to find the cepstrum of $x[n]$

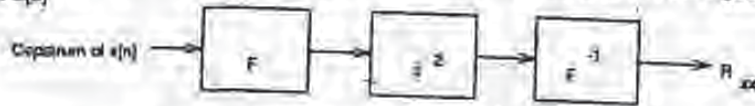


Fig. 22. Once we have the cepstrum, we square it

domain. The inverse fourier transform from step one (Figure 21) and the fourier transform from step two (Figure 22) will cancel each other when combined. In the end, we are left with the system shown in Figure 23.

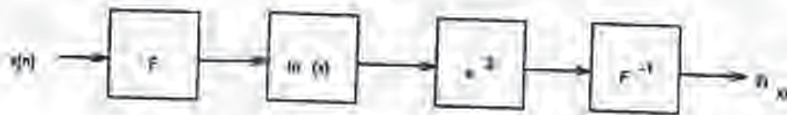


Fig. 23. Systems representation of Cepstral Autocorrelation

Autocorrelation is an order n^2 operation. Using the system in Figure 23, the operation is reduced to a $n \log(n)$ operation. Thus for large n , finding the autocorrelation while taking the cepstrum is much more efficient.

C Complex Logarithm

The fourier transform is a complex function of ω . It can be decomposed into magnitude and phase/angle terms. Thus, if we have some finite signal $x[n]$, the Fourier transform can be represented as a magnitude and an angle:

$$X(e^{j\Omega}) = |X(e^{j\Omega})|e^{j\text{ARG}X(e^{j\Omega})} \tag{14}$$

ARG (angle modulus 2π) is used instead of arg (angle) since adding 2π (where n is any arbitrary integer) to an angle has no effect:

$$e^{j(\omega+2n\pi)} = e^{j\omega}e^{j2n\pi} = e^{j\omega}(\cos 2n\pi + j \sin 2n\pi) = e^{j\omega} \tag{15}$$

In most cases, the phase will be a non-zero value. Therefore, we can not use the natural logarithm when taking the cepstrum (Figure 18). Instead, we must use the complex logarithm which is defined as:

$$\log X(e^{j\Omega})$$

Once again (as in Appendix A) the complex log is identical to the sum of the

$$\log X(e^{j\Omega}) =$$

Exploiting that log and e

$$\log X(e^{j\Omega})$$

In order to further motivate the use of the complex logarithm, let's mathematically re-examine convolution. We begin by first con-

Convolution becomes multiplication

$$Y(\omega)$$

Taking the complex log:

$$\log Y(\omega)$$

Finding the mathematical

$$\log Y(e^{j\Omega})$$

Now, we can substitute in

$$\log Y(e^{j\Omega}) = (\log |X_1(e^{j\Omega})| + k$$

The use of the complex log separates the magnitude and phase components instead of



$$\log X(e^{j\Omega}) = \log(|X(e^{j\Omega})|e^{j\text{ARG}X(e^{j\Omega})}) \quad (16)$$

Once again (as in Appendix A) we exploit the fact that the log of a product is identical to the sum of the individual logs:

$$\log X(e^{j\Omega}) = \log(|X(e^{j\Omega})|) + \log(e^{j\text{ARG}X(e^{j\Omega})}) \quad (17)$$

Exploiting that log and e^x are inverses, we get:

$$\log X(e^{j\Omega}) = \log|X(e^{j\Omega})| + j\text{ARG}X(e^{j\Omega}) \quad (18)$$

In order to further motivate the idea of converting from convolution to addition, let's mathematically re-examine Appendix A in light of the complex logarithm. We begin by first convolving two finite signals $x_1[n]$ and $x_2[n]$:

$$y[n] = x_1[n] * x_2[n] \quad (19)$$

Convolution becomes multiplication in the frequency domain:

$$Y(e^{j\Omega}) = X_1(e^{j\Omega})X_2(e^{j\Omega}) \quad (20)$$

Taking the complex log:

$$\log Y(e^{j\Omega}) = \log(X_1(e^{j\Omega})X_2(e^{j\Omega})) \quad (21)$$

Finding the mathematical equivalent:

$$\log Y(e^{j\Omega}) = \log(X_1(e^{j\Omega})) + \log(X_2(e^{j\Omega})) \quad (22)$$

Now, we can substitute the result from Equation 17 and rearrange to get:

$$\log Y(e^{j\Omega}) = (\log|X_1(e^{j\Omega})| + \log|X_2(e^{j\Omega})|) + (j\text{ARG}(X_1(e^{j\Omega})) + j\text{ARG}(X_2(e^{j\Omega}))) \quad (23)$$

The use of the complex logarithm in cepstral analysis allows the addition of signal components instead of the convolution of the signals.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGES CUT OFF AT TOP, BOTTOM OR SIDES

IMAGES WITH BLURRY IMAGES

IMAGES WITH UNREADABLE TEXT OR GRAPHICS

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

A Variable-Bit-Rate Buried-Data Channel for Compact Disc

A.W.J. Oomen, M.E. Groenewegen, R.G. van der Waal
and R.N.J. Veldhuis*
Philips Research Laboratories
P.O. Box 80000
5600 JA Eindhoven
The Netherlands

* R.N.J. Veldhuis currently works at the Institute for Perception Research

3833 (P9.4)

**Presented at
the 96th Conyention
1994 February 26 - March 01
Amsterdam**



AES

This preprint has been reproduced from the author's advance manuscript, without editing, corrections or consideration by the Review Board. The AES takes no responsibility for the contents.

Additional preprints may be obtained by sending request and remittance to the Audio Engineering Society, 60 East 42nd St., New York, New York 10165-2520, USA.

All rights reserved. Reproduction of this preprint, or any portion thereof, is not permitted without direct permission from the Journal of the Audio Engineering Society.

AN AUDIO ENGINEERING SOCIETY PREPRINT

A Variable-Bit-Rate Buried-Data Channel for Compact Disc

A.W.J. Oomen, M.E. Groenewegen, R.G. van der Waal and
R.N.J. Veldhuis*
Philips Research Laboratories
P.O.Box 80000
5600 JA Eindhoven
The Netherlands

Abstract

Recently, an elegant method was published to add buried data in a CD signal in a compatible way [1]. This method is based on subtractively dithered noise-shaped quantization, and provides a fixed-rate buried-data channel. In this paper we describe an adaptive extension to this method resulting in a variable rate of higher average value.

1 Introduction

To increase the amount of services provided via existing digital audio channels with fixed capacity, 'Buried-Data Channel' [1] or 'Hidden Channel' [2] techniques can be used. Recently, Gerzon and Craven proposed a method to add additional services to the current CD format, maintaining backward compatibility. The method is proposed for CD, but also applies to other digital formats, such as NICAM [3] and 14 bit PCM channels for TV or even speech channels. Possible additional services can be related to the audio signal, such as video, extra audio channels [2], speech, text (karaoke), and services can be unrelated to the CD-signal, such as signatures.

The additional service is encoded with the audio signal by means of a subtractively dithered noise-shaped quantizer. The dither is a reversible randomization of the additional service and is situated in the b Least Significant Bits (LSBs) of the encoded signal. On a conventional CD player, the process of encoding will have no audible effect. However, a special decoder can recover the additional service by extracting the b LSBs and feeding them through the inverse randomization process. For a fixed noise-shaping filter H and fixed quantizer stepsize $\Delta = 2^b$, a maximum fixed capacity for the additional service of 176.4 kbit/s is obtained. This capacity is limited by the worst case (zero) input signal.

*R.N.J. Veldhuis currently works at the Institute for Perception Research.

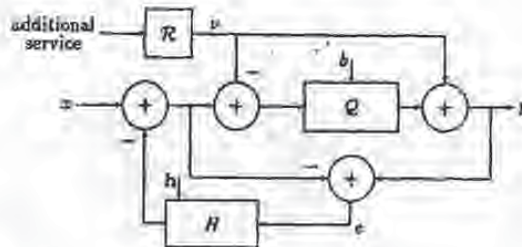


Figure 1: A subtractively dithered noise-shaped quantizer used as buried-data encoder [1].

In this paper it will be shown that higher average bit rates can be obtained by exploiting input-signal masking properties. We will describe an algorithm to determine the best settings for the noise-shaping filter and the stepsize under the restriction that the shaped error signal is below the masked-error power spectral density (psd).

In Section 2 the process of dithering and noise shaping used in a fixed bit-rate buried-data encoder is reviewed. The algorithm realizing the optimal variable bit rate is described in Section 3. Finally, in Section 4 the results of experiments with the adaptive algorithm will be discussed.

2 Fixed-rate buried-data encoder

In Fig. 1 the basic diagram of a subtractively dithered noise-shaped quantizer is depicted. It is used as a buried-data encoder [1].

The 16 bit audio signal x is uniformly quantized in Q with stepsize $\Delta = 2^b$ to form a $(16 - b)$ bits signal. A b bits dither signal v is produced from the additional service by randomizer \mathcal{R} [1]. The dither signal v is subtracted before and added¹ after the quantizer. The result of this action is that, under the condition that the dither v complies with the proper statistical properties [4], the quantiser error signal e is statistically independent of the input signal x . In a subtractively dithered quantizer, v must have a uniform probability density function (pdf) of width Δ [4]. In this particular case the pdf of v is chosen to be uniform in the range $[0, \Delta)$. The addition after the quantizer is then a replacement of the b LSBs which are zero, by the dither v . The decoder can simply recover the dither by extracting the b LSBs from y . Furthermore, the dither v is independent, resulting in a white power spectral density and variance $\Delta^2/12$ for the signal e . There is thus no additional noise due to the dither. Without the noise-shaping filter H , the encoded signal can be represented as

$$y = x + e, \quad (1)$$

¹Normally the dither is added prior to quantisation. For this application however, subtraction is more convenient in terms of complexity.

where e has zero mean. Due to the quantization, the noise level increases by an amount of $20 \log \Delta \approx 6b$ dB relative to the 16 bit noise floor in CD.

To minimize the audible effect of this increase in noise level, a noise-shaping filter H is applied. This filter is able to decrease the noise floor below $\Delta^2/12$ in spectral areas where the human ear is most sensitive. Since the noise-shaping filter shapes the white noise floor e and subtracts it from the input signal x , the Fourier transform of the encoded signal y satisfies

$$Y(\theta) = X(\theta) + (1 - H(\theta))E(\theta). \quad (2)$$

The encoded signal y is thus equal to the sum of the input signal x and a noise signal with psd

$$|1 - H(\theta)|^2 \frac{\Delta^2}{12}. \quad (3)$$

The transfer function $H(\theta)$ is optimized such that $(1 - H(\theta))$, which is the transfer function of a minimum-phase filter [4, 5] satisfying

$$\int_{-\pi}^{\pi} \log |1 - H(\theta)|^2 d\theta = 0, \quad (4)$$

renders the least audible noise floor. Since $(1 - H)$ is a minimum-phase filter, the minimum amount of noise given a certain power spectral density shape is obtained.

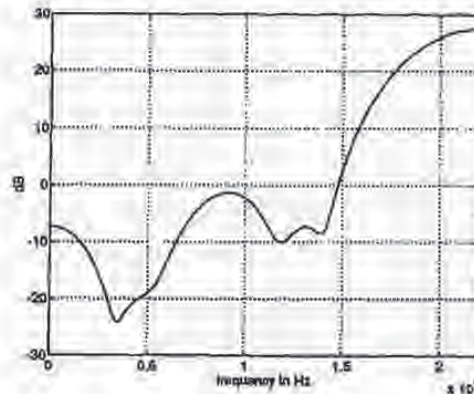


Figure 2: Psd of a minimum phase filter matching the threshold in quiet.

The noise must be inaudible for all input signals. For a fixed setting of H , informal listening tests on different noise-shaping curves revealed that the maximum amount of gain which can be obtained by noise-shaping is about 16 dB. This gain is limited by the worst case signal, namely a zero input. For an integer value of b , this allows a

maximum of $b = 2$ bits. From Fig. 2, displaying the psd of the optimized minimum-phase filter $(1 - H)$ [6], we see that the suppression at 4 kHz is down 24 dB. A possible explanation for the difference with the measured gain of 16 dB can be the following. According to [7], the threshold of detection for the combination of multiple targets, each presented at their individual threshold, lies below each of these individual thresholds. This decrease in the threshold is proportional to the square root of the number of detections. In a simple model with 25 critical bands [8] this results in a decrease of $\sqrt{25}$ corresponding with 7 dB.

In conclusion, the obtained bit rate of 2 bits per sample yields a buried-data channel with a capacity of $2(\text{bits}) \times 44.1(\text{kHz}) \times 2(\text{channels}) = 176.4 \text{ kbit/s}$. In the next section it will be shown how higher capacities can be obtained using a more sophisticated approach.

3 Algorithm for a variable bit rate

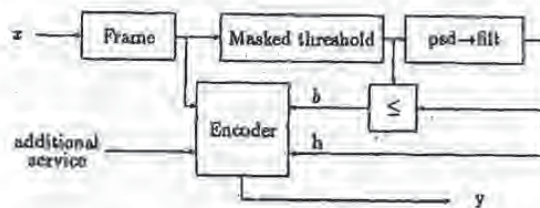


Figure 3: Algorithm block diagram.

An algorithm is used to compute the noise-shaping filter H and the number of bits b available for the additional service. A basic block diagram of the algorithm is given in Fig. 3.

The input signal x is analyzed in overlapping frames. For each frame, the masked-error psd is calculated according to an excitation model. The noise-shaping filter H has to be designed such that the shape of $|1 - H|^2$ matches the shape of the masked-error psd as good as possible. In addition, using a comparison on a critical-band grid,

$$|1 - H(\theta)|^2 \frac{\Delta^2}{12} \tag{5}$$

is raised as high as possible by increasing Δ , under the restriction that the noise remains below the masked-error psd. This results in a value for b for that frame.

Since the bit rate can vary between frames, there cannot be a fixed bit rate for all pieces of music. In order to be able to evaluate the variable bit rate, we define the bit

rate over N frames of a piece of music as

$$\bar{b} = \frac{1}{N} \sum_{i=1}^N b_i, \quad (6)$$

where b_i denotes the bit rate for frame i .

The calculation of the masked-error psd is discussed in Section 3.1. In Section 3.2 the calculation of the minimum-phase filter is elaborated. Section 3.3 will discuss the handling of transients. Section 3.4 will discuss how the values b_i are transmitted as part of the side information.

3.1 Masked-error psd

The masked threshold represents the detection threshold for a single tone in the presence of the input signal. The tone to be detected is also called the target. Instead of a single tonal target, the shaped noise can be thought to consist of multiple noise targets. Since the human ear seems to add up noise-targets within critical bands [8], the threshold for noise-targets within a critical band will be lower. These thresholds constitute the masked-error psd which is used to generate the noise-shaping filter H . The masked-error psd can be derived from the masked threshold.

In order to calculate the masked threshold, the samples within a frame are first Hanning windowed and subsequently Fourier transformed. The thus obtained estimate of the single sided psd is then convolved with the masking function, resulting in the masked threshold [8].

The masked-error psd is obtained by converting the masked threshold to the 1/3 octave equivalent threshold, corresponding to the critical-band size of the human ear [8]. For each frequency the masked threshold is multiplied by $2^{1/6} - 2^{-1/6} = 0.2316$. This operation is equivalent to tilting the original masked threshold curve -3 dB per octave.

3.2 Adaptive minimum-phase filter

In conventional filter-design methods such as [9, 10], the target filter is specified on a uniform grid. Since the comparison between the masked-error psd and the shaped noise-floor takes place on a critical-band grid, it seems logical to specify the target filter on a non-uniform grid as well. For other applications we had already developed a filter-design method, which allows specification on a non-uniform grid. This method is described next. In Section 4 we will comment on the usefulness of this approach.

The procedure for calculating the adaptive filter H is organized such that the filter curves $F(\theta) = (1 - H(\theta))$ are 'minimum-phase' FIR filters. The filter H has at least one delay [5] and uses q coefficients. We thus have

$$H(\theta) = \sum_{i=1}^q h_i e^{-j\theta i}. \quad (7)$$

The filter coefficients h_i are optimized such that $F(\theta)$ matches the masked-error psd $S(\theta)$ as good as possible.

With $\mathbf{h} = [h_1 \cdots h_q]^T$, this optimization is equivalent to minimizing

$$Q(\mathbf{h}) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1}{S(\theta)} |F(\theta)|^2 d\theta, \quad (8)$$

by calculation of

$$\frac{\delta Q(\mathbf{h})}{\delta h_l} = 0, \quad l \in \{1, \dots, q\}. \quad (9)$$

Equation (8) is minimal in the case that $F(\theta)$ is a minimum-phase filter. In order to obtain an analytical expression for better evaluation of the integral (8), $1/S(\theta)$ is approximated by a weighted sum of windows $S_k(\theta)$. As a result we have

$$\frac{1}{S(\theta)} \approx \sum_{k=1}^m t_k S_k(\theta). \quad (10)$$

For the windows $S_k(\theta)$ we choose cosine-shape windows

$$S_k(\theta) = \begin{cases} \frac{\pi}{2\Delta_k} (1 + \cos(\frac{\pi}{\Delta_k}(|\theta| - \theta_k))), & \theta_k - \Delta_k \leq |\theta| < \theta_k + \Delta_k \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

where θ_k and Δ_k represent the center and the width of the window S_k . The approximated inverse masked-error psd is thus described by m weighting factors t_k which are obtained from the original masked-error psd by sampling on the grid θ_k . Inserting (10) in (8) and evaluation of (9) results in

$$\sum_{l=1}^q \sum_{k=1}^m t_k \frac{1}{2\pi} \int_{-\pi}^{\pi} S_k(\theta) e^{j\theta(n-l)} d\theta = - \sum_{k=1}^m t_k \frac{1}{2\pi} \int_{-\pi}^{\pi} S_k(\theta) e^{j\theta n} d\theta, \quad n \in \{1, \dots, q\}, \quad (12)$$

and can be reduced to

$$\sum_{k=1}^m h_k \rho_{k,n} = -\rho_n, \quad n \in \{1, \dots, q\}, \quad (13)$$

with

$$\begin{aligned} \rho_n &= \sum_{k=1}^m t_k \rho_{k,n}, \quad n \in \{1, \dots, q\}, \\ \rho_{k,n} &= \frac{1}{2\pi} \int_{-\pi}^{\pi} S_k(\theta) e^{j\theta n} d\theta, \quad n \in \{1, \dots, q\}. \end{aligned} \quad (14)$$

Defining the $q \times q$ matrix \mathbf{R} by

$$r_{i,j} = \rho_{i-j}, \quad i, j \in \{1, \dots, q\}, \quad (15)$$

and the vector \mathbf{r} of length q by

$$r_i = \rho_i, \quad i \in \{1, \dots, q\}, \quad (16)$$

we can rewrite (13) into the matrix vector equality

$$\mathbf{R}\mathbf{h} = -\mathbf{r}. \quad (17)$$

The noise-shaping filter coefficients h_l can now be solved from (17) by applying the Levinson-Durbin algorithm [11]. The $\rho_{k,n}$ can be calculated in advance since they only depend on θ_k and Δ_k which are fixed for the procedure.

3.3 Handling of transients

When compared with psycho-acoustic time constants governing the detection of short events, the frames are relatively long, (e.g. 20 ms versus 2–5 ms) [12]. Consequently, if the input signal has a transient behavior, it can occur that in the encoded signal artefacts are audible in the passages just before or after the transient.

To prevent this, the algorithm is extended with a test on the presence of a sudden increase of power. Such an attack is detected if the position of the center of gravity of the total power in a frame exceeds certain bounds. One strategy, which is found effective in all situations tested, is that if an attack is encountered, b_i is taken equal to the previous setting b_{i-1} .

3.4 Side information

Due to the adaptivity of our system, the bit rate b_i can be different for each frame. The decoder must know the current setting for b_i in order to extract the correct number of LSBs from the encoded signal. Side information is necessary to enable the decoder to find the frame boundaries and the local setting for b_i .

Since the decoder has no a priori knowledge of b_i , the side information must be decodable independently of b_i for every frame. The capacity of the buried-data channel can vary between 2 and a maximum b_{max} bits. Hence a capacity of two LSBs is always available and of this, a fixed portion can be used for side information. In order to satisfy the independent decodability requirement, the variable-rate channel of b_i bits is split into a fixed rate channel of 2 bits and a variable-rate channel for the remaining $b_i - 2$ bits. Instead of applying one randomizer \mathcal{R} as in [1], two separate randomizers are used. Randomizer \mathcal{R}_1 for the channel of 2 LSBs and \mathcal{R}_2 for the channel of the remaining $b_i - 2$ bits. Experiments have shown that the dither ν generated in this way is sufficiently random.

This approach requires the decoder to first retrieve the side information from the fixed channel. Until b_i has been decoded, the receiver has to store the buried data for its largest possible width b_{max} . Only then this buffered data and the following data can be interpreted for the correct b_i . The buffering results in a small delay.

4 Experiments

Initially, the adaptive noise-shaping filter H was designed using a critical-band grid. On a critical-band grid, at high frequencies the distance between two frequency points is large. As a consequence, the matching of the filter with the target filter around these frequencies is poor, resulting in a suboptimal filter. Therefore we used the filter-design method described in Section 3.2, but with the target filter specified on a uniform grid.

As discussed in Section 2, the minimum number of LSBs available for the additional service equals 2. By allowing H and the quantizer stepsize Δ to adapt, bit rates b_i in the range of 2–11 were obtained. In the cases where the algorithm selects high values for b_i , we notice that the spectrum flattens and thus the high frequency boost is moderate. Still, the high-frequency noise is significantly above $\Delta^2/12$ and although

(If the noise appears inaudible, it is not clear what the consequences are for listeners and equipment). For this reason the maximum allowed value for b_1 is somewhat arbitrarily set to 8.

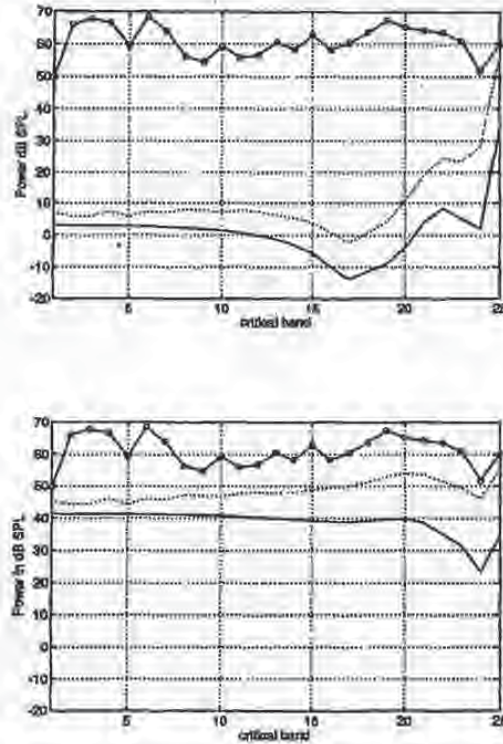


Figure 4: Fixed noise-shaping filter H with $b_1 = 4$ (top graph) and adaptive noise-shaping filter H with $b_1 = 8$ (bottom graph). The curve marked with dots is the masked threshold, the solid curve is the pad of $(1 - H)$ and the dotted curve is the +3 dB per octave tilted version of the solid line.

Leaving the filter curve H fixed and only adapting Δ , leaves much buried data.

capacity unused. Allowing the filter H to adapt to the masked-error psd, this capacity is exploited to a higher extent. This is recognized in Figure 4, which demonstrates this potential gain. In these graphs the masked-threshold and the shaped-error psd are sampled on a critical-band grid. In the top graph the fixed noise-shaping filter described in Section 2 is used. In the bottom graph the adaptive filter is used, yielding an extra 4 bits for the additional service.

To illustrate the global performance of the algorithm, Fig. 5 displays the time signal in combination with the values for b_i for 400 frames in sequence.

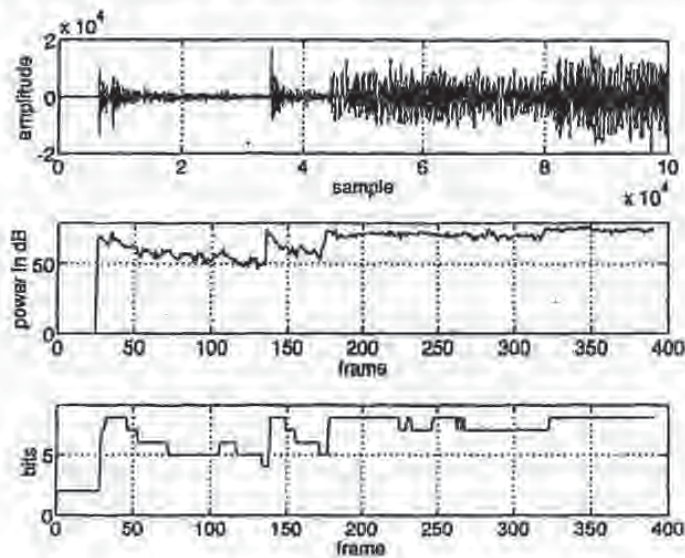


Figure 5: The upper graph is the time signal of 2.26 sec audio. The lower graph represents the bit rate b_i as a function of the frame number i . For reference the power in blocks of 256-samples is shown in the middle graph. Its correlation with b_i is striking.

The aforementioned results are typical: we have processed many musical pieces of different kinds and from this we conclude that average bit rates of 5 to 6 bits per sample are feasible. This corresponds to a variable bit rate of about 500 kbit/s for a stereo buried-data channel.

5 Conclusion

We have presented a buried-data channel-encoder. This encoder exploits input-signal masking properties by using an adaptive noise-shaping filter and a variable quantizer stepsize. In this way, higher variable bit rates are obtained than with conventional techniques using a fixed filter and fixed stepsize. Typical variable bit rates of 500 kbit/s have been realized. It is possible to convert the variable bit rate into a more constant bit rate by applying buffers.

Our encoder will be more complex than the conventional encoder. However, encoding is an action which has to be done only once during the processing of the CD. Also the complexity of the decoder will be slightly higher, since the side information has to be retrieved.

We also presented a method for designing a minimum-phase filter where the target filter is specified on an arbitrary grid.

Further research has to be done to investigate the consequences of high-level apparently inaudible noise.

References

- [1] Michael A. Gerzon and Peter G. Craven,
A High-rate Buried Data Channel for Audio CD.
94th Convention of the AES, Berlin, 1993 March 16-19, preprint 3551.
- [2] W.R.T. ten Kate, L.M. van de Kerkhof and F.P.M. Zijderfeld,
A New Surround-Sound Coding Technique.
J. AES, Vol. 40, p376-383, 1992 May.
- [3] J.R. Emmett,
Buried Data in NICAM Transmissions.
92nd Convention of the AES, Vienna, 1992 March 24-27, preprint 3260.
- [4] Stanley F. Lipshitz, Robert A. Wannamaker and John VanderKooy,
Quantization and Dither: A Theoretical Survey.
J. AES, Vol. 40, p355-375, 1992 May.
- [5] Michael A. Gerzon and Peter G. Craven,
Optimal Noise Shaping and Dither of Digital Signals.
87th Convention of the AES, New York, 1989 Oct. 18-21, preprint 2822.
- [6] Robert A. Wannamaker,
Psychoacoustically Optimal Noise Shaping.
J. AES, Vol. 40, p611-620, 1992 Jul./Aug.
- [7] W.M. Hartmann,
Temporal Fluctuations and the Discrimination of Spectrally Dense Signals by Human Listeners.
Auditory processing of Complex sounds.

- [8] Raymond N.J. Veldhuis,
Bit Rates in Audio Source Coding.
IEEE J. Select. Areas Commun., vol. 10, pp.86-96, 1992 Jan.
- [9] J.S. Lim and A.V. Oppenheim,
Advanced Topics in Signal Processing.
Prentice Hall, Englewood Cliffs, New Jersey, 1988.
- [10] Stanley P. Lipshitz, Tony C. Scott and John VanderKooy,
Increasing the Audio Measurement Capability of FFT Analyzers by Microcomputer Post-Processing.
74th Convention of the AES, New York, 1983 Oct. 8-12, preprint 2050.
- [11] S.L. Marple,
Digital Spectral Analysis with Applications.
Prentice Hall, Englewood Cliffs, New Jersey, 1987.
- [12] Brian C.J. Moore,
An introduction to the psychology of hearing.
Academic Press, London, 1989.

A New Surround–Stereo–Surround Coding Technique*

W. R. TH. TEN KATE, *AES Member*, L. M. VAN DE KERKHOFF, AND F. F. M. ZIJDERVELD

Philips Research Laboratories, 5600 JA Eindhoven, The Netherlands

A new technique is described in which a stereo signal (two-channel) is derived from a multichannel surround-sound signal without the original multichannel information being lost. There are no restrictions on the way in which the down mix to two channels takes place. An extra code is generated which contains the information required for the expansion to the multichannel version, and this code is added inaudibly to the down-mixed signal. An inaudible addition is possible because of the masking properties of human hearing. By retrieving from the stereo signal the information added, it is possible to produce again the original multichannel surround-sound sensation. The technique is very suitable for application in HDTV: a surround-sound signal can be down-mixed to a compatible stereo signal. Because of the compatibility, stereo reception is possible. By equipping the receivers with additional electronics, however, the surround-sound signal can also be decoded from this stereo signal. Multichannel surround-sound reception is thus obtained over a two-channel transmission path.

0 INTRODUCTION

The trend is for cinema films to have multichannel sound [1], as this improves the listening experience of the public. High-definition television (HDTV) will therefore also have multichannel audio [2]. Typically, four or five channels are thought of. The bandwidth available is however limited. In addition, people may be satisfied with stereo sound for their television set and may not want a multichannel audio system in the home.

This paper presents an elegant solution to this problem. The basis of this is a multichannel recording. From this recording a two-channel down mix is now made, which is suited for stereo reproduction. In order to enable the retrieval of the original multichannel signal, additional channels are required. These are also generated during the down mix. The solution proposed now mixes these additional information signals inaudibly in the stereo down mix created. This can be done by using the masking effect. The information signals are added so that they are under the masked threshold which the audio signals generate, which means that they are not audible to the human ear. However, the information added can be detected electronically and

the original multichannel effect can thus be called up again from the two-channel stereo signal at the receiver end.

The method thus enables optimization of the stereo down mix for two-channel reproduction. After the addition of the information signals, a two-channel signal is formed which is fully compatible, that is, it can be processed by any (stereo) receiver. Mono compatibility is also guaranteed with this method. Extension of the receiver with extra electronics now enables the detection of the multichannel recording. However, two channels are used for the transmission.

This paper is divided into two sections. The first describes the technique of adding data inaudibly to an audio signal [3], while the second describes in greater detail how this technique can be used to achieve a surround–stereo–surround coding system.

1 ADDING INFORMATION INAUDIBLY TO AUDIO SIGNALS

1.1 Adding and Retrieving Data

The basic principle is that the existence of the masking effect in fact means that another weaker signal can be added inaudibly to any audio signal. The masking effect is a psychoacoustic phenomenon where the hearing threshold for sounds shifts upward as a result of the presence of other, louder sounds. This has been studied and is still subject to further study [4], [5]. Masking

* Manuscript received 1991 April 30; revised 1991 November 11. A German version of this paper appeared in *KTA*, vol. 35, pp. 10–16 (1991).

works best on sounds whose spectral components are close to those of the masking sound, but also occurs for components further away. The effect decreases more quickly toward lower frequencies than toward higher ones. The same is true for the time behavior; the masking is greatest for sounds which occur simultaneously, but can also be perceived in the time intervals shortly before and after the masking sound is supplied.

As stated, it can be deduced from the masking effect that there are signals which can be added inaudibly to an audio signal. The momentary power spectrum of these signals should therefore remain at all times under the masked threshold of that point in time. This means therefore that a data flow (series of bits) can also be added, that is, by constructing a signal of this kind from these bits. This can be done in the following way (see Fig. 1).

In order to use the masking effect, the signal is first split into subbands by means of filtering. The samples in each subband are then grouped into consecutive time windows (of approximately 10 ms in length). The windows from all subbands which represent the same time interval form blocks. For each block the power spectrum is calculated, which is then used to determine the masked threshold in each subband [6]. From this the maximum permitted power of a signal to be added can be obtained per subband, so that this can be constructed from the data flow. After the addition the subband signals are joined together again by a reconstruction filter bank to form a wide-band signal. On the premise that the implemented scheme determines the masked threshold correctly, the resulting wide-band signal will sound the same as the original audio signal. In the paper it is assumed that the used masking model is correct. Extensive listening tests, however, have confirmed this [7].

The signal to be added from the data flow and the set masked threshold is constructed as follows. A certain

number of consecutive bits from the data flow are taken together to form words. Each word is interpreted as an address which indicates a unique sample value, as shown in Fig. 2. The series of bits is therefore converted into a series of samples via this word series. These data samples are then grouped into windows and added to the corresponding samples in the subband window of the original audio signal.

The number of bits n_b which are used to form one word depends on the set masked threshold in the subband and the difference Δ_b between the consecutive sample values (see Fig. 2; Δ_b will be indicated in the following by the bit step size). By assuming that the incoming series of bits has a uniform probability density distribution, a power

$$\hat{P}_b = (2^{2n_b} - 1) \frac{\Delta_b^2}{12} \quad (1)$$

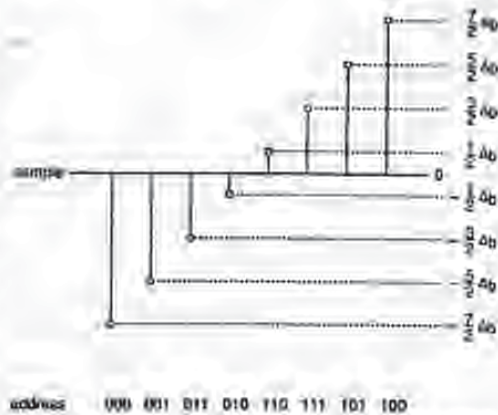


Fig. 2. Example as illustration of data sample construction with 3-bit words.

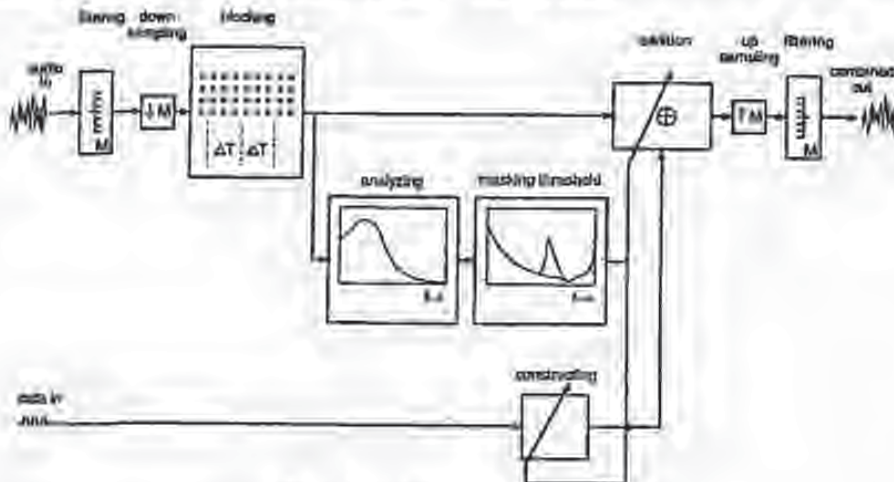


Fig. 1. Basic diagram for data addition.

can be assigned to each window of samples constructed in this way. With a given bit step size Δ_b , the number of bits per word is thus obtained from Eq. (1) as the maximum number n_b that still supplies a power under the set masked threshold in the corresponding subband. How the size of Δ_b is determined is discussed in Sec. 1.2.

The signal constructed in this way will have a power spectrum, the height of which is given by Eq. (1), but which is extended over the whole frequency range. However, the addition of the data signal at subband level limits the width of this spectrum to that of the subband. The grouping in subband time blocks is thus used not only to determine the masking properties of the audio signal, but also to modify the frequency-time characteristic of the data signals to be added.

The schematic diagram for retrieving the data added from the audio signal produced is shown in Fig. 3. The audio signal is first filtered in subbands and grouped in time windows, so that the same blocks are formed again (the filter banks to be used are of the (nearly) perfect reconstruction type [8]). After the position of the masked threshold has been determined, the sample values are extracted from the data signal as they were constructed during the addition. From the position of the masked threshold, the number of bits n_b that was added is again determined using Eq. (1). Finally, by using the same addressing table as that used during the addition (Fig. 2), the conversion in bit words can be made which, by placing them one after the other, again from the original data flow. Retrieval is thus obtained.

In order to distinguish between the added data sample value and the original audio sample value, it is necessary to apply a reference level in the combined signal. A level of this kind can be achieved by first quantizing the audio samples before carrying out the addition. In this case, quantizing can be described as

$$Q(x) = \Delta_Q \cdot \text{ROUND}(x/\Delta_Q) \quad (2)$$

where x is the value of the sample to be quantized, $Q(x)$ its value after quantization and Δ_Q the quantization step size. In order to distinguish between audio sample value and data sample value, a step size Δ_Q should be used which is greater than the range of possible data sample values:

$$\Delta_Q > 2 \frac{2^{n_b} - 1}{2} \Delta_b \quad (3)$$

The data sample value can then be recognized as the "quantization noise," which results from quantizing the combined sample again (see Fig. 4).

The quantization of the audio signal reduces the accuracy of its representation, and this can be modeled as an increase in its noise level. Because the quantization has been used on a time-limited subband signal, this noise is however masked as long as its power remains under the masked threshold. (This property is also used with bit-rate reduction techniques [6].) The noise power is given as [9]

$$P_Q = \frac{\Delta_Q^2}{12} \quad (4)$$

Because the quantization noise and the data signal are not correlated, the total power to be masked is obtained from the sum of their respective powers, given by Eqs. (1) and (4). Using Eq. (3), this power can be written as

$$P_t = P_b + P_Q < \frac{\Delta_Q^2}{6} \quad (5)$$

The addition and retrieval parameters Δ_Q and n_b can therefore be determined as follows. After determining the masked threshold, the maximum possible quantization step size Δ_Q is determined using Eq. (5). The maximum number of n_b bits which can be added is

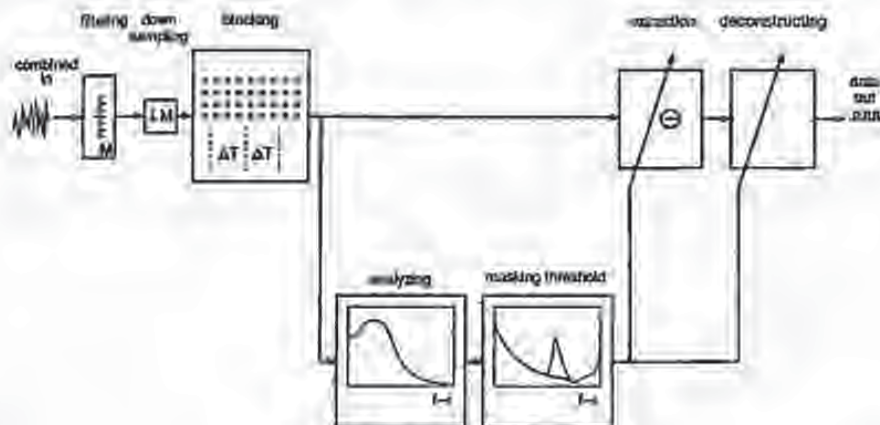


Fig. 3. Basic diagram for data retrieval.

then obtained from Eq. (3).

The resulting addition process can also be viewed as follows. It is determined for each sample value which part of its representation is significant and which part is not. This distinction is made possible by the masking effect: only a limited accuracy can be detected by the human ear. The insignificant part of the signal is then replaced by a different value, which indicates the information to be added.

1.2 Noise

The starting point is that the processing takes place with digital audio signals. This means that the combined signal produced will be quantized after the final filtering to a wide-band signal (see Fig. 1) in the representation accuracy of the transmission channel over which it will be sent. This creates quantization noise with, in the case of a channel with a linear quantization (PCM), a flat spectrum (that is, over the whole audio band) and a power P_N of [9]

$$P_N = \frac{\Delta_{ch}^2}{12} \tag{6}$$

in which Δ_{ch} indicates the quantization step size of the transmission channel.

The audio signal is filtered again in subbands at the receiver end (see Fig. 3). This affects the channel quantization noise in two ways. First, the probability density distribution of the noise will change into a Gaussian one and second, the power in each subband will decrease in proportion to the bandwidth of this subband. Thus in the case of a perfect transmission channel and a filtering in M subbands of equal width, the subband samples received have a noise component with a probability density function

$$p(\epsilon) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\epsilon^2}{2\sigma^2}\right) \tag{7a}$$

where ϵ is the magnitude and σ the standard deviation. σ is given by

$$\sigma = \sqrt{\frac{\Delta_{ch}^2}{12M}} \tag{7b}$$

It is this standard deviation σ which determines the selection of the bit step size Δ_b in Eq. (1).

The data bits are recovered by converting the data samples received back to their address bit words according to a procedure as shown in Fig. 2. As a result of the noise, faults may occur in this process. By the use of a Gray code conversion [9] (Fig. 2) only 1 bit will toggle in the bit word each time the noise exceeds a decision threshold. (These thresholds lie in the middle between the noise-free sample values.)

Using Eq. (7a) an estimate can now be made of the error probability that n bits will be converted incorrectly ($n > 1$):

$$P(n) = \int_{-\infty}^{-(n-1)\Delta_b} p(\epsilon) d\epsilon + \int_{(n-1)\Delta_b}^{\infty} p(\epsilon) d\epsilon \\ = 1 - \operatorname{erf}\left(\frac{2n-1}{2\sqrt{2}} \frac{\Delta_b}{\sigma}\right) \tag{8}$$

Thus with σ according to Eq. (7b), Δ_b can be set for a certain error probability $P(n)$. On the other hand, Δ_b affects the number of bits n_b that can be added [see Eq. (3)]. As a result there is a tradeoff between n_b and $P(n)$.

In fact, the audio signal itself can be regarded as a "channel" over which the data are transported. A channel capacity C can then be defined as

$$C = \frac{1}{M} \sum_{m=0}^{M-1} n_{b,m} \tag{9}$$

where M is the number of subbands; and $n_{b,m}$ is the number of added bits per sample in subband m . According to Eq. (3), $n_{b,m}$ follows as

$$n_{b,m} = \operatorname{TRUNC}\left[2 \log\left(\frac{\Delta_{Q,m}}{\Delta_{b,m}} + 1\right)\right] \tag{10}$$

in which $\Delta_{Q,m}$ and $\Delta_{b,m}$ are the quantization step size and bit step size in subband m , respectively. If the subbands are all of equal width, then the channel noise σ [Eq. (7b)] is of equal strength in each subband and $\Delta_{b,m}$ can thus be taken the same in each subband [Eq.

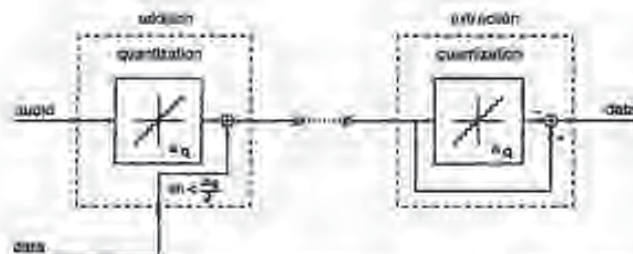


Fig. 4. Addition and extraction blocks from Figs. 1 and 3 in greater details.

(8), $\Delta_{b,m} = \Delta_b = C_b \sigma$. Eq. (9) can now be written as

$$C = \frac{1}{M} \sum_{m=0}^{M-1} \text{TRUNC} \left[{}^2\log \left(\frac{\sqrt{12M}}{C_b} \frac{\Delta_{Q,m}}{\Delta_b} + 1 \right) \right] \\ \approx {}^1\log \frac{\sqrt{12M}}{C_b} + \frac{1}{M} \sum_{m=0}^{M-1} {}^2\log \Delta_{Q,m} - {}^2\log \Delta_b. \quad (11)$$

The first term reflects the effect of the channel noise. An increase in the parameter M , that is, splitting up the signal into more subbands, reduces the noise contribution in each band, which means that more bits can be added. This increases the complexity of the system and also the delay of the audio signal as a result of the narrow-band filtering. The coefficient C_b takes into account the tradeoff between the number of bits added and the error probability occurring. The second term indicates the masking effect of the audio signal: the greater the masking, the greater Δ_b , and thus the more information can be added. (As a result of the filtering, addition is also possible if some bands have $\Delta_{Q,m} = 0$.) The third term indicates that an increase in the representation accuracy of the audio signal increases the channel capacity by approximately the same size. For example, representation with 18 bits instead of 16 (linear PCM) means a four-times reduction of Δ_b and thus an increase of C by 2 bits. (It is assumed here that addition has already taken place in each subband.) In the case of a transmission channel in which the representation accuracy varies, such as, for example, in NICAM [10], it may be useful to normalize $\Delta_{Q,m}$ by $\Delta_{Q,0}$ to a new parameter, which means that the varying property can then be eliminated.

As stated, (nearly) perfect reconstruction filter banks are used [8]. This is necessary to ensure that the (subband) sample values used in the retrieval are (almost) the same as those which occurred after the addition (except for the wide-band quantization noise). In the filter structures used up and down sampling takes place (Figs. 1 and 3). This makes the system a multirate system. For a proper functioning the total delay between the two filters on both sides of the transmission channel must be a complete number of times the highest down-sampling factor (M). In that case the delay at subband level is also a complete number of sample periods. Consequently, synchronization is required at the receiver end (processing in windows also makes this necessary). By up and down sampling, this syn-

chronization seems to be no longer required. However, the perfect reconstruction property will then be lost. Because of the processing (quantizing and adding) the spectrum of the subband samples changes over the whole bandwidth (given by the sampling frequency), while their filters only allow through the part in the corresponding subband. These two only coincide when sampling at the critical rate, and only then is perfect reconstruction possible. (The filter sequence for which the (nearly) perfect reconstruction property must apply is synthesis analysis, that is, the reverse to what the filter banks were designed for [8]. The fact that in this case the perfect reconstruction property is also valid can be seen by looking at the analysis-synthesis-analysis cascade. The first two filters form a perfect reconstruction pair as they were designed. The signals at the input of both analysis filters are therefore identical. Because the analysis filters are the same, it follows that the synthesis-analysis pair must also be a perfect reconstruction pair.)

A different approach to the one stated here is Nyquist's first criterion. From this it also follows that with an ideal bandpass filter no intersymbol interference occurs if the symbols are on (a multiple of) the critical rate (and are detected synchronously).

3 COMPATIBLE CODING

3.1 The Principle

Using the technique presented, a surround-stereo-surround coding system can now be developed which is very suitable for use in HDTV. Multichannel audio can be sent over a stereo transmission channel so that stereo reception is possible without additional modification, while there is the possibility of surround reception with a receiver equipped with additional electronics. In the following it will be assumed that the HDTV audio consists of five audio channels.

Fig. 5 shows the principle of the system. The programs are supplied with five-channel sound. A down mix to two-channel stereo is then made from this version. There are no restrictions on the way in which this down mix is made, that is, a signal with an optimum stereo effect can be produced. In addition to the stereo signal, a three-channel (audio) signal is also generated which, together with the stereo signal, contains all the information on the original five-channel composition. These information signals are then added to the stereo signal according to the technique described in Sec. 1 and retrieved at the receiver end.

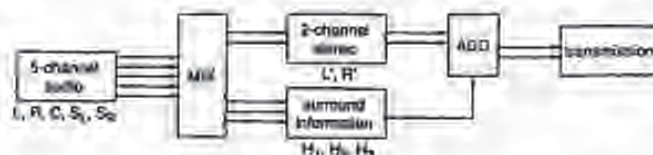


Fig. 3. Proposed coding scheme.

Because of the identical format, the signal transmitted is compatible and existing receivers can still be used. Reproduction of this signal will give the listener the stereo sensation as it was optimized during the down mix. Of course, the extra information is also reproduced but, because of the masking effect, the listener is not aware of this. This information is however still available by means of the technique described. The receiver must be expanded for this with additional electronics. After retrieving this information, the down mix carried out can be reversed, which means that the reproduction of the five-channel surround-sound sensation becomes possible.

2.2 The System

The original five audio channels are indicated with L , R , C , S_L , and S_R . Of these the first two signals are thought to be supplied to loudspeakers which are on the left and right of the video screen, respectively, the third (central) signal to a loudspeaker near the screen, and the latter two signals (surround) to the loudspeakers behind the listener (see Fig. 6). A stereo down mix could be

$$L' := L + \frac{1}{2} \sqrt{2} C + S_L \tag{12a}$$

$$R' := R + \frac{1}{2} \sqrt{2} C + S_R \tag{12b}$$

(Other possibilities are conceivable.) Numerous signals can store the surround information here, but one possibility is

$$H_1 := C \tag{12c}$$

$$H_2 := S_L \tag{12d}$$

$$H_3 := S_R \tag{12e}$$

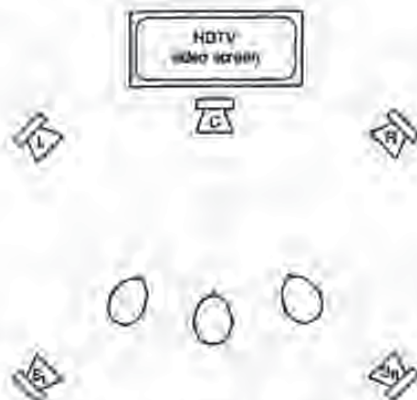


Fig. 6. Loudspeaker setup for five-channel surround sound.

In this case it is, of course, sensible to use first data reduction on C , S_L , and S_R [6]. The L' and R' signals are processed according to the method described in Sec. 1, and the information H_1 , H_2 , H_3 is added. After retrieving this information, the down mix can be reversed and the five-channel sensation can be produced again:

$$L'' := L' - \left(\frac{1}{2} \sqrt{2} H_1 + H_2 \right) \tag{13a}$$

$$R'' := R' - \left(\frac{1}{2} \sqrt{2} H_1 + H_3 \right) \tag{13b}$$

$$C'' := H_1 \tag{13c}$$

$$S_L'' := H_2 \tag{13d}$$

$$S_R'' := H_3 \tag{13e}$$

A problem may occur as a result of this dematrixing. During the addition of the information, a quantization must be carried out (see Sec. 1.1). This quantization is carried out on the subband samples of L' and R' and in such a way that the resulting quantization noise is masked by these audio signals and thus remains inaudible. The stereo signal including the added information thus still creates the same listening experience. Dematrixing [Eqs. (13)] can however separate the audio signal from the quantization noise, which means that the noise could become audible. The effect becomes clear by looking at a silent channel (and switching off the other loudspeakers when listening). Assume, for example, that all channels with the exception of channel C are silent. In that case L' and R' are both equal to $\frac{1}{2} \sqrt{2} C$ [see Eqs. (12a,b)]. These signals are quantized and H_1 ($= C$), H_2 (silent) and H_3 (silent) are added. After retrieval, C , S_L , and S_R are determined from H_1 , H_2 , and H_3 . The result is used to reverse the down-mixing. This dematrixing will remove $(\frac{1}{2} \sqrt{2} H_1 + H_{2,3}) = \frac{1}{2} \sqrt{2} C$ from L'' and R'' [see Eqs. (13a,b)]. As a result of this the quantization noise produced during the addition procedure remains in the left and right channel L'' and R'' , while the signal that masked this noise, $\frac{1}{2} \sqrt{2} C$, is now transmitted to another loudspeaker, C'' . Because the audio signal is still present, it will still have a masking effect on the quantization noise, though this will be less effective than if they were both generated by the same loudspeaker.

A remedy is to expand the information signals $H_{(1,2,3)}$ with some extra control information. This information then indicates which channels are silent, so that after dematrixing, any residual sound can be removed from these channels. Possibly the information is given for every subband separately. In addition, instead of always coding C , S_L , and S_R in H_1 , H_2 , and H_3 , it is better to take the weakest three of L , R , C , S_L , and S_R . This ensures that the quantization noise is always in those

signals which give the greatest masking and therefore that the chance of its audibility is limited. The choice made is added as control information to $H_{(2,2)}$ and used during dematrixing. Informal listening tests on various types of program material have proven the validity of this procedure. Only by switching off some channels, it could occur that noises in the other channels became audible. Those cases only happened with especially constructed signals. Common audio signals did not reveal any problem.

A complete abundance of audible quantization noise is possible by adapting the (audio) input of the masking model [11]. Instead of the power spectrum of the down-mixed stereo signal, that of the signal which will remain after dematrixing should be used. For example, in the case described by Eqs. (12) and (13) the power spectrum of L and R instead of L' and R' should be taken to determine the masked threshold.

A final question is whether there is always sufficient room available in the stereo signal to add the information. As explained in Sec. 1 with Eq. (11), this amount of room depends on two main factors, namely, the masking power of the audio signal and its representation accuracy (Δ_{10} and Δ_{20} in Eq. (11)). It is clear that a higher representation accuracy simplifies the task because the amount of information to be added is independent of it. Experiments have, however, shown that the representations currently used offer sufficient space for the information required. With regard to the masking power of the audio signal, one might naively expect there to be problems with low masking power. In this application, however, the information to be added, H_1 , H_2 , and H_3 , is an audio signal which is also present in the masking signal itself, L' and R' . In other words, if there is limited masking, that is, if little room is available, there is also little information to be added. In the extreme case of no masking (L , R , C , S_L , and S_R are all silent), for example, there is also no need to add information. Another example is given by assuming L and R to contain the direct sound and early reflections and S_L and S_R to contain the reverberation of a concert-hall recording. When the music stops, there is still a (decreasing) reverberation. However, in the down-mixed stereo signal L' and R' , this reverberation is also present and as a result there is still an audio signal in order to mask the information to be added (which information is that L and R are silent).

Within the European HDTV project EUREKA-95, the system is considered as a potential way to transmit HDTV sound. An interesting feature is the compatibility to the two-channel D2MAC transmission standard. After various informal listening tests, which showed the system's potential, a formal listening test on the system's performance was organized by EUREKA-95. During the summer of 1990 these tests have been conducted. Critical signals were constructed. The tests did not reveal any significant audible degradation of these signals after having been mixed into a two-channel NICAM stereo signal. Further formal listening tests are planned for early 1992.

3 CONCLUSIONS

A new surround-stereo-surround coding technique is presented. The down mix to the stereo signal may be optimized to give the best stereo effect. The extra information required to reproduce the original multi-channel surround sensation using the stereo signal is added in this stereo signal. Here the masking effect is used so that the addition remains inaudible. Compatibility with current stereo standards is therefore guaranteed. Using the system it is possible to maintain the original channel separation.

4 ACKNOWLEDGMENT

The authors would like to express their thanks to Dr. W. F. Druyvesteyn, who came up with the idea of using the masking effect for information addition, and to Dr. R. N. J. Veldhuis, who devised the basic algorithms for this addition.

5 REFERENCES

- [1] E. Stetter, "Mehrkanaal-Stereocodung zum Bild für Kino und Fernsehen" (Multichannel Stereo Sound for Cinema and Television Picture), *Rundfunktech. Mitt.*, vol. 35, pp. 1-9 (1991).
- [2] D. J. Meares, "Sound Systems for High Definition Television," *Acoust. Bull.*, vol. 15, pp. 6-11 (1990).
- [3] W. R. Th. ten Kate, L. M. van de Kerkhof, and F. P. M. Zijderfeld, "Digital Audio Carrying Extra Information," in *Proc. ICASSP90* (Albuquerque, NM, 1990 Apr.), pp. 1097-1100.
- [4] B. C. J. Moore, *An Introduction to the Psychology of Hearing*, 3rd ed. (Academic Press, London, 1989).
- [5] E. Zwicker and H. Fastl, *Psychoacoustics: Facts and Models* (Springer, Berlin, 1990).
- [6] R. N. J. Veldhuis, M. Breeuwer, and R. van der Wal, "Subband Coding of Digital Audio Signals," *Philips J. Res.*, vol. 44, pp. 329-343 (1989).
- [7] C. Gerwin and T. Rytén, "Subjective Assessments on Low Bit-Rate Audio Coders," in *Proc. 10th Int. AES Conf. on Images of Audio* (London, 1991 Sept.), pp. 91-102.
- [8] M. Vetterli and D. LeGall, "Perfect Reconstruction FIR Filter Banks: Some Properties and Factorizations," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-37, pp. 1057-1071 (1989).
- [9] N. S. Jayant and P. Noll, *Digital Coding of Waveforms*. (Prentice-Hall, Englewood Cliffs, NJ, 1984).
- [10] C. R. Calvo, A. R. English, and J. W. H. O'Clary, "NICAM 3: Near-Instantaneously Compressed Digital Transmission System for High-Quality Sound Programmes," *Rad. Elec. Eng.*, vol. 50, pp. 519-530 (1980).
- [11] W. R. Th. ten Kate, P. M. Boers, A. Mäkitö, J. Kuusama, E. Sørensen, and K. E. Christensen, "Matrixing of Bit Rate Reduced Audio Signals," in *Proc. ICASSP92* (San Francisco, CA, 1992 March).

THE AUTHORS



W. R. Th. ten Kate



L. M. van de Kerkhof



F. F. M. Zijderfeld

Warner R. Th. ten Kate was born in Leiden, The Netherlands, in 1959. He studied electrical engineering at Delft University of Technology, graduating in 1982 cum laude, and received the 1983 prize awarded by the Delft University Fund. During the final stages of his studies his research was directed at solar cells of amorphous silicon and silicon radiation detectors. He received the Ph.D. degree in 1987.

Since 1988 Dr. ten Kate has been working in the Acoustics Group of Philips Research Laboratories. In 1985 he also began studying the French horn at the Royal Conservatory in The Hague and graduated in 1989 with distinction.

Leon M. van de Kerkhof was born in Eindhoven, The Netherlands, in 1958. In 1978 he joined Philips Research Laboratories, where he worked on noise control (including reactive sound absorbers and aerodynamic noise) and the use of adaptive filters in acoustics. At the same time he began an evening course in electrical engineering at the Institute of Technology. After graduating in 1981 he continued his studies at the Eindhoven University of Technology and received a degree in

1987 cum laude. He then moved to Philips Consumer Electronics. His activities are in the sphere of digital audio, in particular audio source coding and HDTV sound. He is involved in various international projects, including Eureka 95 (HDTV), Eureka 147 (Digital Audio Broadcasting), JESSI AB14 (JESSI DAB), and ISO/MPEG Audio.

Franz F. M. Zijderfeld was born in Helmond, The Netherlands, on 1961 November 20. In 1985 he completed his studies in electrical engineering at the Eindhoven Institute of Technology, his final project being the realization of an autofocus system for a CCD video camera. He then joined Philips Consumer Electronics, where he worked in the development laboratory for video equipment and was mainly involved in analog video signal processing in CCD cameras. In 1987 he moved to the Audio Signal Processing Group at the Philips Consumer Electronics Advanced Development Centre, working on the installation of an experimental four-channel audio postproduction room and on the digital 4-2-4 system. His current interest is centered on digital audio broadcasting.

BEST AVAILABLE COPY

A High-Rate Buried Data Channel for Audio CD

Preprint 3551 (D3-1)

Michael A. Gerzon
Technical Consultant, Oxford, United Kingdom
Peter G. Craven
Oxon, United Kingdom

**Presented at
the 94th Convention
1993 March 16-19
Berlin**



AES

This preprint has been reproduced from the author's advance manuscript, without editing, corrections or consideration by the Review Board. The AES takes no responsibility for the contents.

Additional preprints may be obtained by sending request and remittance to the Audio Engineering Society, 60 East 42nd Street, New York, New York 10165, USA.

All rights reserved. Reproduction of this preprint, or any portion thereof, is not permitted without direct permission from the Journal of the Audio Engineering Society.

AN AUDIO ENGINEERING SOCIETY PREPRINT

A High-Rate Buried Data Channel for Audio CD

Michael A. Gerzon

Technical Consultant, 57 Jason St., Oxford OX2 8DU, UK

Petar G. Crayen

11 Wessex Way, Grove, Wantage, Oxon OX12 0BS, UK

Abstract

The paper describes a new proposal for burying a high data rate data channel (with up to 360 kbit/s or more) compatibly within the data stream of an audio CD without significant impairment of existing CD performance. The new data channel may be used for high-quality data-reduced related audio channels, or even for data-compressed video or computer data, while retaining compatibility with existing audio CD players. The theory of the new channel coding technique is described.

0. Introduction

The paper describes a new proposal for burying a high data rate data channel (with up to 360 kbit/s or more) compatibly within the data stream of an audio CD without significant impairment of existing CD performance. The proposal in this paper is to replace a number (up to four per channel) of the least significant bits (LSBs) of the audio words by other data, and to use the psychoacoustic noise shaping techniques associated with noise shaped subtractive dither to reduce the audibility of the resulting added noise down to a subjective perceived level equal to that of conventional CD.

Simply replacing the LSBs of existing audio data would, of course cause a drastic audible modification of the existing audio signal for two reasons :

1) the wordlength of existing signals would be truncated to (say) only 12 bits, which would not only reduce the basic quantization resolution by 24 dB, but also would introduce the problems of added distortion and modulation noise caused by truncation (e.g. see refs. [1-4]).

2) Additionally, the replaced (say) 4 LSBs would themselves constitute an added noise signal, which itself may not have a perceptually desirable random-noise like quality, and will also add to the perceived noise level in the main audio signal, typically increasing the noise by a further 3 dB above that due to truncation alone, giving in this case as much as 27 dB degradation total in noise performance.

This paper describes methods of overcoming all these problems in replacing the last few LSBs of an audio signal by other data. The new method involves the following steps:

A) Using a pseudo-random encode/decode process, operating only on

the LSB data stream itself without extra synchronizing signals, to make the added LSB data effectively of random noise form, so that the added signal becomes truly noise-like.

B) Using this pseudo-random data signal as a subtractive dither signal (e.g. see [1-4]), so that simultaneously it does not add to the perceived noise and that it removes all nonlinear distortion and modulation noise effects caused by truncation. Remarkably, and unlike in the ordinary subtractive dither case [3], this does not require the use of a special subtractive dither decoder, so that the process works on a standard off-the-shelf CD player, and

C) additionally, at the encoding stage, incorporating psychoacoustically optimized noise shaping of the (subtractive) truncation error, thereby reducing the perceived truncation noise error by around 17 dB further.

The overall effect of combining these three processes is that if one incorporates data into the last few LSBs, then the effects of distortion, modulation noise and perceived audible patterns in the LSB data are completely removed, and the resulting perceived steady noise is reduced by around 23 dB below that of ordinary unshaped optimally dithered quantization to the same number of bits. For example, when the last 4 LSBs of the 16 bit CD wordlength is used for buried-channel data, the perceived S/N (signal-to-noise ratio) is around 91 dB - approximately the same as ordinary 16 bit CD quality when unshaped dither is used.

The result of this process is that as much as $2 \times 4 = 8$ bits of data per stereo sample is available for buried data without significant loss of audio quality on CD, giving a data rate of $8 \times 44.1 = 352.8$ kbit/s.

While the new process achieves potentially high data rates for the buried channel, it does of course reduce room for improvements in CD audio quality approaching 20 bits effective audio quality, such as described in refs. [3],[4]. However, there is no reason why the process should only be used with one fixed number of LSBs, and by reducing the data rate of the buried channel to a smaller number of LSBs, one correspondingly improves the resolution of the audio - for example achieving an effective perceived S/N of around 103 dB for a system using 2 LSBs of data per signal channel sample, with a data rate still of 181.4 kbit/s.

One can even make the number of LSBs used fractional, say, $\frac{1}{2}$ or $\frac{1}{4}$ or $1\frac{1}{2}$ LSBs per sample. This may be used either to precisely match the buried channel to a desired data rate, or to minimize the loss of audio quality, especially at very low data rates.

Additionally, by including in the LSB data channel itself low-rate data indicating the number of LSBs "stolen" from the main audio channels, it is possible to vary the number of LSBs stolen in a time-variant way, so that, for example, more LSBs can be taken by the buried channel when the resulting error is masked by a high-level main audio signal. The noise-shaping can

also be varied adaptively at the encoding stage so that at high audio levels, the noise error is maximally masked by the audio signal, thereby increasing the data rate of the buried channel during loud passages to, in some cases, as much as 720 kbit/s.

It is also shown in this paper that with stereo signals, it is possible to code data jointly in the least significant parts of the audio words of the two (or more) channels, using a multichannel version of the data encoding process involving the use of vector quantizers and subtractive vector dithering by a multichannel pseudo random data signal for the dithering. The basic theory of vector dithering is described in section 5, although readers may find it best to omit these technically difficult aspects on first reading. It is shown that the vector multichannel version of the data coding process ensures left/right symmetry of any added noise in the audio reproduction, and an advantageous noise performance.

The approach described in this paper is substantially different from an alternative method of burying data described in [5], which involved a process of splitting the audio signal into subbands, replacing the LSBs of the subbands with data based on auditory masking theory, and then reassembling the resulting data by recombining the subbands. Not only is that process very complicated, with a considerable time-delay penalty in the subband encoding/decoding process, but it has to be done with extraordinary precision to prevent data errors in the band splitting and recombining process. By contrast, the present process involves little time delay, involves relatively simple signal processing, and further is such as to guarantee the lack of audible side-effects due to nonlinear distortion, modulation noise or data-related audible patterns.

Another approach to transmitting data in an audio waveform, for use with the NICAM system, has been described by Emmett [24], in which the shape of the error spectrum is adaptively changed to be masked by the audio signal. This may or may not have some common features with the present proposal, although the details of Emmett's proposal are not clear from his published preprint. However, according to Emmett [24], to attain a high encoded data rate with his proposal requires using a data rate that changes with signal level so as not to be audible during quiet passages. The present proposal does not require the use of such level-adaptive data rates.

1. Uses Of Buried Data

1.1 Advantages over CD ROM media

The availability of a buried data channel with data rates of the order of 360 kbit/s without significant loss of audio quality on audio CDs, fully compatible with conventional playback on standard audio players, opens up prospects for many new products. Unlike standards such as CDi based on CD-ROM, the additional data can be added without destroying compatibility with

playback over tens of millions of existing audio players. This means that the new data channel can be added while still giving the CD the advantages of mass-market economies of scale of production, thanks to the existing audio-only market. Thus applications using the new data channel should result in much lower prices than for media where the number of players is limited.

1.2 Application to multichannel sound

One application of the new data channel is using the additional bits to add, using audio data compression, additional audio channels for three- or more-speaker frontal stereo or surround sound, such as described for example in [6],[7],[8]. Because CD has higher quality than available data compression systems (despite spurious claims of "transparency" or "CD quality" by some less cautious proponents of such systems), care must be taken that the additional channels are not too compromised in quality by the data compression process, which means that a rather lesser degree of compression is desirable than for DAB or film surround-sound. However, since two of the transmitted audio channels are the standard CD audio channels and the design of the buried channel avoids nonlinear or modulation noise effects on these main channels, all the data rate in the buried channel can be used solely for the additional channels, giving each a higher data rate than if the buried channel were used to transmit the whole audio signal. In using the buried channel to transmit additional directional audio channels, it is important to design the codec error signals so that they do not become audible through the mechanism of directional unmasking described in three of one of the author's references [9],[10],[11].

The data rate available is sufficient to transmit a Dolby AC-3 or MUSICA surround 5-channel surround-sound signal, but these systems involve a quality compromise with the data rate, so that this is not a preferred procedure.

High-quality data compressed additional audio channels can, unlike existing data compression systems, minimize the risk of destruction of subtle auditory cues such as those for perceived distance (see [12]), thereby maintaining CD digital audio as the preferred medium for high quality audio, while adding additional channels. For high quality (and especially musical) use, it may be preferred to use additional buried audio channels either for frontal-stage 3- or 4-speaker stereo or for 3-channel horizontal or 4-channel full-sphere with height [13],[14] ambisonic surround sound (see refs. [7],[8],[15]), rather than for the rather cruder theatrical "surround-sound" effects considered appropriate for cinema or video-related surround-sound systems. However, systems have been proposed for intercompatible use of both kinds of system [7],[8].

Since the main audio channels in this proposal convey high-quality audio, it is possible to use the spectral envelope of the main audio channels to convey most or all of the dynamic ranging information used for the subbands in data reduction systems for related subsidiary channels conveyed in the buried

data channel, especially if the main audio channels incorporate a mixture of all the transmitted channels so that no direction is canceled out. This saves the data overhead of conveying ranging data, which in high quality systems may save of the order of 60kbit/s, as compared to a stand-alone data compression system. This will allow a system conveying n related channels using 4 LSBs per main CD audio channel to give a performance equivalent to that of a stand-alone data compression system conveying $n-2$ channels in about 420 kbit/s. For 3-channel systems, such as horizontal B-format surround-sound or 3-channel UHJ [15] or frontal-stage 3-channel stereo, this quality is unlikely to be audibly distinguishable from an uncompressed data channel, and for 4-channel systems, the results will still subjectively approach that of critical studio-quality material, and even for 5-channel material, the results will be considerably less compromised than that for DAB or cinema surround-sound, using a data rate for the additional channels of well over twice that use in those applications.

1.3 Video and computer data

Alternatively, the buried data channel can be used for conveying related computer data, such as graphics, multilingual text or track copyright information. Because of the high available data rate, this can be done with very much higher quality than is possible on the subcode channels of CD, conveying for example with JPEG image data compression of the order of one high quality color photographic image per second. A data rate of 360 kbit/s is even enough to convey a reasonable video image. Using the existing MPEG standard, this would have very low resolution (although certainly good enough for moving inserts within a still image), but near-future image data-compression methods based on using the highly non-Gaussian nature of images are expected to make consumer-quality video available within this data rate.

1.4 Dynamic range data

Another use would be to convey dynamic-range reduction or enhancement data, e.g. a channel conveying the setting of a gain moment by moment. This would allow the same CD automatically to be played with different degrees of dynamic compression according to environment, by choosing the gain adjustment channel appropriate to that environment. This would include the possibility of completely uncompressed quality for high-quality use, without making the CD incompatible for more normal use, e.g. in broadcasting. An advantage of providing the dynamic range gain data in the data subchannel rather than using automated dynamic range modification algorithms is that one can always do a much better subjective job using manual intervention based on a knowledge of the music and its needs, but at the expense only of considerable time and effort. This effort can be recorded for consumer use in the buried data channel. If automated algorithms are used for the dynamic range gain conveyed by the buried data channel, these can be of a much more sophisticated and subtle nature than those normally available to the consumer (e.g. [16]).

1.6 Frequency Range Extension

A further use related to the original audio would be to add in the subchannel data-reduced information allowing information above 20 kHz to be reconstructed. One of the limitations of compact disc is that the frequency range is limited to 20 kHz. Although the ears' sine wave hearing is, for all except a small minority of (generally young and often female and/or asthmatic) listeners, limited to below 20 kHz, this does not mean that there is no loss of perceived quality caused by the sharp bandlimiting to 20 kHz. It is widely noted that there is a significant loss of perceived quality when comparing high-quality digital signals sampled at say 44.1 kHz as compared to 88.2 kHz.

From a quality viewpoint, it may be more important to use an extended bandwidth to provide a more gentle roll-off rate than to provide a response flat to 40 kHz, since (unlike the brickwall filters used with ordinary CD), such gentler roll-offs are similar to those encountered in natural acoustical situations.

The extended bandwidth can be provided by using a high-order complementary mirror filter pair of the kind described in Regalia et al. [21] and in Crochiere and Rabiner [22] to split an 88.2 kHz-rate sampled digital signal into two bands sampled at 44.1 kHz. The filters involved will overlap, although using a high-order filter [21], the region of significant overlap can be reduced to of the order of a kHz. Within the overlap region there will be aliasing from the other frequency range, although the reconstruction of the full bandwidth [21,22] will cancel out this aliasing. The band below 22.05 kHz can then be transmitted as the conventional audio, and the band above 22.05 kHz can be transmitted in data reduced form in the buried data channel at a reduced data rate of, say, between 1 and 4 bits per sample per channel, using known sub-band or predictive coding methods. Phase compensation inverse to the phase response of the low pass filter in the complementary filter pair may be employed to linearize the phase response of the main sub-22.05 kHz signal for improved results for standard listeners, with the use of an inverse phase compensating filter in the decoding process for reconstructing the wider bandwidth signal.

1.6 Combined applications

Any or all of these uses can, of course, be combined, subject only to the restrictions of the data rate, so that the buried data channel could be used for example to convey one additional audio channel, a dynamic range gain signal, extended bandwidth and additional graphics, text (possibly in several languages), copyright and even insert video data as appropriate.

For historical material, where the dynamic range may be significantly less than 90 dB, it may even be possible to increase the data rate available further by allocating even more bits to the buried data channel, since an increased

noise level may not be significant. For this reason, it may be desirable to allow the possibility of allocating as many as 12 or even 16 bits of audio data (say bits 10 to 15 or even 8 to 15 of each audio channel) to the buried data channel.

2. Pseudo-Random Coding of Data

2.1 Pseudo-Randomized data

It is essential, if the LSBs of an audio signal are to be replaced by data, that the replacing data should truly resemble a random noise signal (albeit perhaps one that may be spectrally shaped for psychoacoustic reasons). Most data signals, when listened to as though they were digital audio signals, have some degree of systematic pattern which may well prevent them from sounding or behaving truly like random noise. Such departures from random noise like behavior are generally much more perceptually disturbing or distracting than a simple steady noise.

Also, if we can ensure that added data behaves like a noise signal with known statistical properties, one can use all that is known in the literature on dither and noise shaping (see [1]-[4],[17]-[20]) to optimize the perceptual properties of the added data to minimize its audible effects.

The data signal is rendered pseudo-random with predictable statistics in our proposal by a data encode/decode process, the encode process having the effect of pseudo-randomizing the data signal, and the decode process having the effect of recovering the original data signal from the pseudo-randomized data signal, as in figure 1. From a practical point of view, it is highly desirable that the encode and decode process require no use of an external synchronizing signal, but that the decode process should work entirely from the pseudo-randomized data sequence itself.

The simplest way of constructing such an encode/decode pseudo-randomizing process for data is to use a cyclic pseudo-random logic sequence generator separately on each bit. For example, if its input is zero, fig.2 shows a well-known binary pseudo-random logic sequence generator using feedback around three logic elements and a total shift register delay of 16 samples (a 1-sample delay is denoted by the usual notation z^{-1}). Provided that the logic state in the 16 samples stored in the shift register is not all zero, this binary sequence generator has the 16 logic states cycle through all $2^{16}-1 = 65,535$ non-zero states in a pseudo-random manner.

If, instead of using a zero input, the pseudo-random sequence generator of fig. 2 is fed with a binary data stream s_n , then it has the effect of a pseudo-randomizer for the input data. This encoding scheme is based on the recursive logic

$$t_n = s_n \oplus t_{n-1} \oplus t_{n-3} \oplus t_{n-14} \oplus t_{n-16}, \quad (2-1)$$

where t_n is the output binary logic value of the network at integer sample time n , s_n is the input binary logic value of the network at integer sample time n ,

and \oplus represents the logic "exclusive or" or Boolean addition operator (with truth table $0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$).

Conversely, if exactly the same arrangement of logic gates is fed with the pseudo-randomized data t_n , then the effect of the "exclusive or" gates on the input signal is to restore the original data stream. This is achieved by the inverse decoding logic process

$$s_n = t_n \oplus t_{n-1} \oplus t_{n-3} \oplus t_{n-14} \oplus t_{n-16} \quad (2-2)$$

illustrated in the second diagram in fig. 2.

Thus by using a logic network recursively with a total of $L = 16$ samples delay and only 4 "exclusive or" gates, a binary data stream can be pseudo-randomized, and the same network can decode the data stream back to its original form. For constant signals, there is a one in 65,536 chance that the undesirable non-random zero state will be encountered, but this low probability is probably acceptable, given that even a single binary digit change of input is likely to "jog" the system back into a pseudo-random output state.

Other well-known pseudo-random binary sequence logic generators with shift registers of longer length L than 16 samples can be used for encoding and decoding in the same way, with their feedback output given by subjecting the delayed sequence output and the input to a "sum" logic gate. Such length L sequences will have, for a constant input, only one chance in $2^L - 1$ of giving an unrandomized output, and will have a sequence length of $2^L - 1$ samples.

Although the pseudorandom binary sequence generator described in (2-1) and fig. 2 is a maximum length sequence for a zero input, it has a shorter length for an all-one constant input, and in general, the precise behavior with, say periodic inputs is hard to predict. Partly for this reason, it is not absolutely essential to use a maximum-length sequence generator, provided that the length of the sequence is not too short for constant inputs.

It will be noted that the network of fig. 2 only has $L = 16$ samples of memory, so that when used as a decoder, any data errors in the input will only propagate for L samples, and then the output will recover. This lack of long-term memory in the decoding process means that there are no special requirements on the error-rate of the transmission channel. Because of the small number of logic elements in fig. 2, a single sample error in the received data stream will only cause five sample errors in the decoded output.

As shown in fig. 3, typically, for use with CD, the data will first be arranged to form a number of bits of data per sample of each audio channel, for example 8 bits of data constituting bits 12 to 15 of the left and the right audio channels (where bit 0 is the most significant bit (MSB) of a 16 bit audio word and bit 15 the least significant bit).

Then each of these (say 8) bits will, separately, be encoded by a pseudo-random logic such as that of fig. 2 to form a pseudo random sequence, and

the resulting pseudo-randomized bits used to replace the original bits in (say) bits 12 to 15 of the left and the right audio channels. The resulting noise signals in the left and right audio channels will be termed the (left and right) data noise signals.

Alternatively, instead of pseudo-randomizing individual bits of the audio words representing data separately, they can be pseudo-randomized jointly by regarding the successive data bits of a word as being ordered sequentially in time, and applying a pseudo-random encoder such as that of figure 2 to this sequence of bits. For example, eight bits of data per audio sample can be sequentially ordered before the next eight bits of data corresponding to the next audio sample, and the pseudo-random-logic encoding can be applied to this time series of bits at eight times the audio sampling rate.

An advantage of this strategy is that errors in received audio samples propagate for (in this example) for only one eighth of the time as in the case where each word bit is separately pseudo-randomized.

M-level data signals, taking one of M possible values, conveying $\log_2 M$ bits per sample can also be pseudo-randomized by a direct process involving congruence techniques, whereby the coded version w'_n of the current sample M-level word w_n is given by

$$w'_n = w_n + \sum_{j=1}^L a_j w_{n-j} \pmod{M}, \quad (2-3)$$

where the a_j 's are (modulo M) integer coefficients chosen (if necessary by empirical trial-and-error) to ensure that all M possible constant inputs result in a pseudo-randomized output with reasonably long sequence lengths. The inverse decoding of the pseudo-randomized M-level words is

$$w_n = w'_n - \sum_{j=1}^L a_j w_{n-j} \pmod{M}. \quad (2-4)$$

The logic techniques described with reference to figure 2 are just the special case when $M = 2$ of this more general congruence technique. The congruence technique can result in sequence lengths for constant inputs of length up to a maximum of $M-1$ samples, so that in general, the larger the value of M, the smaller need be L, with a consequent shortening of the time duration of propagation of errors.

A slightly more complex pseudo-randomization of data will provide an initial pseudo-randomization of M-level data by a method such one of those described here, and follow it by an additional one-to-one map between the M possible data values. The decoding will first subject the M levels to an inverse map before applying the inverse of the above pseudo-random encodings.

There are many similar but more complicated methods of pseudo-randomization of data streams, and as we have seen, these need have no coding delay or increase in data rate after coding, and can limit the duration

of any errors in received data in the inversely decoded output to not more than a few samples after the occurrence of an erroneous audio sample.

As audio signals, the resulting pseudo-randomized data noise signals have a steady white noise spectrum and a (discrete) uniform or rectangular PDF (probability distribution function), in the example case described above having 16 levels in each of the left and right channels. Such discrete noise does not have the ideal properties of rectangular dither noise, although Wennamaker *et al* [17] have shown that it approximates many of these desirable properties in a precise mathematical sense. However, adding to it an extra random or pseudo-random white rectangular PDF noise signal with peak level $\pm \frac{1}{2}$ LSB converts it into noise with a true rectangular PDF with peak levels (in this example) of ± 8 LSB. In this case the added noise to convert from a discrete to a continuous PDF is at a very low level, being 24 dB below the level of the data noise signal.

2.2 Stereo parity coding

Although in the above example, we have described data being conveyed on each audio word bit of the data signal separately, it will be realized that data can alternatively be conveyed by more complicated combinations of the least significant digits (in any numerical base M, not just the binary base 2) of audio words, for example on the Boolean sum of the corresponding bit in the left and right audio signal.

For example, consider the case that a data rate of only one bit per stereo audio sample is required. Such a signal can be conveyed as the Boolean sum of the LSB in the left and the right audio channels, leaving the values of the LSB in individual audio channels separately unconstrained. Conveying a data channel using the Boolean sum of the corresponding bits of the left and right audio signals is herein termed stereo parity coding.

It is of course desirable that the effect on the conventional audio of reallocating bits to a buried data channel should be left/right symmetrical. In particular, if a buried data channel is used with a data rate of just one BPSS (bit per stereo sample), then one does not wish to code the data in the LSBs of only one of the two stereo channels. If the value of the respective Nth bits of the respective left and right channel signals are denoted by L_N^n and R_N^n at time n, then one codes a pseudo-randomized one bit per sample data channel I_N^n as

$$I_N^n = L_N^n \oplus R_N^n \quad (2-5)$$

If desired, an additional second pseudo-randomized one bit per sample data channel u_N^n can be encoded in the Nth bits of the stereo audio signal say as

$$u_N^n = L_N^n \quad (2-6)$$

in which case the data can be encoded via $L_N^n = u_N^n$, $R_N^n = L_N^n \oplus I_N^n$, and decoded via $u_N^n = L_N^n$, $I_N^n = L_N^n \oplus R_N^n$. Alternatively u_N^n can be encoded as R_N^n . The use of stereo parity encoding allows the separate one BPSS data channels to be separately decoded while maintaining left/right symmetry in the audio when an odd number of one BPSS channels are used.

One could standardize a basic one BPSS data channel as being conveyed via the parity (Boolean sum) of the LSBs (i.e. bit 15) of the left and right audio channels. Information about the way other data channels conveying more BPSS are coded will, in such a standardization, be conveyed by this basic data channel. By this means, a data decoder can read from the basic one BPSS stereo parity data channel how to decode any other data channels (if any) present. In particular, this allows if desired moment-by-moment variation of the data rate, either adaptively to the amount of data needing transmission or adaptively to the audio signal according to its varying ability to mask the error signal caused by the hidden data channels.

For example, in loud passages in pop/rock music, the data rate allocated to say a video signal could be increased, allowing quite high quality video images in, say, heavy metal music.

2.3 Fractional bit rates

There is no reason why the buried data channels should be restricted to data rates of an integer number of BPSS, although this may be a convenient implementation. Several methods can be used to allocate less significant parts of audio words to data at fractional bit rates.

One method conveys $\log_2 M$ bits for integer M in the less significant parts of audio words by conveying data in the M possible values of the remainder of the integer audio word after division by M , whereas the rounding quantization process used for the audio involves rounding to the nearest multiple of M . For M a power of 2, this reduces to conventional quantization to $\log_2 M$ fewer bits.

In Eqs. (2-3) and (2-4) above, we described how such M -level data channels can be pseudo-randomized by pseudo-random congruence encoding and decoding. Alternatively, if M can be expressed as nontrivial product of $K =$

two or more integer factors $M = \prod_{j=1}^K M_j$, then one can uniquely expand the M -

level data word w in the form

$$w = \sum_{k=0}^{K-1} w_{(k)} \prod_{j=1}^k M_j \quad (2-7)$$

with $w_{(k)}$ an integer between 0 and $M_{k+1}-1$. Eq. (2-7) is the generalization of the expansion of a number to base M_0 in the case $M_j = M_0$ for all $j = 1, \dots, K$. Each of the expansion coefficients $w_{(k)}$ can, if desired, be separately pseudo-randomized before the final length M word is formed. Again, this generalizes the binary case described above where the M_j 's equaled 2.

A second method for fractional bit rates especially suitable for very low data rates of $1/q$ BPSS for integer q is to code data only in one out of every q audio samples. The encoding schemes are as before but with a data

sampling rate divided by q , and decoding involves the decoder trying out and attempting to decode each of the q possible sub-sequences until it finds out (e.g. by confirming a parity check encoded into the data) which one carries data.

For integers $p < q$, a data rate of p/q BPSS can similarly be obtained by encoding data in the LSBs of p out of every q samples (for example, samples 1 and 3 out of every successive 5 samples for $p = 2$ and $q = 5$).

A third method for fractional bit rates also codes data in the LSBs of q successive samples, but codes the data into different logical combinations of all q bits. For example, a data rate of $1/q$ BPSS can be obtained by encoding data as the parity (Boolean sum) of the q LSBs. It turns out that this option is often capable of significantly less audio noise degradation than the simpler scheme of the second method. A part of the advantage is that if one needs to modify the parity, then one can choose to modify that sample out of the q successive samples causing the least error in an original high-resolution audio signal, rather than being forced to alter a fixed sample.

We shall see in the following that, for all three kinds of fractional bit rate data encoding, it is possible to use a subtractive dithering technique by a data noise signal to eliminate unwanted modulation noise and distortion side effects on the modified waveform data. The advantages of the new process are not confined to integer bit rates per sample.

3. Subtractively dithered noise shaping

3.1 Subtractive dither

Here we briefly review the ideas of subtractively dithered noise shaping, detailed by the authors in refs. [1], [3] and [4]. In this paper, by a "quantizer" we mean a signal rounding operation that takes higher resolution audio words and rounds them off to the nearest available level at a lower resolution. We assume that the quantizer is uniform, i.e. that the available quantization levels are evenly spaced, with a spacing or step size denoted as STEP.

The quantizer rounding process introduces nonlinear distortion, but this distortion may be replaced by a benign white noise error at the same typical noise level by using the process of subtractive dither shown in figure 4. The process comprises adding a dither noise before the quantizer and subtracting the same dither noise afterwards. Provided that the statistics of the dither noise are suitable, it can be shown (see [1], [2]) that this results in the elimination of all correlations between the error signal across the subtractively dithered quantizer and the input signal. One such suitable dither statistics is what we term RPDF dither, i.e. dither each of whose samples is statistically independent of other samples and with a rectangular probability distribution function with peak levels $\pm \frac{1}{2}$ STEP.

An audio word of B bits each of which is a pseudo-random binary sequence,

is a 2^B -level approximation to a signal with RPDF statistics, so that the data noise signals considered above may be used as dither signals for dithering audio to eliminate nonlinear quantization distortions and modulation noise. Similarly, the M-level data noise signals described above in section 2.3 using the remainder modulo M for data, if made to be of a pseudo-random form by a pseudo-random data encoding/decoding process, can be used as an M-level approximation to RPDF noise.

Although data noise signals are discrete approximations to RPDF noise, they can be converted to continuous RPDF noise statistics by the simple process of adding to them an additional smaller RPDF noise with peak levels $\pm \frac{1}{4}$ LSB, where LSB is the step size of the LSB's of the transmitted audio words (as distinct from the step size STEP = M LSBs of any rounding process used in encoding hidden data channels.) This is shown schematically in figure 5.

Conventionally, as described in refs. [1] and [3], the use of subtractive dither requires the use of a decoding process in which during playback, the original dither noise added before the quantizer is reconstructed before being subtracted; this requires either the use of synchronized pseudo-random dither generation algorithms, or an encode/decode process in which the dither noise is generated from the LSB's of previous samples of the audio signal [3]. However, in the application of this paper, as will be seen, no special dither reconstruction process is required for the discrete dither, since this is already present in the transmitted LSBs.

3.2 Noise shaping

A white error spectrum is not subjectively optimum for audio signals, where it is preferred to weight the error spectrum to match the ears' sensitivity to different frequencies so as to minimize the audibility or perceptual nuisance of the error. The spectrum of the error signal may be modified to match any desired psychoacoustic criteria by the process of noise shaping, discussed for example in refs. [1], [4], [18]-[20].

Noise shaping may be static (i.e. adjusting the spectrum in a time-invariant way) and made to minimize audibility or optimize perceptual quality at low noise levels, or alternatively it can be made adaptive to the audio signal spectrum so as to be optimally masked by the instantaneous masking thresholds of audio signals at a higher level. The latter option is particularly valuable in the present application, where loud audio signals may well allow an increased error energy to be masked, thereby allowing a higher data rate to be transmitted in the hidden data channels during loud audio passages.

The form of noise shaping with subtractive dither used in this paper is indicated in the schematic of figure 6. It will be noted that, while it is equivalent to some of the forms described in ref. [1], it is not the arrangement described previously by the authors in ref. [3], in that here we put the noise shaping loop around the whole subtractive process. With the arrangement of figure 6, the output of the quantizer itself differs from the noise shaped output

of the whole system by a spectrally white dither noise, so that in this arrangement, unlike those suggested in ref. [3], the spectral shape of the quantizer output error and system output error is not identical.

With the noise-shaped subtractively dithered quantizer of fig. 6, the error feedback filter $H(z^{-1})$ must include a 1-sample delay factor z^{-1} in order to be implementable recursively, and the originally white spectrum of the subtractively dithered quantizer is filtered by the frequency response of the noise shaping filter

$$1 - H(z^{-1}), \quad (3-1)$$

which is preferably chosen to be minimum phase to minimize noise energy for a given spectral shape [1], and may be chosen to be of any desired spectral shape.

Other implementations of noise shaping around a dithered quantizer system are possible. Alternative implementations are reviewed in ref. [4]. By way of example, fig. 7 shows an alternative "outer" form of noise shaping architecture described in ref. [4], that is equivalent to fig. 6 if one puts

$$H'(z^{-1}) = H(z^{-1})/(1-H(z^{-1})). \quad (3-2)$$

The application of noise shaping around a subtractively dithered quantizer will not result in any unwanted nonlinear distortion or modulation noise, provided that the dither noise added in figs. 6 or 7 is RPDF dither matched to the step size STEP of the quantizer.

4. Application to buried data channels

4.1 Noise-shaped subtractively dithered buried channel encoding

Either the arrangement of fig. 6 or fig. 7 can be applied to obtain subtractively dithered noise-shaped audio results when the last digits of an audio signal word (whether the last N binary digits or the remainder after division by M) are replaced by buried data bits.

The procedure is now simple to describe. First the data is pseudo-randomized, and then used to form a data noise signal as described above. This data noise signal has (discrete M-level) RPDF statistics, and may be used as the dither noise source in figures 6 or 7, as shown in figs 8 and 9, where the quantizer is simply the process of rounding the signal word to the nearest integer multiple of M LSB's (or the nearest level if the levels are placed uniformly at other than the integer multiple of M LSB's). The process shown in figures 8 or 9 subtracts the data noise signal from the audio at the input of the uniform quantizer (which has step size STEP = M LSBs), and adds it back again at the output of the quantizer so as to make the least significant digits of the output audio word equal to the data noise signal. Noise shaping is performed around this whole process.

For best results using the algorithms of figs. 8 or 9 (or equivalent algorithms such as that in figures 10 below), it is best if the input audio word signal is

available at a higher resolution or wordlength than that used in the output, since this will avoid cascading the rounding process used in figs. 8 or 9 with another earlier rounding process. By making the input signal available at the highest possible resolution, any overall degradation of signal-to-noise ratio is minimized.

Since the output equals the output of the quantizer plus the data noise signal, the noise shaping has no effect on the information representing the data in the output audio word, but merely modifies the process by which the quantization of the audio is performed so as to minimize the perceptual effect of the added data noise on the audio. It is remarkable that this output signal, being the output of a noise-shaped subtractively dithered quantizer, automatically incorporates all the benefits of noise shaped subtractive dither without the audio-only listener needing any special subtractive decoding apparatus.

Moreover, because the information received by the data-channel user is not dependent on the noise shaping process, the noise shaping can be varied in any way desired without affecting reception of the data (provided only that no overflow occurs in the noise shaping loop near peak audio levels - fitting a clipper in the signal path before the quantizer to prevent this may be desirable). Thus the noise-shaping process does not affect the way the signal is used by either audio or data end-users of the signal, and so does not need any standardization, but may be used in any way desired by the encoding operative to achieve any desired kind of static or dynamic noise shaping characteristic.

Other equivalent noise-shaped dithering architectures may be used in place of those shown in figs. 8 and 9 for encoding the data signals into the output audio word, using the kind of equivalent architectures discussed in ref. [4]. Purely by way of example, fig. 10 shows yet another implementation having identical performance to that shown in figs. 8 or 9. It is also evident that in a similar way, the data noise signal can be added and subtracted outside the "outer" noise shaper of fig. 9 rather than inside the noise shaper as shown.

4.2 Buried Channel Decoding

Optimum recovery of the audio channels involves no need for any kind of decoder in this proposal. Playback is conventional, with the effect of subtractive dither by the data noise signal being automatic as described above.

Recovery of the buried data is also straightforward, simply being recovery of the data noise signal by rejecting highest bits of the received audio word, or in the case of M-level data, the inverse process to the encoding, of reading the remainder of the audio word after division by M, i.e. resolving the least significant digits of the audio word via modulo M arithmetic. This is followed by the inverse pseudo-random decoding process to recover the data before pseudo randomization, and then the data is handled as data in the usual way.

This decoding process is shown schematically in figure 11.

In the case that the data is encoded as integer coefficients w_{kj} with more than one base M_j as in Eq. (2-7) above, the data is recovered by K successive divisions by M_1 to M_K , at each stage discarding the fractional part, the K coefficients w_{kj} being the integer remainders of the division by M_{k+1} . This is the same process shown in figure 11, but with K stages of the modulo division.

5. Vector quantization and dither

5.1 Reasons for digression

It may not be completely clear to the reader without further explanation that the above descriptions of the use of noise shaped subtractive dithering also apply to the stereo parity coding case as well. To see this, we need first to look at vector quantization and vector dithering, and show that exactly the same ideas for subtractive dithering, noise shaping and data encoding can be applied to the vector quantizer case as the scalar case described above. Because the description in this section (section 5) may be found rather technical, we suggest that it be omitted on first reading.

The description here is given in greater generality than needed just for the stereo parity coding case, since it has applications to coding information in the parity of the corresponding bits in 3 or more channels in transmission media carrying more than two audio or image channels, for example in the 3 channels containing the 3 components of a color image.

5.2 Uniform vector quantizers

As briefly indicated in earlier papers [1], [3], [9], the concepts of additive and subtractive dither can be applied to vector as well as scalar quantizers. Vector quantizers quantize a vector signal y comprising n scalar signals (y_1, \dots, y_n) in geometrical regions covering the n -dimensional space of n real variables. As in the scalar case, we shall say that a vector quantizer Q is a uniform quantizer if the signal y is quantized to a point in a discrete grid G of quantization vectors $\{y_g : g \in G\}$, where there exists a region C around $(0, \dots, 0)$ of n -dimensional space such that the regions $y_g + C = (y_g + c : c \in C)$ cover without overlap (except at their boundary surfaces) the range of signal variables y being quantized. Thus a uniform vector quantizer divides the n -variable space into a grid of identical vector quantization cells that are translates of the cell C to the points of the grid G , and quantizes or rounds any point in the cell $y_g + C$ to the point y_g .

There are many examples of uniform vector quantizers, the simplest of which has a hypercubic cell $C =$ the region $\{(c_1, \dots, c_n) : |c_i| \leq \frac{1}{2} \text{STEP} \forall i = 1, \dots, n\}$, i.e. separate scalar quantization of the n variables. The grid G in this case is simply points of the form $(m_1 \text{STEP}, m_2 \text{STEP}, \dots, m_n \text{STEP})$ for integer m_i 's, and

the associated vector quantizer is simply that that takes (y_1, \dots, y_n) to $m_j = \text{integer}(y_j/\text{STEP})$ for $j = 1, \dots, n$. This case is trivial in the sense that it is equivalent to using separate uniform scalar quantizers on each of the n channels.

A more complicated but easily visualized example is the 2-channel case where C is a regular hexagon in the plane, for example the region consisting of the points (c_1, c_2) in the plane such that

$$|c_1| \leq \frac{1}{2} \text{STEP}, \quad |-\frac{1}{2}c_1 + (\sqrt{3}/2)c_2| \leq \frac{1}{2} \text{STEP}, \quad |-\frac{1}{2}c_1 - (\sqrt{3}/2)c_2| \leq \frac{1}{2} \text{STEP}, \quad (5-1)$$

and the grid G is the centers of the hexagons in the honeycomb grid covering the plane, i.e. G is the points

$$((m_1 + \frac{1}{2}m_2)\text{STEP}, (\sqrt{3}/2)m_2\text{STEP}) \quad (5-2)$$

for integer m_1 and m_2 .

A uniform vector quantizer of particular interest and practical use in n dimensions is what we shall term the rhombic quantizer. This starts off with a conventional hypercubic grid G_C of points at positions $(m_1\text{STEP}, m_2\text{STEP}, \dots, m_n\text{STEP})$, where STEP is a step size, and m_1 to m_n are integers, which of course has the hypercube quantizer cell described just above and corresponds to the use of n separate scalar uniform quantizers. However, we produce a new grid $G \subset G_C$ which consists of just those grid points in G_C with $m_1 + \dots + m_n$ having even integer values. This new grid only has half as many points as the original, and can be equipped with a new vector quantization cell C as follows, which we shall term the n -dimensional rhombic quantizer cell.

The rhombic quantizer cell can be described geometrically by thinking of the original hypercubic cells as being colored white if $m_1 + \dots + m_n$ is even and black if $m_1 + \dots + m_n$ is odd, forming a kind of n -dimensional checkerboard pattern of alternately black and white hypercubes. Then attach to each white hypercube that "pyramid" portion of each adjacent black hypercube lying between the center of the black hypercube and the common "face" with the white hypercube. The resulting solid is the rhombic cell C .

It is evident, since the pyramid portions taken from adjacent black hypercubes are in total enough to form one black hypercube if pieced together, that the volume occupied by the rhombic quantizer cell is twice that occupied by the original hypercube quantizer cell, and that the versions of the rhombic quantizer cell translated by the grid G indeed cover the n -dimensional n -parameter vector signal space.

For $n = 2$, the rhombic quantizer cell C is a diamond-shape, being a square whose sides are rotated 45° relative to the channel axes, as shown in fig. 12. For $n = 3$, the rhombic quantizer cell C is a rhombidodecahedron, a 12-faced solid whose faces are rhombuses. For $n = 4$, the rhombic quantizer cell C is a regular polytope unique to 4 dimensions termed the regular 24-hedroid [23].

Calculations involving quite complicated multidimensional integrals, which we

shall not detail here, show, for a given large number of quantizer cells covering a large region of n-dimensional space, that for $n = 2$, rhombic quantization has the same signal-to-noise ratio (S/N) as conventional independent quantization of the channels, but that for $n \geq 3$, rhombic quantizers give a better S/N than conventional independent quantization of the channels. The improvement reaches a maximum of about 0.43 dB when $n = 6$. This improvement in the S/N is maintained when additive or subtractive dither is used as described below. (The hexagonal 2-channel quantization described above gives a 0.16 dB better S/N than independent quantization of 2 channels.)

Mathematically, the rhombic quantizer has grid G consisting of the points
 $(m_1 \text{STEP}, m_2 \text{STEP}, \dots, m_n \text{STEP}),$ (5-3a)

where the m_i have integer values with
 $m_1 + \dots + m_n$ having even integer values. (5-3b)

The rhombic cell C is that region of points (c_1, \dots, c_n) satisfying the $n(n-1)$ inequalities

$$|c_i + c_j| \leq \text{STEP}, |c_i - c_j| \leq \text{STEP}, \quad (5-4)$$

for $i \neq j$ selected from $1, \dots, n$. The associated uniform vector quantizer rounds a vector signal (y_1, \dots, y_n) by an algorithm whose outline form might be

```

 $m'_1 := \text{integer}(y_1/\text{STEP}),$ 
If  $m'_1 + \dots + m'_n$  is even
  then  $m_i := m'_i$  for all  $i = 1, \dots, n,$ 
  else  $c_j := y_j/\text{STEP} - m'_j,$ 
(*)    $d_j := \text{sgn}(c_j)$  if  $|c_j| > |c_l|$  for all  $l < j$  and  $|c_j| \geq |c_l|$  for all  $l > j$ 
       $d_j := 0$  for all other  $l,$ 
       $m_i := m'_i + d_i$  for all  $i = 1, \dots, n.$ 
End if

```

(5-5)

There are, of course, various equivalent forms for this kind of rhombic quantizer algorithm, a computationally demanding aspect on typical signal processors being the determination in line (*) of that j for which $|c_j|$ is biggest.

In the $n = 2$ case, there is a simpler rhombic quantization algorithm as follows

$$\begin{aligned}
 x_1 &:= y_1 + y_2, & x_2 &:= y_1 - y_2, \\
 m'_1 &:= \text{integer}(x_1/(\sqrt{2}\text{STEP})) \\
 m'_2 &:= \text{integer}(x_2/(\sqrt{2}\text{STEP})) \\
 m_1 &:= m'_1 + m'_2, & m_2 &:= m'_1 - m'_2,
 \end{aligned} \quad (5-6)$$

which is based on the observation that the rhombic quantizer cell for $n = 2$ is the same shape as the square cell used for ordinary independent quantization of the two channels, but rotated by 45° and with an increase of the step size by a factor $\sqrt{2}$. (See fig. 12).

5.3 Subtractive vector dither

The concepts of dithering for uniform quantizers developed in refs. [1-4] for scalar uniform quantizers may be applied also to the vector case by using appropriate vector dithers. An n-signal dither noise vector (v_1, \dots, v_n) is said to have uniform probability distribution function in a region C of n-dimensional

space if its joint probability distribution function is constant within the region C and zero outside it. This is the n -dimensional generalization of rectangular PDF dither for vector signals, and we denote the associated n -vector dither signal by r_C .

It can be shown (we omit any proofs here) that if the subtractive dither arrangement of figure 4 is used for modifying an input vector signal, where the "uniform quantizer" becomes a vector uniform quantizer with quantization cell C , and the dither noise becomes a uniform PDF vector dither r_C on the region C , then the output vector signal of the system is free of all nonlinear distortion and modulation noise effects (i.e. the first moment of the output signal error is zero, and the second moment independent of the input signal (4)). Moreover, this is still the case if any statistically independent additional noise is added to the uniform PDF dither noise r_C on the region C .

Moreover, noise shaping can be applied around such subtractive dither in exactly the same way as before, as shown in figs. 6 and 7, or in equivalent noise shaping architectures, the only difference being that any filtering is now applied to n parallel signal channels. It is also possible, if desired, to use an $n \times n$ matrix error feedback filter $H(z^{-1})$ or $H'(z^{-1})$ in order to make the noise shaping dependent on the vector direction, for example to optimize directional masking of noise by signals (9), (10).

It is possible to generate uniform PDF vector dither r_C over the rhombic cell C described above by an algorithm such as the following: First generate, for example by the well-known congruence method, n statistically independent rectangular PDF dither signals r_i ($i = 1, \dots, n$) with peak values $\pm 1/2$ STEP, and also generate an additional two-valued random or pseudorandom signal u with value either 0 or 1. Then the values of the noise signal $r_C = (v_1, \dots, v_n)$ are given by:

```

if u = 0
  then  $v_i := r_i$  for all  $i = 1, \dots, n$ ,
  else  $d_j := \text{sgn}(r_j)$  if  $|r_j| > |r_i|$  for all  $i < j$  and  $|r_j| \geq |r_i|$  for all  $i > j$ 
       $d_i := 0$  for all other  $i$ ,
       $v_i := r_i - d_i \text{STEP}$  for all  $i = 1, \dots, n$ .
End if.

```

(5-7)

However, in applications of subtractive dither, this algorithm may involve unnecessary complication, since it can be shown that with the subtractive dither arrangement of fig. 4 with a uniform vector quantizer with quantization cell C , that a uniform PDF vector dither signal r_D may be used for any other uniform quantization cell D sharing the same grid G , and still will eliminate nonlinear distortion and modulation noise in the output. Whatever the shape of the other quantization cell D used for the dither signal, the resulting error signal from the subtractive dither arrangement of fig. 4 is a noise signal with uniform PDF statistics on the quantizer cell C of the uniform vector quantizer used.

This can allow a much simpler algorithm to be used for generating the vector dither in which $uSTEP$ is added to (or subtracted from) just one of the n rectangular PDF noise components. For example, a uniform PDF vector dither noise signal $r_D = (v_1, \dots, v_n)$ given by

$$\begin{aligned} v_1 &:= r_1 - uSTEP \\ v_j &:= r_j \text{ for } j = 2, \dots, n. \end{aligned} \quad (5-8)$$

may be used to subtractively dither the above rhombic quantizer.

5.4 Nonsubtractive case

Although we shall not need to use the nonsubtractive vector dither case in the hidden data channel application of this paper, it is easy to note the extension of the above to the nonsubtractive case. As in the scalar case reported in ref. [2], it can be shown that a uniform vector quantizer with quantizer cell C can be made to give an output suffering from no nonlinear distortion or modulation noise if dither noise is added before the quantizer that has the form of the sum of two statistically independent uniform PDF vector dithers each of the form r_C over the region C .

Such a dither is a vector analog of the triangular PDF dither [2] used in the scalar case, and may similarly be subjected to noise shaping of the dithered vector quantizer without introducing nonlinear distortion or modulation noise effects. As in the scalar case, such nonsubtractive dithering with no modulation noise gives a noise energy 3 times as large as does subtractive dithering.

6. Refinements of the basic proposal.

6.1 Further developments

The encoding process described above will work well as it stands, but does not incorporate various desirable refinements which we shall now describe. These include methods to take account of the fact that the data noise signal has a discrete and not a continuous PDF dither, and applications involving stereo parity coding.

6.2 Non-discrete dither

The fact that the dither given by the data noise signal has an M -level discrete probability distribution function rather than a continuous RPDF means that there is still unwanted quantization distortion at the level of the LSB of the audio word which is not properly dithered. Preferred methods of adding "non-discrete" dither (or, strictly speaking, dither at a significantly high arithmetic accuracy such as implemented using 24 or 32 bit arithmetic) are now described. The method of adding such dither shown in fig. 5 is not preferred for three reasons:

(i) Optimum playback requires subtractive decoding of the $\pm \frac{1}{2}$ LSB RPDF dither signal, with all the usual problems of implementing subtractive

dither [1], since unlike the discrete data noise signal, this is not explicitly transmitted in the audio word.

(ii) the $\pm 1/2$ LSB RPDF dither signal added before the quantizer does not eliminate modulation noise in non-subtractive playback, having the wrong statistics for this purpose [2], and

(iii) if the whole system is noise shaped as in figs. 6 or 7, the nonsubtractive listener will hear the $\pm 1/2$ LSB RPDF dither signal as having a white spectrum not affected by the noise shaping, so will perceive an increase in noise level.

A correct way of adding extra dither to avoid nonlinear quantization distortion and modulation noise at the $\pm 1/2$ LSB level is shown in figure 13. The dither used has a triangular PDF with peak levels ± 1 LSB (so-called TPDF dither) with independent statistics at each discrete time instant, so as to eliminate modulation noise in nonsubtractive playback [2], and is added before the quantizer in the noise shaping loop, but not subtracted in the noise shaping loop. This ensures that the added noise in nonsubtractive playback is noise shaped.

Subtractive playback of the extra dither is done, also as shown in fig. 13 by reconstituting the triangular ± 1 LSB PDF dither at the playback stage, passing it through a noise shaping filter $1 - H(z^{-1})$, and subtracting the filtered noise from the output audio word. Subtractive playback of course reduces the extra noise energy caused by the non-discrete dither by a factor 3, although this will only be highly advantageous in the case that the data noise signal has fairly low energy, e.g. at a data rate of 1 BPSS.

The triangular dither signal may be generated, in encoding, as proposed in the "autodither" proposal of ref. [3] by means of a pseudo-random logic look-up table (or a logic network having the effect of a pseudo-random look-up table) from the less or least significant parts of the output audio word in the last K previous samples, where typically K may be 24, and can be reconstructed from the same audio word at the input of the system by the same look-up table or logic in the decoding stage. This is shown in the case of the system of fig. 13 in fig. 14.

Although figures 13 and 14 are shown for the particular noise shaping architecture of fig. 6, similar ways of adding the extra triangular dither can be used with any other equivalent noise shaping architecture such as the outer form of figures 7 and fig. 10 - again by adding the triangular dither just before the quantizer and subtracting it again, via a noise shaping filter $1 - H(z^{-1})$, only at the output of the decoder. It is clear that the points at which dither signals are added can be shifted around in various ways without affecting the functionality.

6.3 The stereo parity case

Suppose we have 2-channel stereo signals in which data is encoded pseudorandomly in bit N for all $N = 15$ to say $15-h+1$ (where the integer h

may typically be any integer from say 0 to perhaps 6 or 8, the case 0 being the case of no bits being encoded) of the left and right audio words, and data also being encoded in the stereo parity (Boolean sum) of bit 15-h of the left and right audio words, as described in subsection 2.2 above.

Based on the results on uniform vector quantization and subtractive vector dither of section 5 above, the noise-shaped subtractive encoding of the data described above in the scalar case for individual audio channels may be applied to this case too with just two reinterpretations of the above:

(i) The uniform quantizer used in figs. 6-10 now becomes a uniform 2-dimensional rhombic quantizer (such as described in Algorithm (5-6) and illustrated in fig. 12) with $STEP = 2^h$ LSB.

(ii) the "data noise signal" used for dithering is given, for example, by Eqs. (5-8) where r_i is the data noise signal of the last h bits of the i-th channel audio word (with the first channel being say left and the 2nd channel being say right), and u being the parity of bits 15-h of the left and right audio words. In units of LSB, the data noise signal for the left channel is then $L_0 - 2^h u$ and for the right channel is R_0 , where L_0 and R_0 are the respective integer words represented by the last h bits of the audio word formed by the data in the two channels.

Any alternative data noise signal may be used that represents an appropriate uniform PDF vector dither as described in section 5.3, such as for example that given by Algorithm (5-5).

The residual nonlinear distortion and modulation noise effects at the LSB level caused by the fact that the vector data noise is discrete rather than continuous can be removed by using exactly the same technique described in subsection 6.2 and figs. 13 and 14 above by adding and, where appropriate, subtracting ± 1 LSB triangular PDF dither in each channel separately, the only difference being that the uniform quantizer has become a rhombic vector quantizer and the data noise signal has a modified vector form as just described.

The particular case $h = 0$, where data is transmitted only in the parity of the LSB of the audio word in 2 channels, simply uses the parity signal itself at the LSB level as a "data noise signal" in one of the two channels in the encoding process - it does not matter which of the two channels is chosen. With subtractively dithered playback, it turns out that the use of properly designed stereo parity coding of data, using a rhombic vector quantizer in the encoding process, gives a total noise level 1 dB lower than would the process of coding the data into the LSBs of the words of just one of the two audio channels. Thus stereo parity coding at low bit rates not only ensures audio left/right symmetry for added noise, but gives a significant noise level advantage.

6.4 Generalized stereo parity coding

There are various generalizations of the particular stereo parity coding case just described. We outline these briefly to show the applicability of these

ideas to other cases.

A first obvious generalization is that obviously the same process may be applied to other audio wordlengths besides the 16 bit wordlength of CD - for example to the 10 bit wordlengths of NICAM encoded digital signals or to the 20 bit or 24bit wordlengths used in some professional audio applications when it is desired to hide data in the audio words. For example, in ref. [3], the authors described a proposal to add data at the 24th bit in studio operations on signals to detect whether or not they had been modified, and the data encoding techniques of this paper can be used in that application to minimize the audibility of the modification of the signal proposed there.

The second generalization is that one can also apply stereo parity coding to the case where one replaces the 2^h -level data in the last h bits by an M -level case for any integer $M > 1$. In this case, data is coded into the residue of the audio words of the two channels after division by M , and the "stereo parity" data channel is coded into the Boolean sum of the binary LSB in the two channels of the integer parts of the audio words divided by M . This case is handled identically to that in the previous sub-section 6.3 except that 2^h is replaced throughout by M , and the phrase "last h bits" is replaced by "residue modulo M ".

A third generalization instead considers n channels rather than two. As before, this uses a rhombic quantizer in the encoding process for $STEP = M$ LSBs, but now the n -dimensional rhombic quantizer described in (5-3) to (5-5) above, and a vector data noise signal comprising the n M -level data noise signals generated for the residue modulo M data conveyed in each of the n audio channels, to just one of which at each instant is added or subtracted $uSTEP$, where u is the parity (i.e. Boolean sum) of the binary LSB in the n channels of the integer parts of the audio words divided by M . Other than replacing the ordinary uniform quantizers with step size $STEP$ by a rhombic quantizer and using the modified data noise signal, the descriptions given earlier for coding data still apply to this case.

Note that the choice of which channel of the vector data noise signal to add or subtract $uSTEP$, and the choice of whether to add or subtract, can be made freely, and that this choice can be made adaptively instant by instant to minimize data noise energy if desired, e.g. by making that choice which minimizes the maximum of the data noise signals in the n channels at each instant. This choice is (a discrete approximation to) that described in (5-7) for uniform PDF vector dither over a rhombic quantizer cell.

6.5 Low bit-rate case

If one has n transmitted channels of audio, then the parity of their LSBs can be used to transmit a 1 bit per n -channel-sample data channel, with remarkable little loss of S/N, especially in the case that full subtractive dithering is used at the LSB level. One might expect a loss of S/N of $6.02/n$ dB because the loss is shared among n channels, but for $n > 2$, one gets a

smaller loss, typically between 0.3 and 0.4 dB better, because of the fact noted in section 5 that rhombic vector quantization has a better S/N than independent channel quantization for a given density of quantization points in the quantization grid. For $n = 6$, a 1 bit per n -channel-sample subtractively dithered buried data channel causes a S/N degradation of under 0.6 dB compared with a properly dithered case with no buried data channel.

Exactly the same techniques can be used to convey data via q successive samples of a monophonic signal, for example by coding into the parity of the LSBs of each successive block of q samples, as described in section 2.3. What we have now shown is that by using the parity signal as a subtractive dither for any one sample with a q -dimensional rhombic quantizer, plus normal triangular additive or subtractive dither, that this fractional rate channel can be coded with a very small loss of S/N (e.g. 0.6dB for a block length $q = 6$), and yet with no nonlinear distortion or modulation noise in either nonsubtractive or subtractive reproduction.

This kind of efficient low bit-rate culling of data capacity could be used, for example, with successive samples within individual subband channels of a subband data compression system. Its application is not confined to audio; culling say 1 bit per 6 10-bit video samples in a digital video recorder with a video data rate of 200 Megabits per sec. would give a data rate typically enough for 4 16-bit audio channels or a consumer-grade additional data-reduced video signal while losing only 0.6 dB in video S/N in the original video channel.

7. Conclusions

7.1 Audio Quality Considerations

Anyone concerned with the future potential of the audio art will have some concern about using information originally allocated to a high-quality audio signal to transmit other data instead, as in the proposal in this paper. In order to encourage progress in the audio art, there is a need for at least one widely available consumer medium without built-in serious quality compromises, such as CD (unlike data reduced digital systems) offers, so that the market is there in which recordings with improved quality can be made, heard and sold. Without such a medium, we shall find ourselves permanently locked into limitations many of which will only become apparent as the art of recording, psychoacoustics and studio production develop further.

Even the best theoretical models of the ears are still extremely crude, for example not describing the effect of hearing multiple events with individually low but jointly high detection probabilities, especially for non-stationary or transient signals. Many of the musical subtleties of the best "pursist" recordings probably reside in these areas of our technical ignorance.

We have therefore been concerned to devise buried channels that satisfy far

more stringent requirements than simply satisfying crude masking models, which we feel still have limited applicability to state-of-the-art recording quality. This conservative attitude means that (although the option is there with adaptive data rates and noise shaping for our proposal to code data if desired to satisfy existing masking models) such masking models are in no way assumed in the standard. It is a matter of judgment on a case-by-case basis of individual recordings whether such signal manipulations of the error are subjectively acceptable.

In cases where such compromises are not acceptable or are considered too risky (especially for material with high or serious artistic intent), our proposal allows the hidden data channels to produce the most benign kind of error - namely a steady noise error free of all nonlinear distortion or modulation noise, and having any desired spectral shape. Unlike previous proposals, this allows avoidance of all psychoacoustically disturbing patterns in the error signal, whether related to the audio signal or to patterns in the transmitted data.

The beauty of this proposal is that, by incorporating noise shaping and subtractive dither, it avoids adding any more error noise to the audio signal than is strictly necessary to handle the desired data rate, typically allowing up to 20 dB better perceived signal-to-noise ratio than would be achieved simply by replacing the relevant audio word bits by data, and typically allowing up to 25 dB better perceived signal-to-noise ratio than would be achieved were one also to attempt adding dither in a simple replacement scheme to avoid nonlinear distortion and modulation noise.

Particularly at low data rates, the audio performance of our proposed scheme will typically be comparable to or better than some of the better noise-shaped dithering systems currently on the market, i.e. a CD carrying the hidden data channels is likely to sound better than current CDs without the data channel, since the encoding standard incorporates properly designed dithering (and optional properly designed noise shaping). Even at the higher data rates, the use of proper dithering may well mean a better sound than is currently the norm.

All other things being equal, an audiophile listener would not choose any degradation of audio quality, even if this takes the form of a smooth steady noise free of unwanted modulation and nonlinear distortion effects. But things are not equal, since the data channels can be used to convey additional audio channels in a fully compatible way. Providing the coding of these additional audio channels is done with sufficient care to avoid audible data reduction artifacts, we believe that the overall improvement obtained by adding at least one extra audio channel, either for horizontal B-format Ambisonic surround-sound or for three-channel frontal stage stereo, may subjectively more than make up for the relatively benign loss of signal-to-noise ratio (compared to the best noise-shaped dithered performance of which CD is capable) of the added data channels.

Alternative audio uses of the additional data channel includes compatible frequency-range extension without the audible degradations of quality heard in existing commercial schemes for this, and the transmission of level-alteration information to allow dynamic range adjustment of the recording for users equipped with data decoders.

7.2 Summary

In this paper, we have described a method of forcing the least significant information in the audio words to conform to the data values of data channels, while ensuring that the effect on the audio is that of adding a noise-shaped steady pattern-free random noise at a level no greater than would be expected from Shannon Information theory from the number of bits "stolen" from the audio for an optimally noise shaped subtractively dithered system.

These techniques involve a process for pseudo-randomizing the data so that the audio sees it as a random noise signal which is optimized for subtractively dithering the audio, to eliminate both nonlinear distortion and modulation noise. Not only is the subtractive dithering automatically operative in ordinary playback, but additionally full noise shaping can be applied to the data dither as well.

This paper has further extended this technique not just to the encoding of data in individual audio signals, but to a technique, stereo parity coding, that allows efficient coding of data jointly into two or more audio channels, by using a vector quantization and subtractive vector dithering process. The joint coding process not only ensures symmetry of the way noise is distributed among the audio channels, but additionally gives a substantial improvement in noise performance, especially at low data rates in the data channels. The attainable noise performance approaches the theoretical Shannon limits for the combined Shannon data rate of the audio and buried data channels.

In describing these techniques, a brief account has been given of the generalization of the ordinary theory of subtractive dither to the vector quantizer and vector dither case.

Possible uses of the resulting benign hidden data channels have been described, including additional audio channels for multichannel stereo or surround sound, audio bandwidth extension, dynamic range control, as well as obvious data applications such as graphics, text/lyrics, copyright, track information, and even data-reduced video.

Unlike previous approaches, no assumptions have been made regarding the masking abilities of the ears - rather the design aim has been to ensure that the only effect on the existing audio of adding data is to cause a minimal increase in steady background noise, ensuring no compromise with other audio virtues of compact disc. If a noise performance comparable to good current CD's is acceptable, this allows data rates of up to 360 kbit/s to be

transmitted in the buried data channel, although much more stringent noise requirements can be met at the expense of a reduced data rate.

The authors are open to approaches from concerns wishing to develop particular applications or develop technical standards for uses of the buried data channels.

8. References

- [1] M.A. Gerzon & P.G. Craven, "Optimal Noise Shaping and Dither of Digital Signals", Preprint 2822 of the 87th Audio Engineering Society Convention, New York (1989 Oct. 16-21)
- [2] S.P. Lipshitz, R.A. Wannemakar & J. Vanderkooy, "Quantization and Dither: A Theoretical Survey", J. Audio Eng. Soc., vol. 40 no. 5, pp. 355-375 (1992 May)
- [3] P.G. Craven & M.A. Gerzon, "Compatible Improvement of 16-Bit Systems Using Subtractive Dither", Preprint 3356 of the 83rd Audio Engineering Society Convention, San Francisco (1992 Oct. 1-4)
- [4] M.A. Gerzon, P.G. Craven, R.J. Wilson & J.R. Stuart, "Psychoacoustic Noise Shaped Improvements in CD and Other Linear Digital Media", Preprint presented at the 94 Audio Engineering Society Convention, Berlin (1993 March.)
- [5] W.R. Th. Ten Kate, L.M. Van De Kerkhof & F.F.M. Zijderveid, "A New Surround-Stereo-Surround Coding Technique", J. Audio Eng. Soc., vol. 40 no. 5, pp. 376-383 (1992 May)
- [6] M.A. Gerzon, "Hierarchical Transmission System for Multispeaker Stereo", J. Audio Eng. Soc., vol. 40 no. 8, pp. 692-705 (1992 Sept.)
- [7] M.A. Gerzon, "Hierarchical System of Surround Sound Transmission for HDTV", Preprint 3339 of the 92nd Audio Engineering Society Convention, Vienna (1992 Mar.)
- [8] M.A. Gerzon, "Compatibility of and Conversion Between Multispeaker Systems", Preprint 3405 of the 83rd Audio Engineering Society Convention, San Francisco (1992 Oct. 1-4)
- [9] M.A. Gerzon, "Problems of Error-Masking in Audio Data Compression Systems", Preprint 3013 of the 90th Audio Engineering Society Convention, Paris (1991 Feb.)
- [10] M.A. Gerzon, "Directional Masking Coders for Multichannel Subband Audio Data Compression", Preprint 3261 of the 92nd Audio Engineering Society Convention, Vienna (1992 Mar.)
- [11] M.A. Gerzon, "Problems of Upward and Downward Compatibility in Multichannel Stereo Systems", Preprint 3404 of the 93rd Audio Engineering Society Convention, San Francisco (1992 Oct. 1-4)
- [12] M.A. Gerzon, "The Design of Distance Panpots", Preprint 3308 of the 92nd Audio Engineering Society Convention, Vienna (1992 Mar.)
- [13] M.A. Gerzon, "Periphony: With-Height Sound Reproduction", J. Audio Eng. Soc., vol. 21, pp. 2-10 (1973 Jan./Feb.)
- [14] M.A. Gerzon, "PracticalPeriphony", Preprint 15__ of the 65th Audio Engineering Society Convention, London (1980 Feb.)
- [15] M.A. Gerzon, "Ambisonics in Multichannel Broadcasting and

- Video", J. Audio Eng. Soc., vol. 33 no. 11, pp. 859-871 (1985 Nov.)
- [16] A.J. Mason, A.K. McParland & N.H.C. Gilchrist, "Unobtrusive Compression of Dynamic Range", Preprint 3433 of the 93rd Audio Engineering Society Convention, San Francisco (1992 Oct. 1-4)
- [17] R.A. Wannamaker, S.P. Lipshitz, J. Vanderkooy & J.N. Wright, "A Theory of Non-Subtractive Dither", submitted to IEEE Trans. Sig. Proc. (1991)
- [18] S.P. Lipshitz, J. Vanderkooy & R.A. Wannamaker, "Minimally Audible Noise Shaping", J. Audio Eng. Soc., vol. 39 no. 11, pp. 836-852 (1991 Nov.) Corrections to be published in JAES
- [19] S.P. Lipshitz, R.A. Wannamaker & J. Vanderkooy, "Dithered Noise Shapers and Recursive Digital Filters", to be presented at the 94th Audio Engineering Society Convention, Berlin (1993 Mar.)
- [20] J.R. Stuart & R.J. Wilson, "A Search for Efficient Dither for DSP Applications", Preprint 3334 of the 92nd Audio Engineering Society Convention, Vienna (1992 March)
- [21] P.A. Regalia, S.K. Mitra, P.P. Vaidyanathan, M.K. Rentons & Y. Nuevo, "Tree-Structured Complementary Filter Banks Using All-Pass Sections", IEEE Trans. Circuits & Systems, vol. CAS-34 no. 12, pp. 1470-1484 (1987 Dec.)
- [22] R.E. Crochiere & L.R. Rabiner, "Multirate Digital Signal Processing", Prentice-Hall Inc., Englewood Cliffs, New Jersey (1983), especially chapter 7.
- [23] H.M. Coxeter, "Regular Polytopes" (2nd Edition), Macmillan
- [24] J.R. Emmett, "Buried Data in NICAM transmissions", Preprint 3260 of the 92nd Audio Engineering Society Convention, Vienna (1992 March)

9. PATENT NOTE

The authors have applied for patents on various techniques described in this paper.

10. ACKNOWLEDGEMENTS

The authors acknowledge useful and relevant discussions with many people on topics related to this paper over the years, including Dr. Geoffrey Barton, Dr. Raymond Veldhuis, and J.R. Emmett.

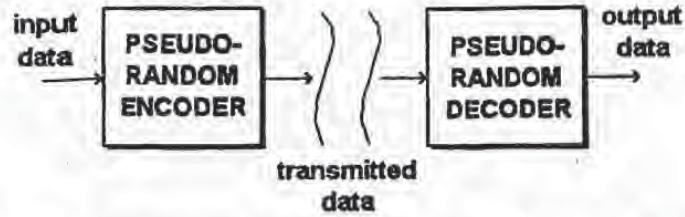


Figure 1. Pseudo random encoding and decoding of data transmitted via CD channel to ensure noise-like behavior.

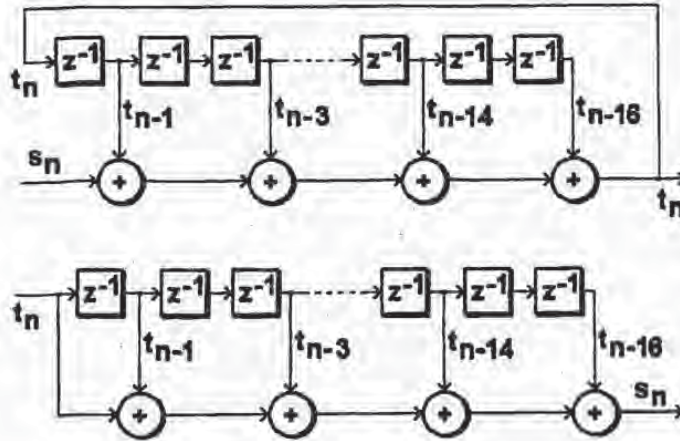


Figure 2. Binary pseudo-random sequence generator using shift-register logic, with input "exclusive or" gate for encoding and decoding of binary data stream.

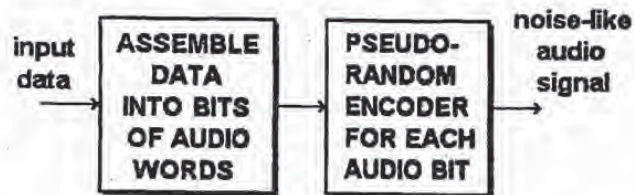


Figure 3. Schematic of processing of data to form audio noise-like signal.

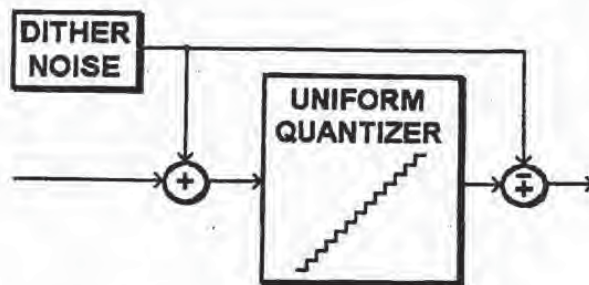


Figure 4. Subtractive dither around a uniform quantizer.

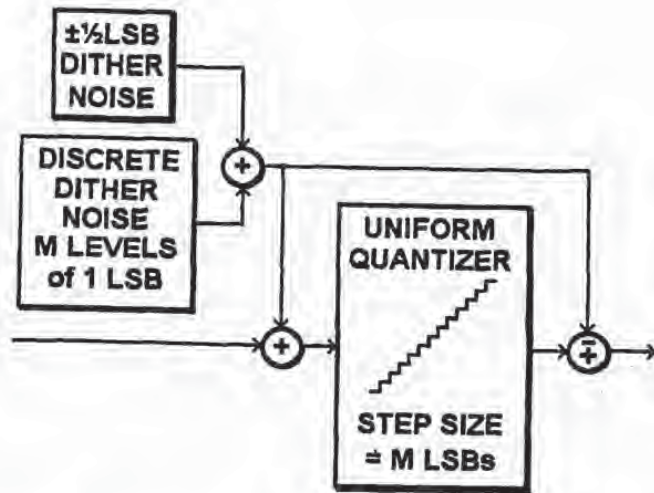


Figure 5. Subtractive dither using a combination of discrete and continuous RPDF dither.

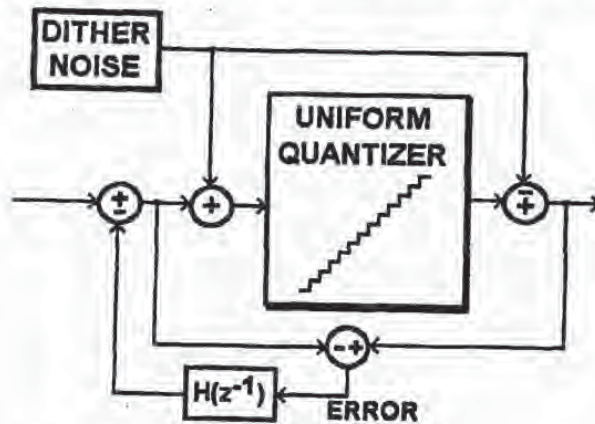


Figure 6. Noise shaped subtractively dithered uniform quantizer.

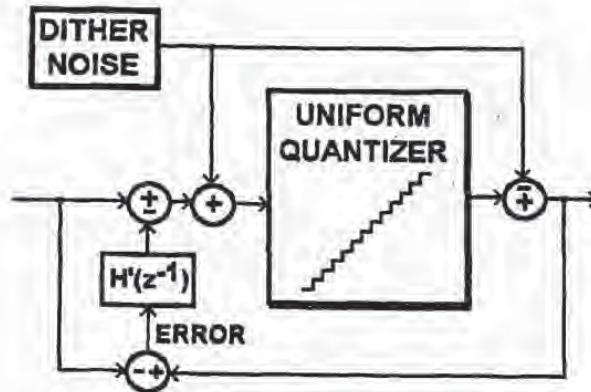


Figure 7. "Outer" form equivalent to that of fig. 6 for noise-shaped subtractively dithered uniform quantizer, where $H'(z^{-1}) = H(z^{-1})/(1-H(z^{-1}))$.

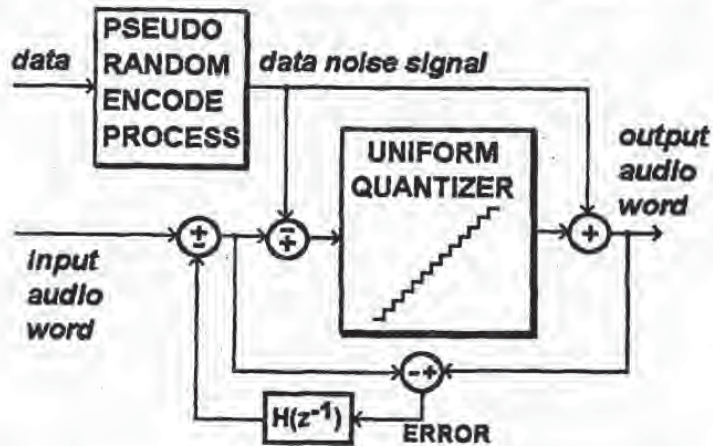


Figure 8. Noise shaping round pseudo random data noise signal encoding of data into an audio word. Standard noise shaper form.

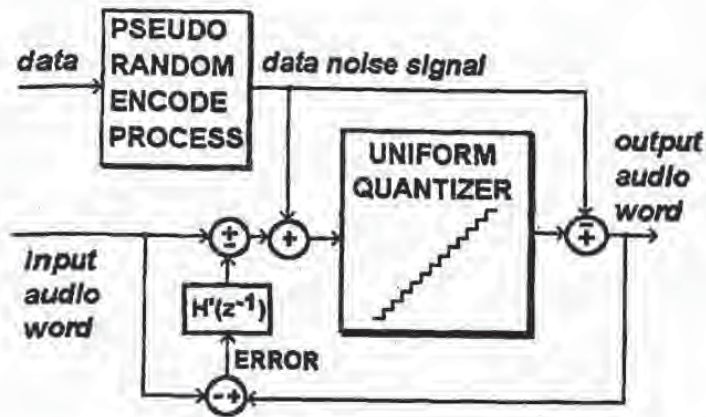


Figure 9. Noise shaping round pseudo random data noise signal encoding of data into an audio word. "Outer" noise shaper form equivalent to fig 8 if $H'(z^{-1}) = H(z^{-1})/(1+H(z^{-1}))$.

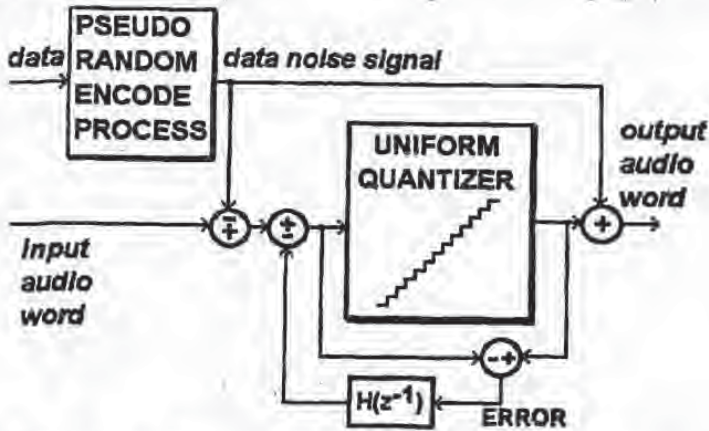


Figure 10. Further implementation of noise shaping round pseudo random data noise signal encoding of data into an audio word.

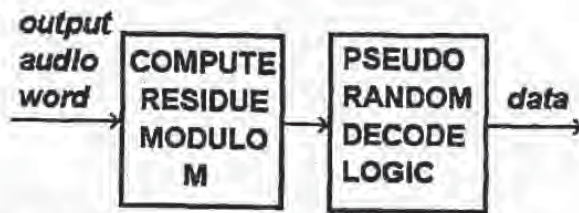


Figure 11. Recovery of the data signal from the received coded audio word.

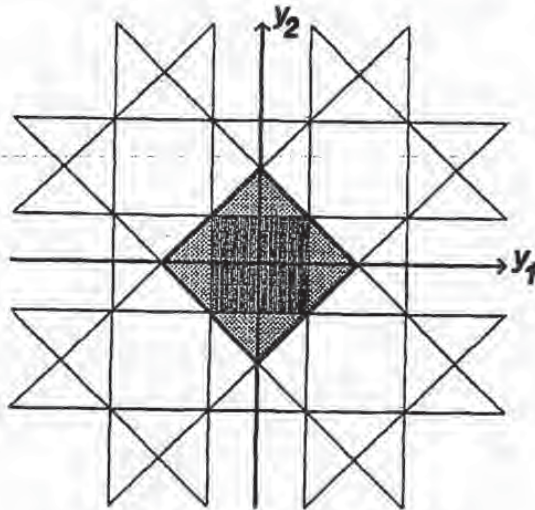


Figure 12. 2-dimensional rhombic quantizer region (shaded square with sides tilted 45°) shown against a background (squares with horizontal and vertical sides) of conventional independent quantizers (whose square quantizer region is darkly shaded) on each channel y_1 and y_2 .

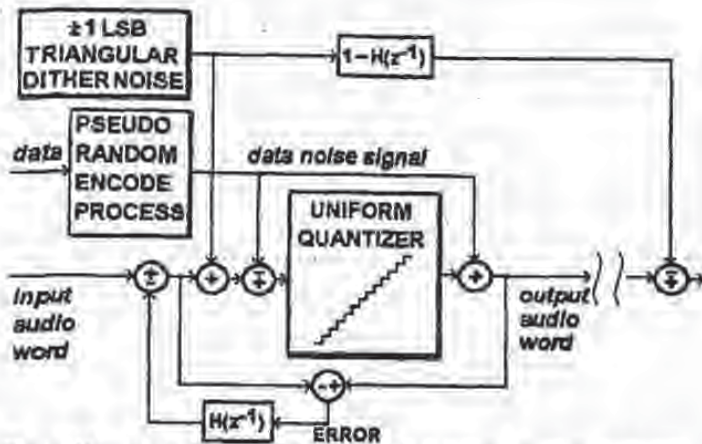


Figure 13. Use of extra subtractive dither to eliminate nonlinear distortion and modulation noise at LSB level, using noise shaped triangular PDF dither having ± 1 LSB peaks to achieve good results in both nonsubtractive reproduction of output audio word and (shown) subtractive reproduction.

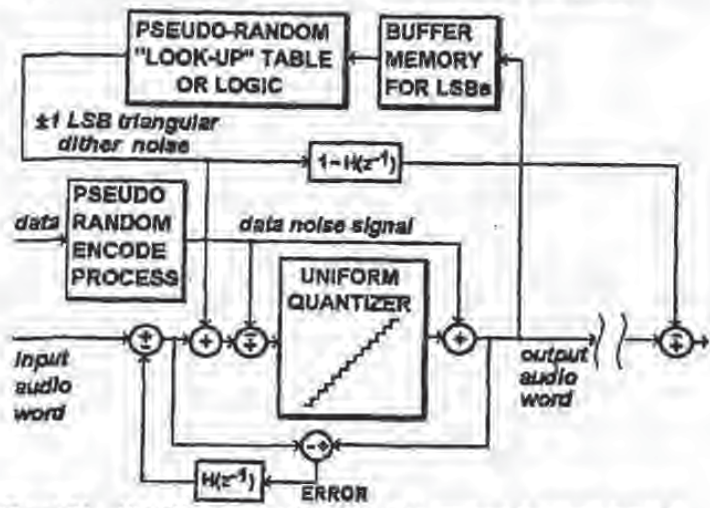
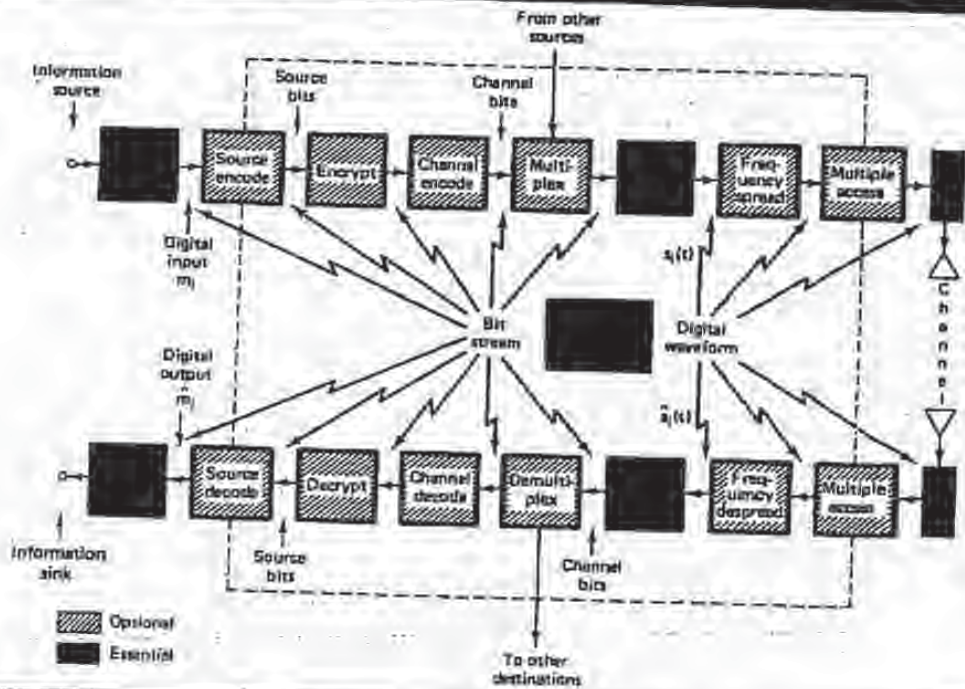


Figure 14. Use of autodither with figure 13 to generate triangular dither in encoder and decoder.

DIGITAL COMMUNICATIONS

Fundamentals and Applications



BEST AVAILABLE COPY

Library of Congress Cataloging-in-Publication Data

SKLAR, BERNARD (date)
Digital communications.
Bibliography: p.
Includes index.
1. Digital communications. I. Title.
TK5103.7.S55 1988 621.38'0413 87-1316
ISBN 0-13-211939-0

Editorial/production supervision and
interior design: Reynold Rieger
Cover design: Wanda Labelska Design
Manufacturing buyers: Gordon Osbourne and Paula Benevento

© 1988 by P T R Prentice Hall
Prentice-Hall, Inc.
Upper Saddle River, New Jersey 07458

All rights reserved. No part of this book may be
reproduced, in any form or by any means,
without permission in writing from the publisher.

Printed in the United States of America

20

ISBN 0-13-211939-0

Prentice-Hall International (UK) Limited, London
Prentice-Hall of Australia Pty. Limited, Sydney
Prentice-Hall Canada Inc., Toronto
Prentice-Hall Hispanoamericana, S.A., Mexico
Prentice-Hall of India Private Limited, New Delhi
Prentice-Hall of Japan, Inc., Tokyo
Pearson Education Asia Pte. Ltd., Singapore
Editora Prentice-Hall do Brasil, Ltda., Rio de Janeiro

BEST AVAILABLE COPY

DISH - Blue Spike-408
Exhibit 1010, Page 0445

the source with
ven though the a

11.2 consists of 0
ccessive symbols
is binary 2-tuples

0.833

1.055

1.045

1.045

opy for this code
10) as follows:

$H(X_2|d)$

ion code, which

23

28

18

13

13

8

8

3

this extension

three-symbol

Chap. 11

descriptions of the source (0.470, 0.412, and 0.408 bit, respectively) are decreasing asymptotically toward the source entropy of 0.357 bit/input symbol. Remember that the source entropy is the lower bound in bits per input symbol for this (infinite memory) alphabet and this bound can only be approached asymptotically with finite-length coding.

11.1.2 Waveform Sources

A waveform source is a random process of some independent variable. We classically consider this variable to be time, so that the waveform of interest is a time-varying waveform. Important examples of time-varying waveforms are the outputs of transducers used in process control, such as temperature, pressure, velocity, displacement, and flow rates. Examples of particularly high interest include speech and music waveforms. The waveform can also be a function of one or more spatial variables (e.g., displacement). Important examples of spatial waveforms include single images such as a photograph, or moving images such as the successive images (at 24 frames/s) of moving picture film. Spatial images are often converted to time-varying functions by a simple scanning operation. This, for example, is done for facsimile transmission and with a slight modification (called interlacing) for standard broadcast television.

11.1.2.1 Amplitude Density Functions

Discrete sources were described by a list of their possible elements (called letters of an alphabet) and their multidimensional probability density functions (pdfs) of all orders. By analogy, waveform sources are similarly described in terms of their probability density functions as well as parameters and functions derived from these functions. We model many waveforms as random processes with classical probability distribution functions and with simple correlation properties. In the modeling process we distinguish between short-term or local (time) characteristics and long-term or global characteristics. This partition is necessary because many waveforms are nonstationary.

The probability density function of the actual process may not be available to the system designer. Sample density functions can, of course, be rapidly formed in real time during a short preceding interval and used as reasonable estimates over the present interval. A less ambitious task is simply to make estimates of short-term waveform-related averages. These include the sample mean (or time-average value), the sample variance (or mean-square value assuming zero mean), and correlation coefficients formed over the previous sample interval. In many applications of waveform analysis, the input waveform is converted to a zero-mean waveform by subtracting the estimates of the mean. This happens, for example, in a digital panel meter in which an auxiliary circuit measures the effects of the internal dc offset voltages and subtracts them in a process known as *auto-zero*. Further, the variance estimate is often used to scale the range of the input waveform to match the dynamic amplitude range of subsequent waveform-handling equipment. This process, performed in the digital panel meter, is called

arranging or automatic gain control (AGC). The function of these signal conditioning operations, mean removal and variance control (gain adjustment) shown in Figure 11.2, is to normalize the probability density functions of the input waveform. This normalization assures optimal utility of the limited dynamic range of subsequent recording, transmission, or processing subsystems.

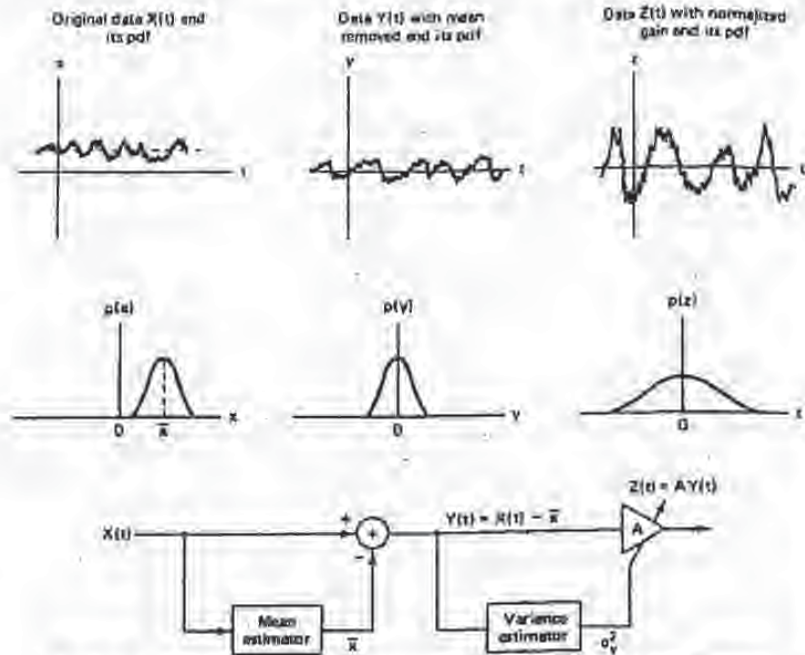


Figure 11.2 Mean removal and variance control (gain adjustment) for a data-dependent signal conditioning system.

11.1.2.2 Autocorrelation Function, Power Spectrum, and Models

There is significant correlation between the amplitudes of many waveform sources in successive time intervals. This correlation means that successive time samples are not independent. If the time sequence is truly independent, the autocorrelation function of the sequence would be an impulse function. The width of the autocorrelation function (in seconds) is called the correlation time of the process and is akin to the time constant of a filter. This time interval is an indication of how much shift along the time axis is necessary to find uncorrelated data samples. If the correlation time is large, we interpret this to mean that the waveform makes significant amplitude changes slowly. Conversely, if the correlation

al con-
shown
l wave-
ange of

10/1/82

A₁

—

rm
oc
uu
jlb
hc
ca
ta
e-
m

11

time is small, we infer that the waveform makes significant amplitude changes very quickly.

The Fourier transform of the autocorrelation function is the power spectral density of the waveform process. Thus an alternative description of the autocorrelation function, which reflects the amount of intersample dependence, is the degree of flatness in the waveform power spectrum. A flat spectrum, sometimes called a *white spectrum*, corresponds to source waveforms with independent values sample to sample. A power spectrum with a wide bandwidth implies a time function capable of rapid changes in envelope, while a power spectrum with a narrow bandwidth suggests a time function capable of only slow changes. In general, the larger the deviation from flatness, the more correlation will be found in the waveform samples. Very large changes from flatness in the power spectrum may warrant source descriptions which partition the spectrum, via filters, into subbands each of which is described and quantized separately.

11.2 AMPLITUDE QUANTIZING

Amplitude quantizing is the task of mapping samples of a continuous amplitude waveform to a finite set of amplitudes. The hardware that performs the mapping is the analog-to-digital converter (ADC or A-D). The amplitude quantizing occurs after the sample-and-hold operation. The simplest quantizer to visualize performs an instantaneous mapping from each continuous input sample level to one of the preassigned equally spaced output levels. Quantizers that exhibit equally spaced increments between possible quantized output levels are called *uniform quantizers* or sometimes *linear quantizers*. Possible instantaneous input-output characteristics are easily visualized by a simple staircase graph consisting of risers and treads of the types shown in Figure 11.3. Figure 11.3a, b, and d show quantizers with uniform quantizing steps, while Figure 11.3c is a quantizer with nonuniform quantizing steps. Figure 11.3a depicts a quantizer with *midread* at the origin, while Figure 11.3b and d present quantizers with *midrisers* at the origin. A distinguishing property of midriser and midread converters is related to the presence or absence, respectively, of output level changes when the input to the converter is idle noise. Further, Figure 11.3d presents a *biased* (i.e., truncation) quantizer, while the remaining quantizers in the figure are unbiased and are referred to as *rounding quantizers*. Most quantizers are truncation quantizers due to implementation considerations. The terms "midread" and "midriser" are staircase terms used to describe whether the horizontal or vertical member of the staircase is at the origin. The unity-slope line passing through the origin represents the ideal nonquantized input-output characteristic we are trying to approximate with the staircase. The difference between the staircase and the unity-slope line segment represents the approximation error made by the quantizer at each input level. Figure 11.4 illustrates the approximation error amplitude versus input amplitude function for each quantizer characteristic in Figure 11.3. Parts (a) through (d) of Figure 11.4 correspond to the same parts in Figure 11.3. This error is often modeled as quantizing noise because the error sequence obtained when quantizing a

BEST AVAILABLE COPY

DIGITAL CODING OF WAVEFORMS
Principles and Applications
to Speech and Video

N. S. JAYANT

*Bell Laboratories, Inc.
Murray Hill, NJ*

PETER NOLL

Technical University of Berlin

ing

PRENTICE-HALL, INC. Englewood Cliffs, New Jersey 07632

Library of Congress Cataloging in Publication Data

Jayant, Nuggethally S., 1946-
Digital coding of waveforms.

Includes index.

1. Signal processing—Digital techniques. 2. Coding theory. I. Noll, P. (Peter), 1936- II. Title.
TK5102.J39 1984 621.38'043 85-22170
ISBN 0-13-211913-7

Editorial/production supervision: *Shari Ingerman*
Cover design: *Edsal Enterprises*
Manufacturing buyer: *Tony Caruso*
Page layout: *Diane Koromhas*

© 1984 by Bell Telephone Laboratories, Incorporated

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN 0-13-211913-7 01

Prentice-Hall International, Inc., *London*
Prentice-Hall of Australia Pty. Limited, *Sydney*
Editora Prentice-Hall do Brasil, Ltda., *Rio de Janeiro*
Prentice-Hall Canada Inc., *Toronto*
Prentice-Hall of India Private Limited, *New Delhi*
Prentice-Hall of Japan, Inc., *Tokyo*
Prentice-Hall of Southeast Asia Pte. Ltd., *Singapore*
Whitehall Books Limited, *Wellington, New Zealand*

11

Sub-Band Coding

11.1 Introduction

In the class of *time domain* coding algorithms (Chapters 5 to 10), the input waveform is treated as a single full-band signal; and in predictive coders, redundancy is removed prior to encoding by prediction and inverse filtering. The main differences in the various algorithms are determined by the degree of prediction (Chapters 6 to 8) that is employed, and by whether schemes are adaptive or not. In delayed decision coding (Chapter 9), input structure is exploited by means of a multipath search.

In Chapters 11 and 12 another class of encoding algorithms will be discussed in which the approach is to divide the input signal into a number of separate frequency components, and to encode each of these components separately. This division into frequency components removes the redundancy in the input and provides a set of uncorrelated inputs to the channel. Recall that the action of a DPCM coder is also similar, if not identical. The encoder in that case, when fed by a redundant signal, outputs a sequence of prediction error components that tend to be uncorrelated. The *frequency domain* coding techniques have the advantage that the number of bits used to encode each frequency component can be variable, so that the encoding accuracy is always placed where it is needed in the frequency domain. In fact, bands with little or no energy may not be encoded at all. Variable bit allocation can in principle provide arbitrary forms of noise shaping, a feature that was realized to some extent by noise feedback in the time-domain methods of Chapter 7.

As in the case of time domain techniques, a large variety of frequency domain algorithms, from simple to complex, are available and the main differences are usually determined by the way in which source statistics are modeled, and the degree to which source redundancy is exploited, in the technique. We will begin by describing one technique of lower complexity called *Sub-Band Coding (SBC)* and then proceed to one of higher complexity called *Transform Coding (TC)* (Chapter 12). In the notation of Chapter 1, SBC with fixed bit allocation will be a *medium-complexity coder* and TC with variable bit allocation will be a *high-complexity coder*.

Unless otherwise mentioned, focus in this SBC chapter will be on speech waveforms. In the sub-band coder the speech band is divided into typically four or more sub-bands by a bank of bandpass filters. Each sub-band is, in effect, lowpass translated to zero frequency by a modulation process equivalent to single-side-band amplitude modulation. It is then sampled (or resampled) at its Nyquist rate (twice the width of the band) and digitally encoded with a PCM or DPCM encoder [Crochiere, Webber and Flanagan, 1976] [Esteban and Galand, 1978]. In this process, each sub-band can be encoded according to perceptual criteria that are specific to that band. On reconstruction, the sub-band signals are decoded and modulated back to their original locations. They are then summed to give a close replica of the original speech signal.

Encoding in sub-bands offers several advantages. By appropriately allocating the bits in different bands, the number of quantizer levels and hence reconstruction error variance can be separately controlled in each band, and the shape of the overall reconstruction error spectrum can be controlled as a function of frequency. In the lower frequency bands, where pitch and formant structure must be accurately preserved, a larger number of bits/sample can be used; whereas in upper frequency bands, where fricative and noise-like sounds occur in speech, fewer bits/sample can be used. Further, quantization noise can be contained within bands to prevent masking of a low-level input in one frequency range by quantizing noise in another frequency range. Section 11.2 gives a quantitative demonstration of objective (SNR) gains due to sub-band coding.

The most complex part of the coder is the filter bank [Bellanger, Bonnerot and Coudreuse, 1976] [Esteban and Galand, 1977]. With newer filter technologies such as CCD filters and digital filters, this complexity is rapidly being reduced. Also the design technique of *quadrature-mirror filters* (Section 11.4) affords distinct advantages in digital implementation of this coder.

Figure 11.1 illustrates a basic block diagram of the sub-band coder. The coder consists of a bank of M bandpass filters, followed by sub-band encoders which typically are PCM-AQB coders, and a multiplexer. The receiver has the inverse stages of demultiplexing, decoding and bandpass filtering prior to sub-band addition. Unlike the spectrum channel vocoder for synthetic speech [Flanagan et al., 1979] [Rabiner and Schafer, 1978] where the object of the filter-bank is only to preserve information about short-time energy as a function of frequency, the sub-band coder in Figure 11.1 transmits individual time waveforms $x_k(t)$; $k = 1, 2, \dots, M$ and the receiver adds decoder versions $y_k(t)$ phase-synchronously to obtain $y(t)$. The sub-band coder is therefore a waveform-preserving coder.

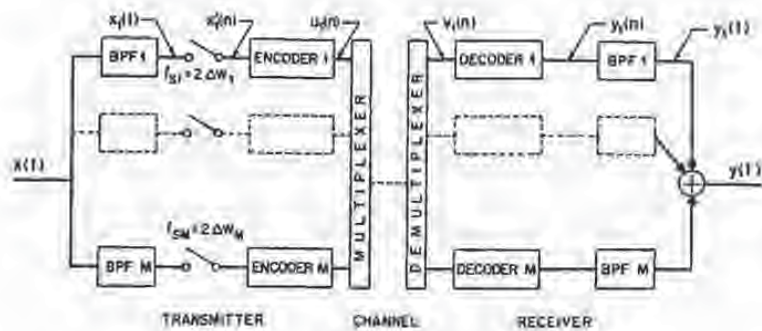


Figure 11.1 Block diagram of sub-band coding (SBC).

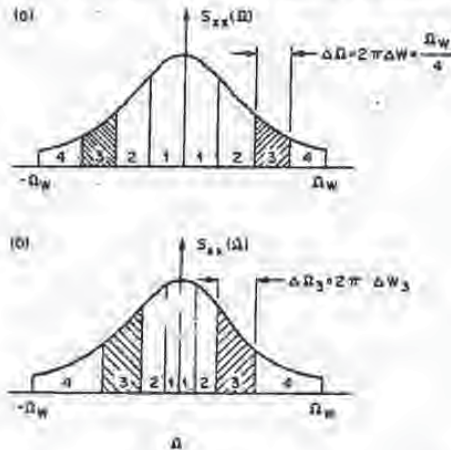
In Figure 11.1, sub-band width ΔW_k was a function of sub-band number k , implying *variable-width* sub-bands. The special case of *equal-width* sub-bands is important for implementation (Section 11.4) as well as analytical tractability (Section 11.2). Both types of arrangements will be considered for the sub-band coding of speech (Section 11.5). Figure 11.2 illustrates the two classes of arrangements for the example of $M = 4$. Shaded regions define sub-band number $k = 3$.

In the case of *equal-width* sub-bands

$$\Delta W_k = \Delta W = W/M; \quad k = 1, 2, \dots, M \quad (11.1)$$

$$\Delta \Omega = 2\pi\Delta W = \Omega_W/M = 2\pi W/M$$

Figure 11.2 Division of input spectrum into $M = 4$ sub-bands of (a) constant and (b) variable width.



where W and Ω_W represent the total input bandwidth in Hz and radians/second, respectively. In the case of unequal sub-bands, they are typically made wider as k increases:

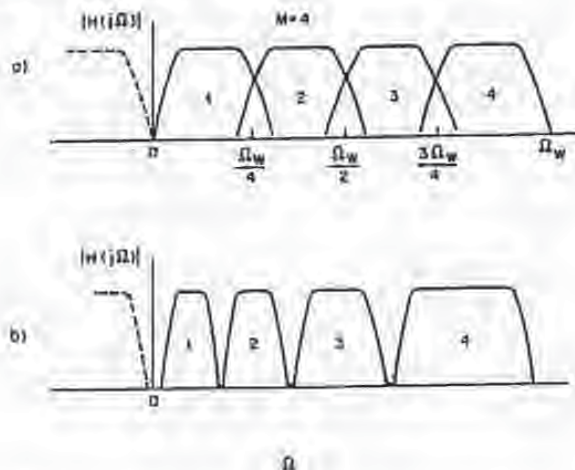
$$\Delta W_{k+1} > \Delta W_k ; k = 1, 2, \dots, M-1 \quad (11.2)$$

The design in (11.2) suggests that the lower frequencies in the speech signal are more carefully isolated or observed than the higher frequencies. This provides a qualitative match to the long-time speech psd [Figure 2.9(a)] and the articulation-index function (Appendix E), both of which are lowpass functions that decrease as frequency increases. The above match is, however, not very critical in the presence of variable bit allocation, which offers the possibility of digitizing sub-bands with varying fidelity (Section 11.3). Indeed, an important filter-bank design (the quadrature-mirror filter bank, Section 11.4) has the defining characteristic that the input psd is split into equal sub-bands.

Figure 11.3 sketches filter-bank amplitude responses that may be appropriate to realize the band-splitting operations shown in Figure 11.2. The observations to be made with Figure 11.3 will also hold for the digital filter banks of Section 11.3, with $H(j\Omega)$ and Ω_W replaced by $H(e^{j\omega})$ and π , respectively. An important distinction in Figure 11.3 is between (a) equal-width and (b) variable-width filters. Another distinction is between filter characteristics that overlap, as in (a), and characteristics that are non-contiguous, as in (b). The in-between situation of exactly contiguous filters is academic because practical implementations involve amplitude responses with finite roll-off characteristics.

The approach in Figure 11.3(b) calls for extremely fast filter roll-offs that minimize inter-band gaps, but it offers the possibility of reduced sampling rates

Figure 11.3 Amplitude responses in filter-banks consisting of four individual bandpass characteristics of (a) equal width and (b) unequal width.



(smaller values of f_{sk}), and hence a lower coding rate I [see (11.3)] for given values of R_k . Inter-band frequency gaps will be non-zero in practical filter designs, and these gaps cause a reverberant quality in the output speech of low bit rate SBC designs, unless the sub-bands can adaptively track regions of significant speech energy, such as formant frequencies in voiced speech [Crochiere and Sambur, 1977]. Discussions of SBC in this book are confined to fixed bands and fixed bit allocations. Sub-band coding systems with adaptive bit allocation perform significantly better because of the dynamic noise-shaping that they provide [Esteban and Galand, 1978] [Grauel, 1980] [Ramstad, 1982] [Heron, Crochiere and Cox, 1983]. However, the higher processing involved in adaptive bit allocation makes it particularly appropriate in the higher-complexity approach of TC (Chapter 12).

11.2 Transmission Rate I , SNR and Gain Over PCM

In SBC, each sub-band waveform $x_k(t)$ is sampled at a rate f_{sk} and encoded using R_k bits per sub-band sample. The transmission rate in SBC is therefore the sum of the bit rates needed to code individual sub-bands:

$$I = \sum_{k=1}^M f_{sk} R_k \quad \text{b/s} \quad (11.3)$$

In the special case of equal-width sub-bands,

$$\Delta W_k = W/M \quad \text{for all } k; \quad f_{sk} = 2\Delta W_k = 2W/M \quad (11.4a)$$

Since individual sub-band k can be sampled at the frequency $2\Delta W_k$ (Section 11.3), (11.3) simplifies to

$$I = \frac{2W}{M} \sum_{k=1}^M R_k \quad \text{b/s} \quad \text{for equal-width bands} \quad (11.4b)$$

Note that (11.4b) reduces to the familiar form $I = 2WR$ for full-band coding if the total number of bits is expressed in the form

$$\sum_{k=1}^M R_k = MR \quad (11.5)$$

where R denotes the average number of bits used to encode a full-band sample. The simple equalities in (11.4b) and (11.5) imply that I is proportional to the sum of R_k values. This makes the design of variable bit allocation much simpler than in the general case of unequal-width sub-bands where the relationship between total bit rate I and the individual R_k values is less direct [see (11.3)].

In the following analysis, we assume non-overlapping equal-width sub-bands, so that the variances σ_{sk}^2 of sub-band inputs can be simply added to obtain the variance σ_s^2 of the full-band input. Similarly, variances σ_{sk}^2 of sub-band

1.3)] for given
 d filter designs,
 w bit rate SBC
 nificant speech
 and Sambur,
 s and fixed bit
 ation perform
 they provide
 run, Crochiere
 : bit allocation
 roach of TC

CM

and encoded
 therefore the

(11.3)

(11.4a)

Section 11.3),

(11.4b)

nd coding if

(11.5)

and sample.
 l to the sum
 pler than in
 tween total

ib-bands, so
 obtain the
 T sub-band

reconstruction errors can be added to obtain the variance σ_r^2 of signal reconstruction error.

The final reconstruction error variance is

$$\sigma_{r,SBC}^2 = \sum_{k=1}^M \sigma_{rk}^2 \quad (11.6a)$$

We assume error-free transmission, and the use of PCM (or DPCM) coding of individual sub-bands. As a result, for any k , the sub-band reconstruction error variance is $\sigma_{rk}^2 = \epsilon_k^2 \sigma_{sk}^2$, a corresponding quantization error variance. Therefore,

$$\sigma_{r,SBC}^2 = \sum_{k=1}^M \epsilon_k^2 2^{-2R_k} \sigma_{sk}^2 \quad (11.6b)$$

The reconstruction error variance of a conventional (full-band) PCM coder, with bit rate equal to the average bit rate R in (11.5), is given by

$$\sigma_{r,PCM}^2 = \epsilon^2 2^{-2R} \sigma_s^2 \quad (11.6c)$$

where R is the number of bits/sample.

The SNR improvement G_{SBC} due to sub-band coding is the ratio of (11.6c) to (11.6b). Assuming for simplicity a constant quantizer performance factor ($\epsilon_k^2 = \epsilon^2$; all k), we obtain a gain over PCM that depends only on the bit allocation algorithm:

$$G_{SBC} = \frac{2^{-2R} \sigma_s^2}{\sum_{k=1}^M [2^{-2R_k} \sigma_{sk}^2]} = \frac{2^{-2\sum R_k/M} \sum_{k=1}^M \sigma_{sk}^2}{\sum_{k=1}^M [2^{-2R_k} \sigma_{sk}^2]} \quad (11.7a)$$

$$SNR |_{SBC}(\text{dB}) = SNR |_{PCM}(\text{dB}) + 10 \log G_{SBC} \quad (11.7b)$$

With a flat spectrum, G_{SBC} can never exceed 1 (Example 11.1). In the case of non-flat spectra, values of $G_{SBC} > 1$ can be realized by bit allocation procedures where R_k values are matched to σ_{sk}^2 values in a sense that will be clear from Examples 11.1 and 11.2. The special case of σ_{sk}^2 -independent and equal R_k simply leads to $G_{SBC} = 1$ in (11.7). In Chapter 12, we will fully develop a theory of optimum bit allocation.

The sub-band coding gain G_{SBC} is really analogous to the prediction gain G_P in that both of these gains result from the non-flatness of input spectrum. Sub-band coding gain increases as a function of number of bands M ; and prediction gain increases with order of prediction. As in prediction, the greatest values of G_{SBC} are realized when spectrum-dependent bit allocation is allowed to be time varying [Stjernvall, 1977] [Esteban and Galand, 1978] [Grauel, 1980] [Ramstad, 1982] [Heron, Crochiere and Cox, 1983]. This will indeed be the approach of Adaptive Transform Coding in Chapter 12.

Example 11.1. Two-band coding of a flat spectrum input

We shall again consider the simple case of equally wide sub-bands of width $W/2$ each. As a result of the flat spectrum,

$$\sigma_{x1}^2 = \sigma_{x2}^2 = \sigma_x^2/2 \quad (11.8a)$$

Using this in (11.7a),

$$G_{SBC} = 2 \frac{2^{-(R_1+R_2)}}{2^{-2R_1} + 2^{-2R_2}} \quad (11.8b)$$

Figure 11.4(a) plots G_{SBC} as a function of R_1 for the example of $R_1 + R_2 = 6$. The maximum value of $G_{SBC} = 1$ occurs for $R_1 = R_2 = 3$. This result can also be seen by identifying the above expression for G_{SBC} as the ratio of geometric mean and arithmetic mean of the terms 2^{-2R_1} and 2^{-2R_2} ; this ratio is maximum when the terms are equal, i.e., when $R_1 = R_2$. ■

Example 11.2. Two-band coding of the two-level spectrum of Figure 2.24 with $\alpha = 2/17$

From the results of Example 2.12,

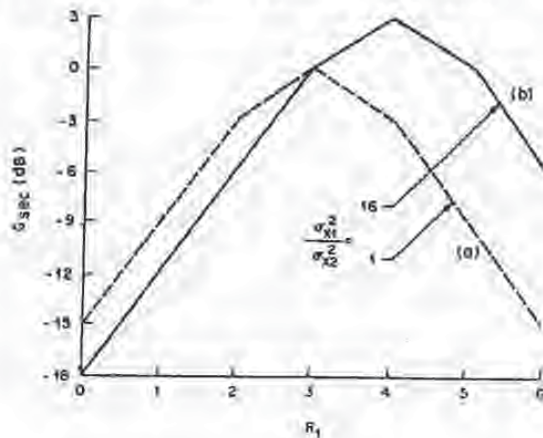
$$\sigma_{x1}^2 = (16/17) \sigma_x^2; \quad \sigma_{x2}^2 = (1/17) \sigma_x^2 \quad (11.9a)$$

Using this in (11.7a),

$$G_{SBC} = 17 \frac{2^{-(R_1+R_2)}}{16 \cdot 2^{-2R_1} + 1 \cdot 2^{-2R_2}} \quad (11.9b)$$

Figure 11.4(b) plots G_{SBC} as a function of R_1 for the example of $2R = R_1 + R_2 = 6$. As in Example 11.1, equal bit allocation ($R_1 = R_2 = 3$) results in $G_{SBC} = 1$. But unlike in the flat-spectrum case, the maximum value of G_{SBC} is now 17/8. This maximum occurs if

Figure 11.4 G_{SBC} versus R_1 in two-band SBC schemes with $R = 3$ bits/sample, for (a) a flat-spectrum input, and (b) an input with the two-level psd of Figure 2.24 (with $\alpha = 2/17$).



width $W/2$ each.

(11.8a)

(11.8b)

$R_1 = 6$. The
iso be seen by
and arithmetic
are equal, i.e.,

$\alpha = 2/17$

(11.9a)

(11.9b)

$L_1 = 6$. As in
unlike in the
am occurs if

flat-spectrum

$R_1 = 4$ and $R_2 = 2$. Note that with this design, the error contributions in both sub-bands (denominator terms in the above expression for G_{SBC}) are equal. In fact, this maximum gain is the inverse of the spectral flatness measure γ_x^2 for the input (Problem 2.23):

$$\gamma_x^2 = [\alpha(2-\alpha)]^M = \left[\frac{2}{17} \frac{32}{17} \right]^M = \frac{8}{17}$$

The equality of maximum gain and γ_x^{-2} will be discussed again in Chapter 12. What is significant for the present discussion is that a two-band SBC procedure is sufficient to utilize all the spectral redundancy of a two-level psd: in other words, sufficient to realize $G_{SBC} = \gamma_x^{-2}$. The exact realization of the maximum possible gain is due to one other property of the input spectrum in question: the ratio of component variances, 16, is an integral power of 2.

The sufficiency of the two-band partition for the two-level spectrum is similar to a result in Chapter 6 where linear prediction of order N was adequate to utilize the *sfm* of an AR(N) process. *

The constraint on $\sum R_k$ used in Examples 11.1 and 11.2 is more meaningful with equal-width sub-bands [where I is directly proportional to $\sum R_k$ (11.4b)] than with variable-width sub-bands [where I is a weighted sum of the R_k (11.3)]. For equal-width sub-bands, the results of Example 11.2 can be generalized to the case of $M > 2$. The gain G_{SBC} in (11.7a) can again be maximized under the constraint of a given number of bits [see (11.5)]. This is equivalent to minimizing

$$\sigma_r^2 = \epsilon^2 \sum_{k=1}^M 2^{-2R_k} \sigma_{xk}^2$$

Using Lagrange multipliers,

$$\frac{\partial}{\partial R_k} \left[\epsilon^2 \sum_{k=1}^M 2^{-2R_k} \sigma_{xk}^2 - \lambda \left(MR - \sum_{k=1}^M R_k \right) \right] = 0$$

from which we can express R_k as a function of λ :

$$R_k = \frac{1}{2} \log_2 \left(2\epsilon^2 \log_e 2 \right) + \frac{1}{2} \log_2 \frac{\sigma_{xk}^2}{\lambda}$$

Using this result in $MR = \sum R_k$, the optimum bit allocation is

$$R_{k,opt} = R + \frac{1}{2} \log_2 \frac{\sigma_{xk}^2}{\left[\prod_{l=1}^M \sigma_{xl}^2 \right]^{1/M}} \quad (11.10)$$

and from the expression for σ_r^2 above, the minimum mse [Goodman, 1967] is

$$\min (\sigma_r^2) = M \epsilon^2 2^{-2R} \left[\prod_{l=1}^M \sigma_{xl}^2 \right]^{1/M} \quad (11.11)$$

and the *maximum gain* is the ratio of arithmetic mean and geometric mean of the sub-band variances $\sigma_{s_i}^2$:

$$\max \{G_{SBC}\} = \frac{\sigma_s^2}{M \left[\prod_{i=1}^M \sigma_{s_i}^2 \right]^{1/M}} = \frac{\frac{1}{M} \sum_{i=1}^M \sigma_{s_i}^2}{\left[\prod_{i=1}^M \sigma_{s_i}^2 \right]^{1/M}} \quad (11.12)$$

The bit allocation in (11.10), which minimizes the mse σ_s^2 , will also imply equal values of noise variance for different k , as a result of (11.6b) and (11.10); this is also shown formally in the analysis of Chapter 12. We will also see in Chapter 12 that specific forms of noise-shaping can be realized by bit allocations that minimize certain types of frequency-weighted mean square error.

In coding a signal such as speech whose psd can be approximated as an M -level psd with $M \gg 2$ (a generalization of Figure 2.24), SBC performance increases with increasing M . Very large values of M can also take into account the fine structure in the psd due to the pitch period, in the sense of maintaining a locally flat psd within each sub-band. The use of fairly small values such as $M = 4$ is therefore for simplicity, rather than because of a saturation of objective gain G_{SBC} as a function of M . In particular, 4-band SBC coding of speech is significantly better than 2-band SBC coding, both objectively and from a subjective quality viewpoint [Cox, 1981, 11]. Improvement of performance with M is maintained at values as high as $M = 16$ [Ramstad, 1982] [Esteban and Galand, 1982].

11.3 The Integer-Band Filter Bank

An important feature in Figure 11.1 is that bandpass filter cutoffs are chosen such that each band can be sampled at twice the corresponding bandwidth

$$f_{2k} = 2\Delta W_k; \quad k = 1, 2, \dots, M \quad (11.13)$$

rather than at twice the highest frequency of the full-band signal. As discussed in Chapter 3, this is possible in the special situation of *integer-band sampling* [Crochiere and Rabiner, 1983] where the lower cutoff frequency W_{1k} in a sub-band k is an integral multiple of bandwidth (Figure 3.10):

$$W_{1k} = n \Delta W_k; \quad n = 0, 1, 2, \dots; \quad k = 1, 2, 3, \dots, M \quad (11.14)$$

The orders of bandpass filtering and sampling in Figure 11.1 can be reversed. Consider that discrete-time inputs $x(n)$ are available, sampled at the full-band Nyquist rate $f_s = 2W$ where $W = \sum \Delta W_k$, with summation from $k = 1$ to M , is the maximum frequency of the full-band signal.

Let the sub-band width be written in the form

$$\begin{aligned} \Delta W_k &= W/\zeta_k; \quad k = 1, 2, \dots, M \\ \zeta_k &= M \text{ for all } k \text{ with equal-width sub-bands} \end{aligned} \quad (11.15)$$

tric mean of the

$$(11.12)$$

also imply equal (11.10); this is as in Chapter 12 as that minimize

as an M -level variance increases account the fine graining a locally as $M = 4$ is tive gain G_{SBC} is significantly tective quality maintained at 82].

offs are chosen width

$$(11.13)$$

is discussed in and sampling in a sub-band

$$(11.14)$$

it be reversed. the full-band = 1 to M , is

$$(11.15)$$

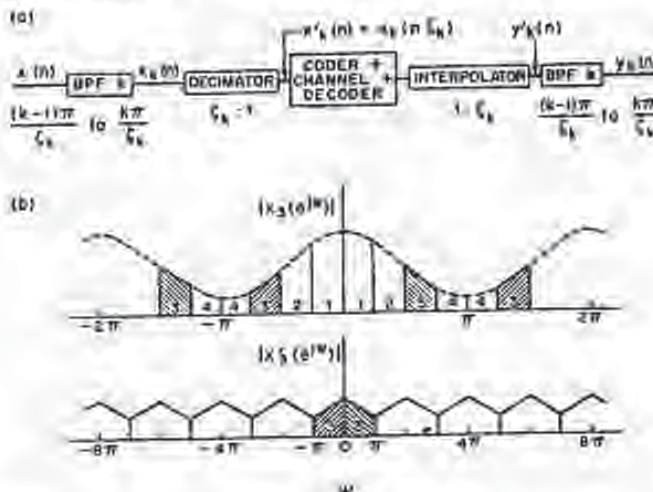
With the sub-band partition of Figures 11.2(a) and 11.3(a), $\zeta_k = 4$ for all k . Some of the speech coding examples mentioned later in this chapter use unequal sub-bands. In these examples, the values of ζ_k range from 4 to 30 (Tables 11.1, 11.2 and 11.3).

Figure 11.5 shows the sequence of filtering and coding operations in SBC, using the general example of sub-band k in Figure 11.5(a) and the special case of $k = 3$ and $\zeta_3 = 4$ in Figure 11.5(b).

The $\zeta_k:1$ decimator sub-samples the bandpass output $x_k(n)$ by a factor ζ_k , implying a sampling rate of $f_{sk} = 2W/\zeta_k = 2\Delta W_k$ for sub-band k . This decimation implies a repetition rate of its spectrum that is higher than that of the full-band spectrum by a factor ζ_k . As a result of this, the x -axes in the two figures of (b) differ by a factor $\zeta_k = 4$. One of the repetitions of the spectrum will be in the baseband, so that the decimation effectively translates the lower frequency edge of the bandpass signal band to zero frequency. The $1:\zeta_k$ interpolator fills in $(\zeta_k - 1)$ zeros in between every pair of incoming lowpass samples. The k th harmonic of the interpolated baseband is thus effectively bandpass-translated to the appropriate initial bandpass region. The explicit modulation processes mentioned in Section 11.1 are therefore replaced by simpler discrete-time processes of decimation and interpolation. It is assumed that the interpolation process includes an amplitude scaling factor of ζ_k . This maintains the original value of input variance in spite of the zero-valued amplitudes that are introduced in the interpolation process.

The amplitude spectra $|X_3(e^{j\omega})|$ and $|X'_3(e^{j\omega})|$ in Figure 11.5(b) refer to sub-band $k = 3$, with $\zeta_3 = 4$; the illustration is equivalent to the continuous-time case

Figure 11.5 Realization of integer-band sampling with a discrete-time input; (a) block diagram of SBC coding for sub-band k ; and (b) original spectrum and resampled spectrum after decimation, for sub-band $k = 3$, with $\zeta_3 = 4$. The baseband spectrum resulting from the decimation is shifted back to the original frequency range of sub-band k after interpolation by a factor ζ_k .



11.3 The Integer-Band Filter Bank

of Figure 3.9, which also used the example of $k = 3$. Note that the spectrum of the decimated sequence has its own frequency scaling. If the procedure of the last two paragraphs is repeated for an even-numbered sub-band ($k = 2$ or $k = 4$), it can be shown that the spectrum gets inverted in the process of lowpass translation to the baseband. This is, however, neutralized by a subsequent inversion in the interpolation process for even k [Crochiere and Rabiner, 1983].

The integer-band constraint in (11.14) is invariably assumed in SBC for the obvious reason of minimizing sub-band sampling frequencies and hence the overall information rate

$$I = \sum_{k=1}^M I_k = \sum_{k=1}^M f_{sk} R_k = \sum_{k=1}^M 2\Delta W_k R_k \text{ bits/second} \quad (11.16)$$

11.4 Quadrature-Mirror Filter Banks

The overlapping sub-band situation in Figure 11.3(a) suggests that aliasing effects can occur if sub-bands are sampled at $f_{sk} = 2W/M = \Omega_M/\pi M$. This problem is very elegantly tackled in the *quadrature-mirror filter bank* (QMF) approach of Figure 11.6 [Esteban and Galand, 1977]. This figure shows the division of a full-band signal of maximum radian frequency π into two of equal width by using a constrained pair of lowpass and highpass filters. In the notation of (11.15), $f_1 = f_2 = M = 2$. By repeated subdivisions of resulting sub-bands using QMF filter banks, one can realize an SBC filter bank with M given by a power of 2, such as $M = 4$ as in Figure 11.3(a). Values of M that are not powers of 2 can also be realized by simply ignoring appropriate sub-band branches in the QMF tree (Table 11.3 and Problem 11.2).

The rest of the following discussion refers to the first stage of such a filter bank, involving two sub-bands as in Figure 11.6. When further stages of band-partitioning are introduced, each of the branches in Figure 11.6(a) will be split into further branches, and sampling frequencies will be reduced by factors of two at each stage; but the results of Figure 11.6(b) will apply repeatedly with appropriate redefinitions of the absolute frequencies represented by 0, π and $\pi/2$ in that figure.

Each of the sub-band signals $x_l(n)$ and $x_u(n)$ is resampled by a factor 2:1. This reduction of the sub-band sampling rates is necessary in order to maintain a minimal overall bit rate in encoding these signals. This reduction of sampling rate introduces aliasing terms in each of the sub-band signals because of the finite rate of roll-off in filter responses. For example, in the lower band the signal energy in the frequency range above $\pi/2$ is folded down into the range 0 to $\pi/2$ and appears as *aliasing distortion* in this signal, in the frequency range covered by the hatched region in the left half of Figure 11.6(b). In the above explanation, and in the rest of this section, π is *not* redefined as in Figure 11.5(b). Aliasing also occurs for the upper band in a similar fashion; any signal energy in the frequency range below $\pi/2$ is folded upward into its Nyquist band $\pi/2$ to π ; this causes aliasing in the frequency range covered by the hatched area in the right half of Figure 11.6(b). This mutual aliasing of signal energy between the upper and lower sub-bands is

trum of
the last
= 4), it
instation
n in the

for the
overall

(11.16)

Using
This
(MFD)
as the
equal
ation
using
wer of
2 can
F tree

bank,
band-
into
wo at
riate
ore.

2:1,
ain a
rate
rate
ty in
ears
shed
rest
the
 $\pi/2$
the
(b),
is

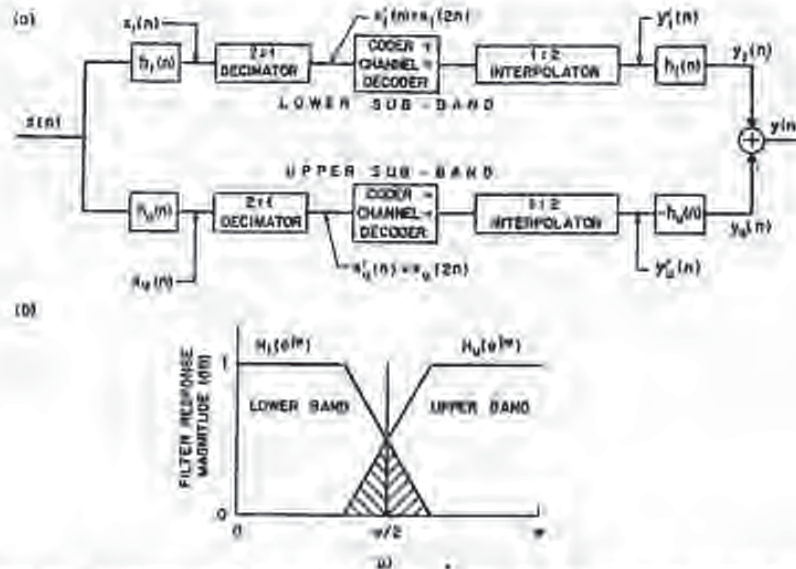


Figure 11.6 Quadrature-mirror filtering for splitting an input into two equal-width sub-bands: (a) implementation; and (b) qualitative illustration of a filter-bank response that provides alias-image cancellation [Eteiba and Galand, 1978] [Crocchiere, 1981].

sometimes called *interband leakage*. The amount of leakage that occurs between sub-bands is directly dependent on the degree to which the filters $h_l(n)$ and $h_u(n)$ approximate ideal lowpass and highpass filters, respectively.

In the reconstruction process, the sub-band sampling rates are increased by a factor 1:2 by filling in zero-valued samples between each pair of sub-band samples. This introduces a periodic repetition of the signal spectra in the sub-band. For example, in the lower band the signal energy from 0 to $\pi/2$ is symmetrically folded around the frequency $\pi/2$ into the range of the upper band. This unwanted signal energy, referred to as an *image* is mostly filtered out by the lowpass filter $h_l(n)$ in the receiver. This filtering operation effectively interpolates the zero-valued samples that have been inserted between the sub-band signals to values that appropriately represent the desired waveform [Crocchiere and Rabiner, 1983]. Similarly, in the upper sub-band signal an image is reflected to the lower sub-band and filtered out by the filter $-h_u(n)$.

The degree to which the above images are removed by the filters $h_l(n)$ and $-h_u(n)$ is determined by the degree to which they approximate ideal lowpass and highpass filters. Because of the special relationship of the sub-band signals in the QMF filter bank, the remaining components of the images can be canceled by aliasing terms introduced in the analysis. This cancellation occurs *after* the addition of the two interpolated sub-band signals $y_l(n)$ and $y_u(n)$, and the cancellation is exact in the absence of coding errors. In the presence of coding, this cancellation is obtained to the level of quantization noise.

If S_l and S_u refer to lower-band and upper-band signals and subscripts A and I denote aliasing and imaging, the adder input $y_l(n)$ in Figure 11.6(a) will consist of the following main components, correct to filter attenuation effects: S_l and S_{uA} in the lower band and S_{lI} and S_{uIA} in the upper band. Similarly, input $y_u(n)$ will consist of components S_{uI} and S_{lIA} in the lower band and S_u and S_{lA} in the upper band. When $y_l(n)$ and $y_u(n)$ are added, components S_{uA} and S_{uI} cancel in the lower band, while components S_{lI} and S_{lIA} cancel in the upper band, leaving S_l and S_{lA} in the lower band and S_u and S_{uA} in the higher band. The components of S_{lIA} and S_{lIA} actually belong in the respective bands, and in the case of a QMF design with an allpass characteristic, these components exactly compensate for the in-band attenuations present in S_l and S_u .

One way of obtaining this cancellation property in the QMF filter bank is to use filters $h_l(n)$ and $h_u(n)$, which are respectively symmetrical and anti-symmetrical finite impulse response (FIR) designs with even numbers of taps, i.e.,

$$h_l(n) = h_u(n) = 0 \quad \text{for } 0 > n \geq N; \quad (11.17)$$

$$h_l(n) = h_l(N-1-n), \quad n = 0, 1, \dots, N/2-1; \quad (11.18a)$$

$$h_u(n) = -h_u(N-1-n), \quad n = 0, 1, \dots, N/2-1 \quad (11.18b)$$

The cancellation of aliasing effects in the QMF filter bank further requires that the filters in Figure 11.6(a) satisfy the condition [Esteban and Galand, 1977] [Crochiere and Rabiner, 1983]

$$h_u(n) = (-1)^n h_l(n), \quad n = 0, 1, \dots, N-1 \quad (11.19)$$

which is a *mirror image* relationship of the filters, implying symmetry about $\pi/2$, as in Figure 11.6(b). The coefficients of the filters are identical except that their signs alternate. Therefore, both filters can be realized using a single N -tap filter as the starting point.

Further, if the filter-bank output $y(n)$ is desired to be a delayed replica of input $x(n)$ (in the absence of coding errors), the filters $h_l(n)$ and $h_u(n)$ must also satisfy the condition

$$|H_l(e^{j\omega})|^2 + |H_u(e^{j\omega})|^2 = 1, \quad (11.20)$$

where $H_l(e^{j\omega})$ and $H_u(e^{j\omega})$ are the Fourier transforms of $h_l(n)$ and $h_u(n)$, respectively; this is simply the condition for an *allpass* characteristic. If the allpass condition (11.20) is included in the mirror-image design (11.19), the point of intersection of the two filter functions in Figure 11.6(b) will be the -3 dB point for each transfer function.

The filter requirement in (11.20) cannot be met exactly by the mirror image filters of (11.19) except when $N = 2$ and when N approaches infinity. However, it can be very closely approximated for modest values of N . Filter designs which satisfy (11.18) and (11.19) and approximate the condition of (11.20) can be obtained with the aid of an optimization program [Johnston, 1980]. Resulting filter



subscripts A and J (a) will consist of S_i and $S_{i,A}$ in input $y_n(n)$ will $S_{i,A}$ in the upper $S_{i,A}$ cancel in the d , leaving S_i and its components of case of a QMF compensate for the

er bank is to use anti-symmetrical S_i .

$$(11.17)$$

$$(11.18a)$$

$$(11.18b)$$

quires that the Galand, 1977)

$$(11.19)$$

y about $\pi/2$, as that their signs ap filter as the

replica of input ust also satisfy

$$(11.20)$$

) and $h_n(n)$. If the allpass the point of 1 dB point for

mirror image

However, it designs which (1.20) can be resulting filter

nd Coolig 11

Table 11.1 Quadrature Mirror Filters of order $N = 32$ and $N = 16$. Listed numbers are values of coefficients $h_i(n)$ for $N/2 \leq n \leq N$. Values of other coefficients follow (11.9) and (11.9') [Johnson, 1980]. [Crochiere and Rabiner, 1983; Reprinted with permission].

| $h(16)$ to $h(32)$ | $N = 32$ | | $h(8)$ to $h(15)$ |
|--------------------|--------------------|--|-------------------|
| | $h(24)$ to $h(31)$ | | |
| 4.6643830E-01 | 1.7881910E-02 | | .47211220E 00 |
| 1.2846510E-01 | -1.7219030E-04 | | .11780660E 00 |
| -9.9800110E-02 | -9.4636330E-03 | | -.99295500E-01 |
| -1.9244910E-02 | 1.4272050E-03 | | -.26273600E-01 |
| 5.2909300E-02 | 4.1581240E-03 | | .46476840E-01 |
| 1.4468810E-02 | -1.2601150E-03 | | .19911500E-02 |
| -3.1155320E-02 | -1.3508480E-03 | | -.20487510E-01 |
| -4.1094160E-03 | 6.5064660E-04 | | .65256660E-03 |

coefficients for N values in the range 8 to 64 have been tabulated [Crochiere, 1981] [Crochiere and Rabiner, 1983].

Table 11.1 lists representative designs for $N = 32$ and $N = 16$. In a QMF tree for $M = 4$ sub-bands, the first subdivision may use filters of order $N = 32$. In view of the 2:1 decimation, a matching design for the second stage of the QMF tree would then be $N = 16$.

Figure 11.7 shows the frequency response characteristics for a 32-tap filter design [Crochiere, 1981]. Figure 11.7(a) shows the magnitude of $H_i(e^{j\omega})$ and $H_o(e^{j\omega})$ expressed in dB as a function of ω . As in the schematic of Figure 11.6(b), note that the roll-off regions of the two responses intersect at the -3 dB point for each characteristic. Figure 11.7(b) shows the magnitude of the expression $|H_i(e^{j\omega})|^2 + |H_o(e^{j\omega})|^2$ expressed in dB as a function of ω . As can be seen from Figure 11.7(b), the requirement of (11.20) is satisfied to within ± 0.025 dB, which is more than satisfactory for good SBC performance. The reconstruction error in the 32-tap design of Table 11.1 is also ± 0.025 dB, but the stop-band attenuation of this filter (measured at the first stop-band peak) is 52 dB, which is much greater than the 37 dB attenuation in the example of Figure 11.7(a). In the 16-tap example of Table 11.1, the reconstruction error is ± 0.07 dB, and the stop-band attenuation is 30 dB.

The use of FIR filters has the advantage of linear-phase characteristics which eliminate the problems of group delay distortions. This feature also allows the 2-band design of Figure 11.6 to be conveniently cascaded in three structures (Example 11.5, Problem 11.2) without the need for phase compensation. However, effective FIR designs imply significant coding delays. For example, with the 32-tap design just mentioned, the coding and decoding delays due to the first level of the QMF tree are 4 ms each, assuming 8 kHz input sampling; and subsequent levels of the QMF partition introduce corresponding additional delays. In order to implement SBC systems with smaller values of delay, there has been at least one proposal for a QMF bank based on *infinite impulse response* (IIR) designs [Ramstad and Foss, 1980]. This proposal includes special procedures for mitigating the group delay distortions inherent in IIR designs.

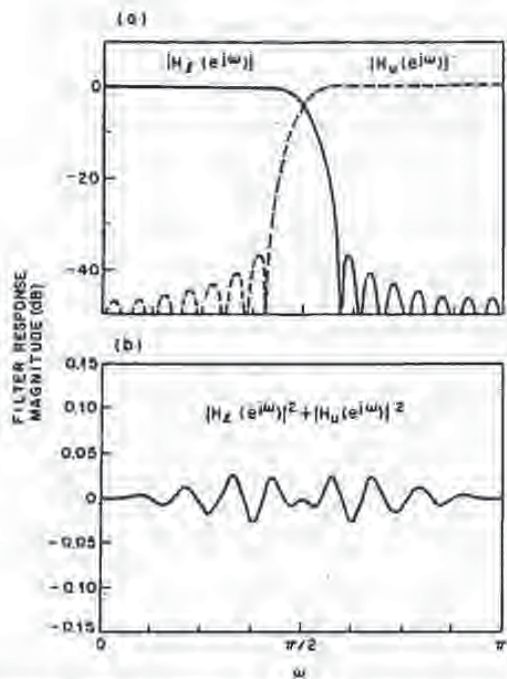


Figure 11.7 Illustration of amplitude-frequency responses in a quadrature mirror filter bank using FIR filters: (a) lowpass and highpass characteristics of individual 32-tap FIR filters; and (b) approximately allpass characteristic of the combination [Crochiere, 1981].

11.5 Sub-Band Coding of Speech

The following examples illustrate the design of fixed bit-allocation SBC systems for speech at bit rates in the range of 9.6 kb/s to 32 kb/s. The 32 kb/s system with fixed bit allocation can provide very high subjective quality, with MOS scores in the order of 4.2, a necessary condition for *toll quality* reproduction of telephone speech, while fixed bit-allocation SBC systems at lower bit rates provide different grades of *communications quality* encoding. Example 11.5 also illustrates the use of the QMF systems discussed in Section 11.4.

Example 11.3. Sub-band coding of speech at 9.6 kb/s

Table 11.2 shows a sub-band partition for a 9.6 kb/s SBC system. The sub-band sampling rates are obtained from an original sampling rate of 9.6 kHz by using $\xi_k:1$ decimations, with ξ_k values of 20, 10, 9 and 5.

The PCM coders use adaptive quantization (for example, the Δ QB system with a one-word memory, Chapter 4); and ranges of step size are individually matched to the long-time-averaged variances of individual sub-band signals. This is indicated by the different Δ_{min} values in Table 11.2. Respective Δ_{max} values are typically 256 times greater.

Table 11.2 Sub-band coder designs for 9.6 kb/s [Crochiere, 1977]

| Band | Ω_s Decimation Factor from 9.6 kHz | Band Edges (Hz) | Sub-band Sampling Rates (Hz) | Relative Δ_{opt} Values (dB) | R_k (bits/sample) | I_k (kb/s) |
|---------------------------|--|-----------------------|---------------------------------------|--|------------------------|-----------------|
| 1 | 20 | 240-480 | 480 | 0.0 | 3 | 1.44 |
| 2 | 10 | 480-960 | 960 | -3.0 | 3 | 2.88 |
| 3 | 9 | 1067-1600 | 1067 | -8.5 | 2 | 2.13 |
| 4 | 5 | 1920-2880 | 1920 | -14.0 | 1.5 | 2.88 |
| Sync | | | | | | 0.27 |
| Total Bit Rate I (kb/s) | | | | | | 9.60 |
| Typical SNR (dB) | | | | | | 10.8 |

The bit allocation of (3, 3, 2, 1.5) bits/sample is a perceptually optimized design; it codes lower frequency sub-bands with greater fidelity than the higher frequency sub-bands. The fractional value of $R_k = 1.5$ bits/sample can be obtained in several ways [Crochiere, 1977]; for example, by the use of $R_k = 1.0$ and $R_k = 2.0$ for alternate samples, with appropriate modification of step size logic.

Notice that in Table 11.2, the transmission rate for each band is a rational fraction of total rate I so that sub-band data can be multiplexed into a repetitive framed sequence. The lowest common denominator of these rational fractions, including the fraction of transmission rate reserved for frame synchronization purposes (denoted by "Sync" in Table 11.2) determines the smallest possible frame size for the SBC transmission system [Crochiere, 1977]. In certain applications such as voice storage and computer voice response, synchronization procedures may be built-in, and there may not be any need for transmitting special "Sync" bits. This is indeed the situation assumed in Table 11.4.

The quality of the time-invariant 9.6 kb/s system is limited by a reverberant quality in the output $y(n)$ due to inter-band gaps. Designs without gaps involve smaller values of R_k , greater quantization noise, and even lower quality. On the other hand, 9.6 kb/s SBC systems, as a class, perform much better than full-band fixed-prediction speech coders at 9.6 kb/s; in particular, better than 9.6 kb/s ADM systems. In subjective tests, the 9.6 kb/s SBC system is judged to be equivalent to an ADM system at twice the coding rate, i.e., 19.2 kb/s [Crochiere, 1977]. This advantage is directly related to variable bit allocation, and the fact that the quantization noise in the coding of sub-band k with R_k bits/sample is contained within that band. *

Example 11.4. SBC coding of speech at 16 kb/s

Table 11.3 refers to a 16 kb/s SBC system. The explanation of the numbers in this table is very similar to that for Table 11.2. In perceptual tests, this coder is comparable to 24 kb/s DPCM-AQB. The quality of 16 kb/s SBC with fixed bit allocation is useful for many communications applications, although this SBC output is clearly distinguishable from the original input in side-by-side comparisons.

A comparison of the Δ_{opt} values in Tables 11.2 and 11.3 shows that the design of Table 11.3 is a better match to the long-time-averaged psd of speech. Note that in Figure 2.9(a), the psd peaks at a value of frequency that is non-zero, and so does the Δ_k versus k profile in Table 11.3. The behavior with respect to frequency k is monotonic in Table 11.2. *

Table 11.3 Sub-band coder design for 16 kb/s [Crochiere, 1977]

| Band | Ω_k Decimation Factor from 10.67 kHz | Band Edges (Hz) | Sub-band Sampling Rates (Hz) | Relative Δ_{noise} Values (dB) | R_k (bits/sample) | f_k (kb/s) |
|---------------------------|--|-----------------------|---------------------------------------|--|------------------------|-----------------|
| 1 | 30 | 178-356 | 356 | -2.0 | 4 | 1.42 |
| 2 | 18 | 296-593 | 593 | 0.0 | 4 | 2.27 |
| 3 | 10 | 533-1067 | 1067 | -6.0 | 3 | 3.20 |
| 4 | 5 | 1067-2133 | 2133 | -11.5 | 2 | 4.27 |
| 5 | 3 | 2133-3200 | 2133 | -18.0 | 2 | 4.27 |
| Sync | | | | | | 0.47 |
| Total Bit Rate f (kb/s) | | | | | | 16.00 |
| Typical SNR (dB) | | | | | | 13.6 |

Example 11.5. SBC coding of speech at 16, 24 or 32 kb/s

Table 11.4 shows a general sub-band partitioning framework that can be used for SBC coding at bit rates of 16, 24 or 32 kb/s. The sub-band partitioning is obtained by repeated use of the QMF partitioning principle (Problem 11.2). Note that the 16 and 24 kb/s systems use four sub-bands while the 32 kb/s system uses five sub-bands. The speech bandwidth allowed in this five-band system includes the 3 to 4 kHz range; this is a capability in excess of the 3.2 kHz limit assumed for telephone speech.

Figure 11.8 shows sub-band signals $x_k(n)$; $k = 1, 2, 3, 4$ in a 4-band system which uses the four lower bands of Table 11.4. As shown in the table, respective sampling rates are $f_{sk} = 1000, 1000, 2000$ and 2000 Hz. These sampling rates are obtained from an original sampling rate of $f_s = 8000$ Hz by using $\Omega_k:1$ decimations. Respective values of Ω_k , also listed in the table, are 8, 8, 4 and 4. Note that as we move the lowest sub-band (0-500 Hz) to the highest (2000-3000 Hz), the left half of the waveform becomes increasingly more prominent. This is because of the preponderance of high frequency energy in the left half of the original full-band waveform. Notice also that the waveforms in the lower two sub-bands do not look very different. This is because the original full-band waveform in this example has significant energies centered at about 700 Hz, and this is a strong common component in both of the lower two sub-bands, which happen to overlap significantly in the 700 Hz region.

Table 11.4 Sub-band coder designs for 16, 24 or 32 kb/s [Crochiere, 1981].

| Band | Ω_k Decimation Factor from 8 kHz | Band Edges (Hz) | Sub-band Sampling Rates (Hz) | R_k (bits/sample) for f (kb/s) = | | |
|------|--|-----------------------|---------------------------------------|---|----|----|
| | | | | 16 | 24 | 32 |
| 1 | 8 | 0-500 | 1000 | 4 | 5 | 5 |
| 2 | 8 | 500-1000 | 1000 | 4 | 5 | 5 |
| 3 | 4 | 1000-2000 | 2000 | 2 | 4 | 4 |
| 4 | 4 | 2000-3000 | 2000 | 2 | 3 | 4 |
| 5 | 4 | 3000-4000 | 2000 | 0 | 0 | 3 |

Figure 11.8 shows sub-band signals $x_k(n)$; $k = 1, 2, 3, 4$ in a 4-band system which uses the four lower bands of Table 11.4.

The duration of the sampled band signals is much longer than the original speech signal. This is because the original full-band waveform in this example has significant energies centered at about 700 Hz, and this is a strong common component in both of the lower two sub-bands, which happen to overlap significantly in the 700 Hz region.

The long-term average power spectrum of the original speech signal is shown in Figure 11.4. The power spectrum of the original speech signal is shown in Figure 11.4. The power spectrum of the original speech signal is shown in Figure 11.4.

With the sub-band coding technique, the original speech signal is decomposed into sub-bands. The sub-bands are then coded and transmitted. The original speech signal is reconstructed by combining the sub-bands.



| I_k (kb/s) |
|-----------------|
| 1.42 |
| 2.37 |
| 3.20 |
| 4.27 |
| 4.27 |
| 0.47 |
| 16.00 |
| 13.6 |

sd for SBC
 ay repeated
 id. 24 kb/s
 The speech
 ; this is a

which uses
 g rates are
 an original
 of f_s , also
 (0-500 Hz)
 singly more
 left half of
) sub-bands
 is example
 mponent in
 Hz region.

11.

| ample) |
|--------|
| 32 |
| 5 |
| 5 |
| 4 |
| 4 |
| 3 |

oding 11

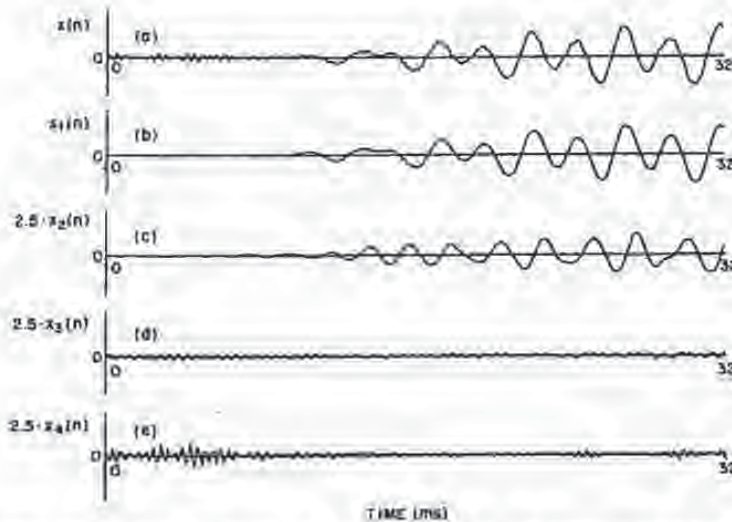


Figure 11.8 (a) Full-band speech waveform of duration 32 ms; and (b)(c)(d)(e) sub-band signals $x_k(n)$ for $k = 1, 2, 3, 4$ in the SBC system of Table 11.4. The sub-band signals $x_2(n)$, $x_3(n)$ and $x_4(n)$ have been magnified by a factor of 2.5 (Cox, 1983).

The full-band signal corresponding to $x_a(k)$ waveforms is a voiced speech segment of duration 32 ms. At the respective Nyquist sampling rates f_{sk} , the sub-band signals exhibit much lower values of adjacent-sample correlation than a full-band speech waveform sampled at its Nyquist rate f_s . The entire waveform $x_1(n)$ in Figure 11.8(b), for example, is sampled only 32 times because of the decimation to 1 kHz. The lower correlations in sub-band signals can also be conjectured from Figure 11.2 where individual sub-bands are seen to have flatter psd's than the full-band speech. (Also, see Problem 11.7). This is the reason why PCM, rather than DPCM, is often assumed in SBC systems, although, with real speech spectra, non-negligible values of prediction gain can be realized even in the case of (individually optimized) fixed predictors of order one.

The nature of the long-time-averaged speech spectrum [Figure 2.9(a)] suggests that the long-term sub-band spectrum can be high-pass in the ranges of sub-bands 1 and 2 of Table 11.4. High-pass spectra in sub-bands can also result from high-frequency pre-emphasis in telephone systems. In fact, in an implementation of the coders of Table 11.4 with telephone speech that includes high-frequency pre-emphasis, the sub-band coders use DPCM-AQB with fixed first-order predictors that reflect highpass spectra in four out of five sub-bands. Recommended values of coefficient h_1 , for pre-emphasized speech, are -0.71 , -0.28 , -0.31 , 0.26 and -0.64 in sub-bands 1 through 5, respectively [Daumer, 1982].

With fixed bit allocation, high quality coding with SBC requires a total bit rate in the order of 32 kb/s. In formal subjective testing, the SBC system of Table 11.4 obtains MOS scores (on a scale of 1 to 5), of 4.3, 3.9 and 3.1 at bit rates of 32, 24 and 16 kb/s [Daumer, 1982]. If the bit rate is at least 24 kb/s, there is an

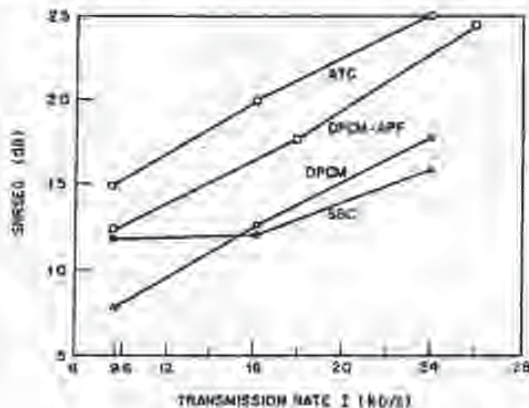
adequate margin of safety for accommodating tandem encodings of 2 to 3 SBC stages with useful final quality.

Although the results of Tables 11.2 to 11.4 refer to specific speech coding systems, they provide general design features that apply to other coding applications as well. An important example is in 9.6 kb/s SBC-TDHS (*time-domain harmonic scaling*) coding systems involving time-compression of input speech by a factor 2:1 prior to sub-band coding at a bit rate slightly under $2(9.6) = 19.2$ kb/s [Malah, 1979] [Malah, Crochiere and Cox, 1981] [Crochiere, Cox and Johnston, 1982]. This procedure can result in an improvement over direct SBC at 9.6 kb/s, but the improvement is obtained at the cost of additional complexity, needed for pitch computations that TDHS is based on. Another example of SBC application is the coding of FM-grade audio signals ($W = 20$ kHz) (Problem 11.3) and AM-grade audio signals ($W = 7$ kHz). For example, a two-band SBC system with the band partition [0-3500 Hz] [3500 Hz-7000 Hz] is a good digitizer for 7 kHz material at a coding rate of 56 kb/s [Johnston and Crochiere, 1979].

Comparison of DPCM, DPCM-AP, SBC and ATC. Figure 11.9 shows the performance of four speech coders as a function of bit rate I . The set of coders includes two time-domain coders (DPCM coders with and without adaptive prediction (prediction order equal to one and eight, respectively) and two frequency-domain coders, SBC and ATC (Chapter 12).

One significant comparison in the figure is between the *medium complexity* techniques, SBC (with fixed bit allocation) and DPCM (with fixed prediction). The DPCM coder degrades rapidly if $I < 16$ kb/s ($R < 2$ bits/sample) because of poor quantization performance, compounded by the effects of quantization error feedback. The other significant comparison is between the *high complexity* techniques, DPCM-AP (APC) and ATC. In this specific study, neither of the two techniques incorporated pitch structure. It is interesting that ATC has a consistent

Figure 11.9 Segmental SNR in time-domain and frequency-domain speech coders as a function of bit rate I [Triboles et al., ©1979, AT&T].



3 SBC

coding
time-
of input
(9.6) =
Cox and
SBC at
plexity,
of SBC
m (1.3)
system
or for 7

ows the
if coders
adaptive
and two

plexity
diction).
cause of
on error
plexity
the two
onsistent

sion of bit

2 to 3 dB advantage. In another study, involving a subjective comparison of APC and ATC, both using pitch information, APC was in fact rated slightly better [Daumer, 1982]. Part of the reason for the very good performance of that APC system was a carefully designed algorithm for noise shaping.

The comparisons between DPCM and DPCM-APF, and between SBC and ATC, are less interesting in that the inferences are well expected in each case. The ATC system can be regarded crudely as the equivalent of an SBC system with two very significant refinements: (a) a much larger number of sub-bands M , and (b) adaptive bit-allocation $|R_k|$ that is matched to short-term rather than long-term-averaged speech spectrum. As a consequence of these refinements, ATC systems utilize the spectral non-flatness in speech more completely and adaptively, in a fashion similar to redundancy-removal in a full-fledged APC system with higher-order spectrum prediction. The nonadaptive SBC system utilizes spectral non-flatness only in a non-adaptive, and hence incomplete sense. A special, but academic, input for which SBC provides complete redundancy removal is one with a staircase-type psd, as in Figure 2.24. For that two-level psd example, SBC with $M = 2$ provides a complete utilization of spectral non-flatness (Example 11.3 and Problem 11.6).

Combinations of sub-band coding and adaptive prediction. The performance of sub-band coding can be significantly improved by supplementing it with the time-domain operation of adaptive prediction [Atal and Remde, 1981] [Honda, Kitawaki and Itakura, 1982]. The general philosophy of these hybrid techniques is to split the burden of redundancy removal between the frequency domain and the time domain. The hybrid approach also provides the possibility of noise shaping in both the frequency domain and the time domain. In one system, the latter is provided by dividing basic time blocks of duration in the order of one pitch period into sub-blocks, typically four in number, and allocating quantization bits on the basis of prediction error energy in each sub-interval. This is done separately for each of typically three to four sub-bands. The bit allocation in the time domain provides better encoding of the higher-valued prediction error samples during the onset of a pitch period and mitigates the problem of quantization error feedback, separately in each sub-band. With spectrum prediction of order four and pitch prediction, the sub-band coder with time-frequency bit allocation provides MOS quality scores in the order of 3.5 at 16 kb/s and 4.0 at 24 kb/s [Honda, Kitawaki and Itakura, 1982].

11.6 Transmission Error Effects

Bit errors in an individual sub-band will generate error contributions at the receiver output within that frequency band. Since the channel error contributions in different sub-bands are expected to be uncorrelated, the corresponding error variances will simply add. The results of Section 11.2 and Section 4.9 can therefore be used to derive an expression for channel error variance σ_e^2 in an SBC system. Also, explicit forms of error-protection can be used to mitigate channel

error effects in SBC decoding. Error-protection systems can exploit not only the different sensitivities of various bits in transmitted codewords (as in Section 4.9), but also the different sensitivities of various sub-bands to transmission error effects. These points will be made more quantitative during the discussion of Transform Coding in Chapter 12.

Example 11.6. Transmission error effects in 24 kb/s SBC systems

Figure 11.10 describes the performance of three SBC systems at $I = 24$ kb/s and bit error rate p_e . In coder A, the adaptive quantizers use the one-word memory logic (4.185). In coder B, the adaptive quantizers use the robust version (4.199a) of the adaptation logic, with step size leakage factor $\beta = 31/32$. In coder C, the sign bit (most significant bit) as well as the most significant magnitude bit in the lowest frequency sub-band are ideally error protected. This protection requires an appropriate amount of bit-stealing from the quantizers, in order to maintain the total bit rate at the original value of $I = 24$ kb/s (Problem 11.8). However, the resulting increase of quantization noise is more than compensated for by reductions in channel noise if the error rate p_e is in the order of 10^{-2} or greater. The overall performance is so as to provide acceptable speech outputs at $p_e = 10^{-2}$, but not at $p_e = 10^{-1}$.

(11.2)

(11.3)

(11.4)

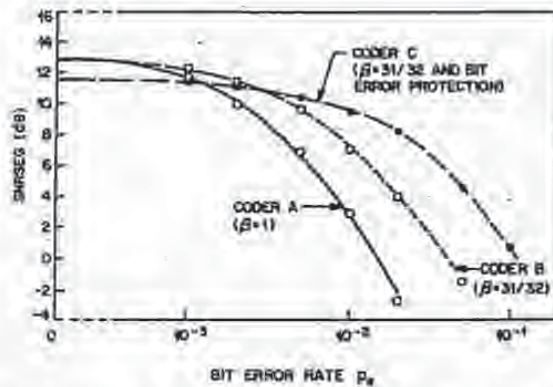


Figure 11.10 Transmission error performance of 16 kb/s SBC systems. Values of segmental SNR as a function of bit error rate p_e , [Crochiere, 1978, AT&T].

(11.5)

Problems

(11.1) Consider a 4-band SBC system where sub-band partitions are constrained by filter-bank considerations to be either (a) or (b) below:

(11.6)

- (a) [0-800] [800-1600] [1600-2400] [2400-3200] Hz
- (b) [225-450] [450-900] [1000-1500] [1800-2700] Hz



not only the
Section 4.9),
error effects.
of Transform

- kb/s and bit
logic (4.185).
aptation logic,
ificant bit) as
e ideally error
ng from the
f $T = 24$ kb/s
is more than
der of 10^{-2} or
at $p_s = 10^{-1}$.

Ignoring side information for synchronization bits, show that bit allocations that provide 9.6 kb/s with the filter-banks above are respectively

- (a) 3, 2, 1, 0 bits/sample
- (b) 4, 3, 2, 1 bits/sample

Note that (b) is closer to the design recommended in Table 11.2.

- (11.2) It is required to design a four-band filter-bank [0-0.5] [0.5-1.0] [1.0-2.0] [2.0-3.0] kHz for 16 kb/s coding of speech.
 - (a) Show the band-division tree that realizes this partition using repeated quadrature mirror filtering of the [0-4.0] kHz band.
 - (b) Assuming that $\max\{R_k\} = 5$ and $\min\{R_k\} = 2$ bits/sample, show that there are at least 2 bit assignments [5,3,2,2] [4,4,2,2] that realize a total bit rate $T = 16$ kb/s. Ignore side information considerations, as in Problem 11.1.

- (11.3) Consider a 6-band SBC system for studio-grade music, with sub-bands [0-0.625] [0.625-1.25] [1.25-2.5] [2.5-5.0] [5.0-10.0] [10.0-20.0] kHz. Allowing 6 kb/s for synchronization information, show that the bit allocation (12, 10, 9, 8, 6, 5) bits/sample permits digital transmission over a 256 kb/s channel.

- (11.4) Consider a SBC system with M bands of equal width ΔW . Consider the SBC input as a 1-second sequence of $2M \Delta W$ samples. Denote variances of individual samples of sub-band k by σ_{2k}^2 ; $k = 1, 2, \dots, M$. Let each of these samples in sub-band k be quantized using R_k bits/sample. Because of a constant sampling rate $2\Delta W$, the total number of samples per second is independent of k . The optimum bit allocation for minimum mse, and the maximum gain G_{SBC} over single-band PCM, are given (on a per sample basis) by (11.10) and (11.12).

It is also useful to give results on a per second basis. Define R as the total bit rate (bits/sec) in the SBC system, $R_k = 2\Delta W R_k$ as the bit rate (bits/second) allocated to encode band k , and $\sigma_{2k}^2 = \sigma_{2k}^2 2\Delta W$ as the power in sub-band k . Show that the formulas (11.10) and (11.12) are equivalent to the pair of formulas

$$R_{k,opt} = \frac{R}{M} + \Delta W \log_2 \frac{\sigma_{2k}^2}{\left[\prod_{l=1}^M \sigma_{2l}^2 \right]^{1/M}}; \quad \max(G_{SBC}) = \frac{\frac{1}{M} \sum_{k=1}^M \sigma_{2k}^2}{\left[\prod_{k=1}^M \sigma_{2k}^2 \right]^{1/M}}$$

entral SNR as a

- (11.5) Refer to Problem 11.4 and the equal-width four-band partition of Problem 11.1(a). Equate the power $\sigma_{2k}^2 = \sigma_{2k}^2 2\Delta W$ to $S_k 2\Delta W$ where S_k represents the average value of input psd in sub-band k . Use the long-time psd of speech in Figure 2.9(a) together with the formula for $R_{k,opt}$ in Problem 11.4 to show that the bit allocations in Problem 11.1(a) are indeed nearly optimal for a mmse criterion.

onstrained by

- (11.6) Consider the highly structured two-level psd of Figure 2.24 and (2.16k).
 - (a) Consider SBC with $M = 2 \Delta \Omega = \Omega_W/2$, and band-edges at 0, $\Omega_W/2$ and Ω_W to follow the shape of the input psd. Use the result of Problem 11.4 to show that the maximum gain in 2-band SBC is

$$\max\{G_{SBC}\} = (\alpha(2-\alpha))^{-M}$$

- (b) Show that $\max\{G_{SBC}\} = \gamma_r^{-2} = \max\{G_{SBC}\}$, the reciprocal of the spectral flatness measure (Problem 2.22) of the process, i.e., SBC with $M = 2$ bands is sufficient to realize the maximum performance for this special psd.
- (11.7) Consider the case of M equal-width sub-bands.
- (a) Show that the adjacent sample correlation ρ_{1k} for the decimated signal in sub-band k vanishes if the psd in that sub-band is flat-topped.
- (b) Determine the four values of ρ_{1k} for the 4-band partition of a signal with an integrated power spectrum and $\psi = 4$.
- (11.8) Consider a 4-band SBC system for 24 kb/s speech coding, with the QMF partition [0, 1000] [1000, 2000] [2000, 3000] [3000, 4000] Hz, and with a normal bit allocation of (5, 4, 2, 1) bits/sample for quantization. Consider that this system is adapted to a noisy channel by protecting all bits in the first sub-band using a (12, 8) Hamming code (with 4 redundant bits for every 8 message bits). Show that if the bit allocation for quantization is changed to (4, 3, 2, 1) bits/sample, the total transmission rate is still 24 kb/s.

References

- B. S. Atal and J. R. Remde, "Split-Band APC System for Low Bit Rate Encoding of Speech," Proc. ICASSP, April 1981.
- H. G. Bellanger, G. Bonnerot, and M. Coudreuse, "Digital Filtering by Polyphase Network: Application to Sample-Rate Alteration and Filter-Banks", IEEE Trans. on Acoustics, Speech and Signal Proc., pp. 252-259, 1976.
- R. V. Cox, unpublished work, Bell Laboratories, 1981.
- R. V. Cox, "A Comparison of Three Speech Coders to Be Implemented on the Digital Signal Processor," Bell System Tech. J., pp. 1411-1421, September 1981.
- R. V. Cox, unpublished work, Bell Laboratories, 1983.
- R. E. Crochiere, "On the Design of Sub-Band Coders for Low Bit Rate Speech Communication," Bell System Tech. J., pp. 747-771, May-June 1977.
- R. E. Crochiere, "An Analysis of 16 kb/s Sub-band Coder Performance: Dynamic Range, Tandem Connections, and Channel Errors," Bell System Tech. J., pp. 2927-2952, October 1978.
- R. E. Crochiere, "Sub-band Coding," Bell System Tech. J., pp. 1633-1654, September 1981.
- R. E. Crochiere, R. V. Cox and J. D. Johnston, "Real Time Speech Coding," IEEE Trans. on Communications, pp. 621-634, April 1982.
- R. E. Crochiere and L. R. Rabiner, "Interpolation and Decimation of Digital Signals - A Tutorial Review," Proc. IEEE, pp. 300-331, March 1981.
- R. E. Crochiere and L. R. Rabiner, *Multirate Digital Processing*. Prentice Hall, 1983.
- R. E. Crochiere and M. R. Sambur, "A Variable-Band Coding Scheme for Speech Encoding at 4.8 kb/s", Bell System Tech. J., pp. 771-780, May-June 1977.

R. E. System
 W. R. Commun
 D. Estel Schemes
 D. Estel pp. 320-
 J. L. Fla
 C. Gula Proc. IC
 L. M. G
 C. Grau
 C. D. F. Vector C
 M. Hon Speech,
 J. D. Jo pp. 291-
 J. D. Jo Soc. Co
 D. Mah Speech
 D. Mah Combin 273-282
 L. R. I Cliffs, I
 T. A. J Digital
 T. A. F EUSIP
 J. E. S Elec. E
 J. M. Our Lt



he spectral
 ith $M = 2$
 pecial psd.
 l signal in
 al with an
 the QMF
 a normal
 that this
 sub-band
 age bits).
 3, 2, 1)
 sch," Proc.
 Application
 Proc. pp.
 Processor,"
 ioe," Bell
 Tandem
 rans on
 Tutorial
 g at 4.8
 ig 11

R. E. Crochiere, S. A. Webber and J. L. Flanagan, "Digital Coding of Speech in Sub-bands," *Bell System Tech. J.*, pp. 1069-1085, October 1976.

W. R. Daumer, "Subjective Evaluation of Several Efficient Speech Coders," *IEEE Trans. on Communications*, pp. 662-665, April 1982.

D. Esteban and C. Galand, "Application of Quadrature Mirror Filters to Split Band Voice Coding Schemes," *Proc. ICASSP*, pp. 191-195, May 1977.

D. Esteban and C. Galand, "32 kb/s CCITT-Compatible Split Band Coding Scheme," *Proc. ICASSP*, pp. 320-325, 1978.

J. L. Flanagan et al., "Speech Coding," *IEEE Trans. on Communications*, pp. 710-737, April 1979.

C. Galand and D. Esteban, "16 kb/s Sub-band Coder Incorporating Variable Overhead Information," *Proc. ICASSP*, pp. 1684-1687, April 1982.

L. M. Goodman, "Channel Encoders," *Proc. IEEE*, pp. 127-128, 1967.

C. Gravel, "Sub-band Coding with Adaptive Bit Allocation," *Signal Proc.*, 1980.

C. D. Heron, R. E. Crochiere and R. V. Cox, "A 32-Band Sub-Band/Transform Coder Incorporating Vector Quantization for Dynamic Bit Allocation," *Proc. ICASSP*, pp. 1276-1279, April 1983.

M. Honda, N. Kitawaki and F. Itakura, "Adaptive Bit Allocation Scheme in Predictive Coding of Speech," *Proc. ICASSP*, pp. 1672-1675, May 1982.

J. D. Johnston, "A Filter Family Designed for Use in Quadrature Mirror Filter Banks," *Proc. ICASSP*, pp. 291-294, April 1980.

J. D. Johnston and R. E. Crochiere, "An All-Digital 'Commentary-Grade' Sub-band Coder," *Audio Eng. Soc. Conv.*, AES preprint, May 1979.

D. Malah, "Time Domain Harmonic Scaling Algorithms for Bandwidth Reduction and Time Scaling of Speech Signals," *IEEE Trans. on Acoustics, Speech and Signal Processing*, pp. 121-133, April 1979.

D. Malah, R. E. Crochiere and R. V. Cox, "Performance of Transform and Sub-Band Coding Systems Combined with Harmonic Scaling of Speech," *IEEE Trans. on Acoustics, Speech and Signal Proc.*, pp. 273-283, April 1981.

L. R. Rabiner and R. W. Schafer, *Digital Processing of Speech Signals*, Prentice-Hall, Englewood Cliffs, N.J., 1978.

T. A. Ramstad, "Sub-band Coder with a Simple Bit Allocation Algorithm: A Possible Candidate for Digital Mobile Telephony," *Proc. ICASSP*, pp. 203-207, May 1982.

T. A. Ramstad and O. Foss, "Sub-band Coder Design Using Recursive Quadrature Mirror Filters," *Proc. EUSIPCO*, pp. 747-752, 1980.

J. E. Sjernvall, "On Rate and Frequency Allocation in Sub-band Coding of Gaussian Sources", Dept. of Elec. Eng. Report No. 1977-12-05, Linköping University, Sweden, 1977.

J. M. Tribolet, P. Noll, B. J. McDermott and R. E. Crochiere, "A Comparison of the Performance of Our Low Bit Rate Speech Waveform Coders," *Bell System Tech. J.*, pp. 699-713, March 1979.

References

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

~~IMAGES CROPPED AT TOP, BOTTOM OR SIDES~~

~~EXCESSIVE CONTRAST~~

~~SMUDGES, STAINING, BLEMISHES OR DRAWINGS~~

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

~~GRAY SCALE DOCUMENTS~~

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

cited in the European Search
Report of EP 96 91 9405 9
Your Ref.: 804 10 0010 EP

XP 000566794

Techniques for data hiding

Walter Bender, Daniel Grub, and Norishige Morimoto
Massachusetts Institute of Technology, Media Laboratory
Cambridge, Massachusetts 02139 USA

PD: '95

pp. 164-173 = 10

ABSTRACT

Data hiding, or steganography, is the process of embedding data into image and audio signals. The process is constrained by the quantity of data, the need for invariance of the data under conditions where the "host" signal is subject to distortions, e.g. compression, and the degree to which the data must be immune to interception, modification, or removal. We explore both traditional and novel techniques for addressing the data hiding process and evaluate these techniques in light of three applications: copyright protection, tamper-proofing, and augmentation data embedding.

1. INTRODUCTION

Digital media facilitate access to audio and image data, potentially improving the portability, efficiency, and accuracy of the information. Side effects of facile data access are violation of copyright, and tampering or modification of content. We are investigating data hiding as a means of protecting intellectual property rights and as an indicator of content manipulation. Data hiding is a class of processes used to embed data, such as copyright information, into media such as image and audio with a minimum amount of degradation to the "host" signal, i.e., the embedded data should be invisible or inaudible to a human observer. Note that data hiding is distinct from encryption. The goal of data hiding is not to restrict or regulate access to the host signal, but rather to ensure that embedded data remains inviolate.

The primary purposes for data hiding in digital media are to provide solid proof of the copyright and assurance of content integrity. Therefore, the data should stay hidden in the host, even if the host signal is subjected to manipulation, such as filtering, re-sampling, cropping, or data compression. Other applications, such as augmentation data embedding need not be invariant to detection or removal, since these data are there for the benefit of both the author and the content consumer. Thus, the techniques used for data hiding vary depending on the quantity of data being hidden and the required invariance to manipulation. A class of processes are needed to span the entire range of the applications.

The technical challenges of data hiding are formidable. Whatever "hole" in the host signal one finds to fill with data is likely to be eliminated by signal compression. The key to successful data hiding is to find holes that are not suitable for exploitation by compression algorithms. A further challenge is to fill these holes with data that remains invariant to host signal transformations. Data hiding techniques should be capable of embedding data in a host signal with the following restrictions and features: (1) Degradation of the host signal should be minimized - the embedded data needs to be "invisible" or "inaudible"; (2) Embedded data needs to be directly encoded into the image or audio signal itself, rather than into a header or wrapper so it remains intact across varying data file formats; (3) The embedded data should be immune to modifications ranging from intentional and intelligent removal to common usage, e.g. channel noise, filtering, re-sampling, cropping, encoding, compressing, etc.; (4) Asymmetrical coding of the embedded data is desirable since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make it difficult to be accessed; (5) It is inevitable that some degradation to the data when the host signal is modified. Error correction coding¹ is used to ensure hidden data integrity; (6) Finding hidden data in a modified host signal also presents a challenge. The embedded data should be self-clocking or arbitrarily re-entrant.

1.1 Applications

Several prospective applications of data hiding are discussed in this section. The amount of data to be hidden and the expected level of modification for each application are different, therefore, different processes based on different techniques are used for each application. There are always trade-offs between the amount of data hidden and the level of immunity to modification.

BEST AVAILABLE COPY

PRODUCED BY ...

0-8194-1767-0/93/00 00

possible to calculate the likelihood that a particular picture has occurred through random choice of points. Now, by choosing the sequence of points in the picture using a pseudo-random number generator and a known seed, the seed becomes the key. Iterate through the picture for n points, moving a , up one brightness quanta, and b , down one. This encodes the picture. To decode the picture, calculate the sum S . Since the expected value of the difference of two points is now 2, the expected sum S will now be $2 \times n$. As n increases, the degree of certainty that this S could not have been arrived at unless the picture is encoded rapidly approaches 100%.

Using this basic method, we have encoded a number of pictures. These modifications improve performance: (1) Treat "patches" of several points rather than single points. This has the effect of shifting the noise introduced by Patchwork into lower spatial frequencies, where it is less likely to be removed by compression and FIR filters; (2) Patchwork decoding is highly sensitive to affine transformations of the host image. If the path of iteration through the picture is offset by translation, rotation, or scaling between encoding and decoding, the code is lost. A combination with either affine coding (described in section 2.2.1) or some heuristic based upon feature recognition (e.g., alignment to the intraocular line of a face) is necessary to make Patchwork more robust; (3) Patchwork is remarkably resistant to cropping. By disregarding points outside of the known picture area, Patchwork degrades in accuracy approximately as $1/n$ of the picture size. Patchwork is also resistant to gamma and tone scale correction since adjacent brightness values move roughly the same way under such modifications.

To validate Patchwork, an experiment was done on three AP wire photographs, each converted to approximately 200×300 pixels and 8 bits per pixel. Our results using this method are encouraging (See Figure 1). A typical 200×300 pixel image can be encoded to between 98% and 99.9% certainty. This is resistant to kernel modifications up to a 5×5 kernel, and after JPEG compression, with parameters set to 75% quality and 0% smoothing, the picture is still encoded to 85% certainty.

The major limitation to this technique is the extremely low bandwidth, usually one bit. However, without the key for the pseudo-random number generator, it is nearly impossible to remove this coding without blurring or obscuring the picture beyond recognition.

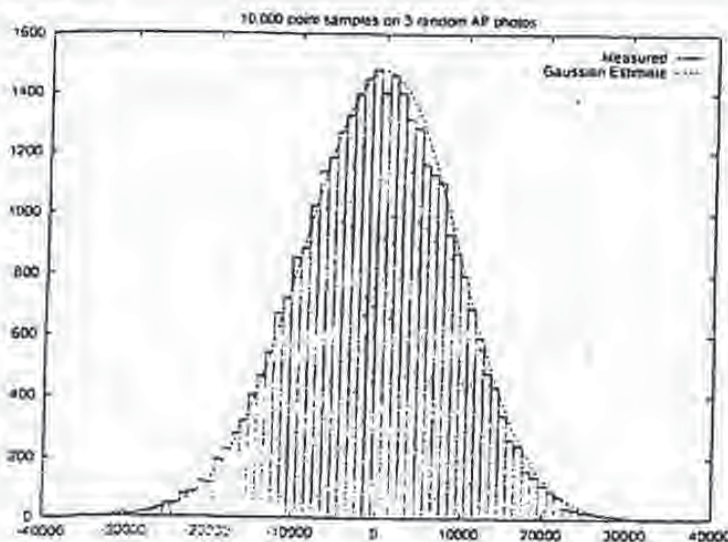


Figure 1: Experimental results from Patchwork. The sum S is plotted along the horizontal axis. The number of trials that yield S is plotted along the vertical axis. The expected value of S is 74.79 where $n=10,000$.

2.1.2 Texture Block Coding: a visual approach

Another method for low bit-rate data hiding is "Texture Block Coding." This method hides data in continuous random texture patterns. The texture blocking scheme is implemented by copying a region from a random texture pattern found in a picture to an area which has similar texture. This results in a pair of identically textured regions in the image. The auto-correlation of the image results in the recovery of the shape of the region.

Since the two regions are identical, they are modified in the same way when if picture is uniformly transformed. By making the region reasonably large, the inner part of the region is immune to most non-geometric transformations. In our experiments, coded 16x16 pixel blocks can be decoded even when the picture is subjected to a combination of filtering, compression and rotation.

Texture block coding is not without its disadvantages. Currently it requires a human operator to choose the source and destination regions, and to evaluate the visual impact upon the image. It is possible to automate this process using a feature recognition system. However, this technique will not work on images that lack moderately large areas of random texture from which to draw.

Future research in this area includes the possibility of cutting and pasting blocks from only part of the image frequency spectrum. This would allow less noticeable blocks to be moved around, and a final image that is considerably more robust to various image compression algorithms.

2.2 High bit-rate coding

As illustrated in Table 1, high bit-rate methods tend not to be immune to image modifications. The most common form of high bit-rate encoding is simply replacing the least significant bit of the image data with the embedded data. Other techniques include the introduction of high-frequency, low-amplitude noise and direct spread-spectrum. All of the high bit-rate methods can be made more robust through the use of error-correction coding, at the expense of data rate. Consequently, high bit-rate codes are only appropriate where it is reasonable to expect that a great deal of control is maintained over the images.

Individually, none of the techniques developed are resistant to all possible transforms. In combination, often one technique can supplement another. Supplementary techniques are particularly important for recovery from geometric modifications such as affine transformations, and maintaining synchronization for spread-spectrum encoding.

2.2.1 Affine coding

Some of the data hiding techniques, such as Patchwork, are vulnerable to affine transforms. It makes sense to develop techniques that can be used in conjunction with others to provide the ability to recover data after affine application. "Affine coding" is such a technique. Any one of the high bit-rate coding techniques is used to encode pre-defined reference patterns into an image. Estimation of any geometric transformation of the image is achieved by comparing the original shape, size, and orientation of the reference patterns to those found in the transformed image. Since affine transforms are linear, the inverse transform can be applied to recover the original image. Once this is done, the image is ready for further extraction of hidden data.

2.3 Applications

The techniques outlined above for placing data in images are useful in a variety of applications. Most of the applications (digital watermark, feature location, embedded captions, and tamper proofing) are suited to one of the above techniques, depending on data requirements and anticipated modifications to the host signal.

2.3.1 Digital Watermark

The object of "Digital Watermark" is to place an indelible mark on an image. Usually, this means encoding only a handful of bits, sometimes as few as one. This has several uses, including the protection of on-line images for news services, and for photographers who are selling their work for publication. One can imagine a digital camera placing such a watermark on every photo it takes, allowing the photographer to be identified wherever the image appears.

It can be expected that if information about legal ownership is to be included in an image, it is likely that someone might want to remove it. If this is a concern then techniques used in Digital Watermark need to be hard to remove. Both the Patchwork and Texture Block Coding techniques show promise for Digital Watermark, with Patchwork used for a more secure system, and Texture Block Coding for a system the public can access.

2.3.2 Feature location

Another application of data hiding is feature location. Using data hiding it is possible (or an editor (or machine) to encode descriptive information, such as the location and identification of features of interest, directly into an image. This enables retrieval of the descriptive information. Since the information is spatially located in the image, it is not removed unless the feature of interest is removed. It also translates, scales and rotates exactly as the feature of interest does.

This application does not have the same requirements for robustness as the digital watermark. It can be assumed that since the feature location is providing a service, it is unlikely someone will maliciously try to remove the encoded information.

2.3.3 Embedded captions

Typical news photograph captions are approximately one kilobyte of data. Thus embedding captions is a relatively high bitrate application for data hiding. Like feature location, caption data is usually immune to malicious removal. While captions are useful by themselves, they become even more useful when combined with feature location. It is then possible for portions of the caption to directly reference items in the picture. Captions can self-edit once this is done. If an item referenced in the caption is cropped out of the picture, then the reference to that item in the caption can be removed automatically.

2.3.4 Tamper Proofing

Both the Digital Watermark and the Tamper Proofing applications pronounce a one bit judgement. Digital Watermark answers the question: "Is the image owned by someone?" Tamper Proofing answers the question: "Has this image been modified?"

There are several ways to implement Tamper Proofing. The easiest way is to encode a check-sum of the image within the image. It is useful to consider a Tamper Proofing algorithm that is not triggered by small changes in the image, such as cropping and gamma correction, but is triggered by gross changes, such as removing or inserting items or people. This suggests an approach involving a pattern overlaid on the image. The key to a successful overlay is to find a pattern resistant to filtering and gamma correction, yet is not be removed easily. This problem remains an active area of research.

3. DATA HIDING IN AUDIO

Data hiding in audio signals provides a special challenge because the human auditory system (HAS) is extremely sensitive. The HAS is sensitive to a dynamic range of amplitude of one billion to one and of frequency of one thousand to one. Sensitivity to additive random noise is also acute. The perturbations in a sound file can be detected as low as one part in ten million (-80dB). Although the limit of perceptible noise increases as the noise contents of the host audio signal increases, the typical allowable noise level is very low. The HAS has very low sensitivity to the phase of the sound. Unfortunately, this "hole" has been exploited by numerous audio compression algorithms.

3.1 Audio environments

There are several environments that need to be considered when hiding data in an audio host signal. An end-to-end digital audio environment has the advantage of absolute amplitude, phase and temporal quantization. Host audio signals that pass through an analog stage and are subsequently re-digitized have only relative characteristic values. Signals that stay digitally encoded but undergo re-sampling may preserve amplitude and phase accurately, but have changing temporal quantization.

Currently, the most popular format for high quality audio is in 16-bit quantization, e.g. WAV on PCs and AIFF on Macintosh™ (8-bit μ -law is also popular). 16-bit quantization yields quanta that is only one part in 65536, approximately 150 times larger than the minimum perceptual level. This would suggest that random noise is not the best way to proceed. One possibility is to adapt the noise insertion to the host signal content. Another is to modify the phase of each frequency component of the sound. This would be ideal to hide data inaudibly, except that many audio compression algorithms, e.g. the ISO MPEG-AUDIO standard, cause considerable corruption of phase information. As is the case in data hiding with still images, it is necessary to investigate several methods for audio, with the understanding that there is no universal answer to "what is the best."

One additional challenge to data hiding in audio is the likelihood that the host audio signal is transferred to analog during its transmission or storage stage. Digital-to-analog conversion introduces noise and distortions to the waveform.

3.2 Low-bit coding

Low-bit coding is the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, we can code a large amount of data in an audio signal. Ideally, the channel capacity will be 8kbps in an 8kHz sampled sequence and 44kbps in a 44kHz sampled sequence for an noiseless channel application. In return for this large channel capacity, audible noise is introduced. The impact of this noise is a direct function of the content of the host signal, e.g., a live sports event contains crowd noise that masks the noise resultant from low-bit encoding.

The major disadvantage of this method is its poor immunity to manipulation. Encoded information can be destroyed by channel noise, re-sampling, etc., unless it is coded using redundancy techniques, which reduces the data rate one to two orders of magnitude. In practice, it is useful only in closed, digital-to-digital environments.

3.3 Phase coding

Phase coding, when it can be used, is one of the most effective coding schemes in terms of the signal-to-noise ratio. When the phase relation between each frequency components is dramatically changed, phase dispersion and "rain barrel" distortions occur. However, as long as the modification of the phase is within certain limits an "inaudible" coding can be achieved (See section 3.3.2).

3.3.1 Procedure

The procedure for the phase coding is as follows:

- (1) Break the sound sequence $s(n)$ into a series of M short segments, $s_i(n)$;
- (2) Apply a N -points Discrete Short Time Fourier Transform (STFT)⁽⁶⁾ to i -th segment, $s_i(n)$, and create a matrix of the phase, $\{\phi_i(\omega_k)\}$, and Fourier transform magnitude, $\{A_i(\omega_k)\}$ for $(1 \leq k \leq N)$, where ϕ_i denotes the phase and A_i the magnitude corresponding to frequency ω_k ;
- (3) Store the phase difference between each adjacent segment for $(0 \leq i \leq M-1)$:

$$\Delta\phi_i(\omega_k) = \phi_{i+1}(\omega_k) - \phi_i(\omega_k)$$

- (4) The binary string used to modify the phase can be a series of a code words. Add these codes to the first set of entries in the phase matrix:

$$\hat{\phi}_0(\omega_k) = \phi_0(\omega_k) + d_n$$

- (5) Re-create phase matrices for $i > 0$ by using the phase difference:

$$\hat{\phi}_1(\omega_k) = \hat{\phi}_0(\omega_k) - \Delta\phi_1(\omega_k)$$

$$\hat{\phi}_i(\omega_k) = \hat{\phi}_{i-1}(\omega_k) - \Delta\phi_i(\omega_k)$$

- (6) Use the modified phase matrix $\hat{\phi}_i(\omega_k)$ and the original Fourier transform magnitude $A_i(\omega_k)$ to reconstruct the sound signal by applying the inverse STFT.

For the decoding process, the synchronization of the sequence is done before the decoding. The length of the segment, the DFT points, and the data interval must be known at the receiver. The value of the underlying phase of the first segment is detected as a 0 or 1, which represents the coded binary string.

Since ϕ_0/ω_0 is modified, the absolute phases of the following segments are modified respectively. However, the relative phase difference of each adjacent frame are preserved. The reconstructed waveform is close enough to the original waveform to be indistinguishable.

3.3.2 Evaluation

Phase dispersion is a distortion caused by a break in the relationship of the phases between each of the frequency components. Minimizing phase dispersion constrains the data rate of phase coding. One cause of phase dispersion is the substitution of phase ϕ_0/ω_0 with the binary code. To minimize error, the magnitude of the phase modifier needs to be as close as possible to the original value. To minimize noise susceptibility the difference between phase modifier states should be maximized. Phase ranges from $-\pi$ to $+\pi$. Our modified phase ranges from 0 to 1.

Another source of distortion is the rate of change of the phase modifier. If the change of the value is as often as one frequency slot per bit, it is likely to break the phase relationship of the adjacent frequency components. Replicating neighbor frequency slots together minimizes audible distortions in reconstruction. Replication causes a linear reduction in the data rate.

As a result of the examination of sound contexts (see section 3.5), we conclude that, for host sounds with quiet backgrounds, a channel capacity of 8bps can be achieved by allocating 128 frequency slots per bit. For host sounds with noisy backgrounds, 16bps to 32bps can be achieved by allocating 32 to 64 frequency slots per slot.

3.4 Spread Spectrum

There is an interesting parallel between data hiding in audio and the work on spread spectrum radio communication. The latter is concerned with hiding kilohertz signals in a megahertz environment, the former with hiding-hertz signals in a kilohertz environment. It turns out that many spread spectrum techniques adapt quite well to data hiding in audio signals. In a normal communication channel, it is often desirable to concentrate the information in as narrow a region of the frequency spectrum as possible. The basic spread spectrum technique, on the other hand, is designed to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible.

While there are many different variations on the idea of spread spectrum communication, the one we concentrated on is Direct Sequence (DS). The DS method spreads the signal by multiplying it by a "chip," a pseudo-random sequence modulated at a known rate. Since the host signals are in discrete-time format, we can use the sampling rate as the "temporal quantum" for coding. The result is that the most difficult problem in DS receiving, that of establishing the correct start and end of the chip quanta for phase locking purposes, is taken care of by the nature of the signal. Consequently, a much higher chip-rate, and an associated higher data rate, is possible.

3.4.1 Procedure

In DS, a "key" is needed to encode the information and the same "key" is needed to decode it. The key is pseudo-random noise that ideally has flat frequency response over the frequency range, i.e., white noise. The key is applied to the coded information to modulate the sequence into a spread spectrum sequence.

The DS method is as follows: First, the data to be embedded is coded as a binary string using error-correction coding so that errors caused by channel noise and host signal modification can be suppressed. Then, the code is multiplied by the carrier wave and the pseudo-random noise sequence, which has a wide frequency spectrum. As a consequence, the frequency spectrum of the data is spread over the available frequency band. Then, the spread data sequence is attenuated and added to the original file as additive random noise (See Figure 2). DS employs bi-phase shift keying since the phase of the signal alternates each time the modulated code alternates. For decoding, phase values ϕ_0 and ϕ_{0+1} are interpreted as a "0" or an "1" which is a coded binary string.

In the decoding stage, the following is assumed: (1) The pseudo random key has maximum randomness and flat frequency spectrum; (2) The key stream for the encoding is known by the receiver. Signal synchronization is done, and the start/stop point of the spread data are known; (3) The following parameters are known by the receiver: chip rate, data rate, carrier frequency, and the data interval.

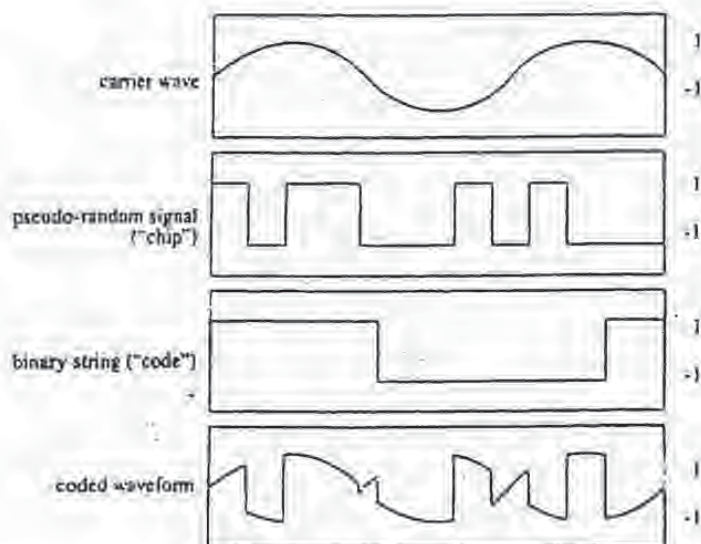


Figure 2: Synthesized spread spectrum information encoded by the Direct Sequence method.

3.4.2 Adaptive data attenuation

As mentioned above, the optimum attenuation factor varies as the noise level of the host sound changes. By adapting the attenuation to the short-term changes of the sound/noise level, we can keep the coded noise extremely low during the silent segments and increase the coded noise during the noisy segments. In our experiments, the quantized magnitude envelop of the host sound wave is used as a reference value for the adaptive attenuation; and the maximum noise level is set to 2% of the dynamic range of the host signal.

3.4.4 Redundancy and error correction coding

Unlike phase coding, DS introduces additive random noise to the sound. To keep the noise level low and inaudible, the spread code is attenuated (without adaptation) to roughly 0.5% of the dynamic range of the host sound file. The combination of simple repetition technique and error correction coding¹ ensure the integrity of the code. A short segment of the binary code string is concatenated and added to the host signal so that transient noise can be reduced by averaging over the segment in the decoding stage. The resulting data rate of the DS experiment is 4bps.

3.5 Sound context analysis

The detectability of noise inserted into a host audio signal is linearly dependent upon the original noise level of the host signal. To maximize the quantity of embedded data, while ensuring it is unnoticed, it is useful to express the noise level quantitatively. The noise level is characterized by computing the magnitude of change in adjacent samples of the host signal:

$$\sigma_{local}^2 = \frac{1}{S_{max}} \times \frac{1}{N} \times \sum_{n=1}^{N-1} |s(n+1) - s(n)|^2$$

where N is the number of sample points in the sequence and S_{max} is the maximum magnitude in the sequence. We use this measure to categorize host audio signals by noise level (See Table 2).

Table 2: Audio noise level analysis

| | studio quality | crowd noise |
|--------------------|----------------|-----------------------------------|
| σ_{local}^2 | <0.005 | 0.005 < σ_{local}^2 < 0.01 |
| | | 0.01 < |

4. CONCLUSION

Several techniques are discussed as possible methods for embedding data in host image and audio signals. While we have had some degree of success, all of the proposed methods have limitations. The goal of achieving protection against intentional removal may be unobtainable.

Automatic detection of geometric and non-geometric modifications applied to the host signal after data hiding is a key data hiding technology. The optimum trade-offs between bit-rate, robustness, and perceptibility need to be defined experimentally. The interaction between various data hiding technologies needs to be better understood.

While compression of image and audio content continues to reduce the necessary bandwidth associated with image and audio content, the need for a better contextual description of that content is increasing. Despite its current shortcomings, data hiding technology is important as a carrier of these descriptions.

5. ACKNOWLEDGMENT

This work was supported in part by the MIT Media Laboratory's News in the Future research consortium and IBM.

6. REFERENCES

1. P. Sweeney, *Error Control Coding (An Introduction)*, Prentice-Hall International Ltd, 1991.
2. E. Adelson, *Digital signal encoding and decoding apparatus*, U. S. Patent 4,939,515, 1990.
3. FTP://sumex-aim.stanford.edu/stego.
4. W. Bender, *Data Hiding*, News in the Future, MIT Media Laboratory, (unpublished lecture notes), May, 1994.
5. A. Lippman, *Receiver compatible enhanced definition television system*, U. S. Patent 5,010,405, 1991.
6. J. Gruber, *Smart Paper*, *Wired*, 2:12, December, 1994.
7. K. Matsui and K. Tanaka, *Video-Steganography: How to Secretly Embed a Signature in a Picture*, IMA Intellectual Property Project Proceedings, 1:1, January, 1994.
8. R. C. Dixon, *Spread Spectrum Systems*, John Wiley & Sons, Inc., 1976.
9. S. K. Marvin, *Spread Spectrum Handbook*, McGraw-Hill, Inc., 1985.
10. A. V. Oppenheim and R. W. Schaefer, *Digital Processing of Speech Signals*, Prentice-Hall, Inc., 1975.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

MISSING CONTENT AT TOP, BOTTOM OR SIDES

MISSING OR BLURRED CONTENT

UNREADABLE OR UNLEGIBLE TEXT OR DRAWINGS

SKEWED/SIANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

cited in the European Search
Report of EP 86 91 0405.9
Your Ref.: 80410 0010 EPO

EMBEDDING ROBUST LABELS INTO IMAGES FOR COPYRIGHT PROTECTION

Jian Zhao & Eckhard Koch
Fraunhofer Institute for Computer Graphics
Wilhelmstr. 7, 64283 Darmstadt, Germany
Email: {zhao, ekoch}@igd.fhg.de

XP 000571967

Abstract

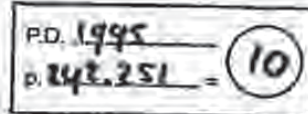
This paper describes a set of novel steganographic methods to secretly embed robust labels into image data for identifying image copyright holder and original distributor in digital networked environment. The embedded label is undetectable, unremovable and unalterable. Furthermore it can survive processing which does not seriously reduce the quality of the image, such as lossy image compression, low pass filtering and image format conversions.

1 Introduction

The wide use of digitally formatted audio, video and printed information in network environment has been slowed down by the lack of adequate protection on them. Developers and publishers hesitate to distribute their sensitive or valuable materials because of the easiness of illicit copying and dissemination [3],[6],[7].

Compared to ordinary paper form information, digitized multimedia information (image, text, audio, video) provides many advantages, such as easy and inexpensive duplication and re-use, less expensive and more flexible transmission either electronically (e.g. through the Internet) or physically (e.g. as CD-ROM). Furthermore, transferring such information electronically through network is faster and needs less efforts than physical paper copying, distribution and update. However, these advantages also significantly increase the problems associated with enforcing *copyright* on the electronic information.

Basically, in order to protect distributed electronic multimedia information, we need two types of protections. First, the multimedia data must contain a label or code, which identifies it uniquely as property of the copyright holder. Second, the multimedia data should be marked in a manner which allows its distribution to be tracked. This does not limit the number of copies allowed (vs. copy protection), but provides a mean to check the original distributor. In order to prevent any copyright forgery, misuse and violation, the copyright label must be unremovable and unalterable, and furthermore survive processing which does not seriously reduce the quality of the data. This requires that first the label must be secretly stored in a multimedia data, i.e. the locations for embedding this label are secret, second the label must be robust even if the labeled multimedia data has been processed incidentally or intentionally.



74 BEST AVAILABLE COPY

This paper describes a set of novel steganographic methods to secretly embed robust labels into image data for copyright protection in open networked environment. The label embedded in the image can be assigned or generated in a way that it is able to identify the copyright holder and the original purchaser (distributor).

Steganographic method is a technique embedding additional information into a data by modifying the original data without affecting the quality of the data. Many steganographic methods have been proposed to aim at storing additional information to identify or label formatted electronic documents [1], images, video [8], and audio data. However, they are far away from the requirements in protecting multimedia information in a networked environment, because although some of them provide secret locations for label embedding, none of them is able to prevent attacks on the embedded information by simple image processing, i.e. they do not adequately address the possibilities of using data compression, low pass filtering and/or simply changing the file format to remove an embedded code.

The discussion begins with a general framework for copyright label embedding. Then two specific methods are developed: one is based on the JPEG compression model for embedding labels in gray-scaled and color images, and the other is based on the black/white rate for binary images. Finally, these methods are tested experimentally and the future work is discussed.

2 Robust Label Embedding Framework

The system developed along the methods presented in this paper is called 'SysCoP' (System for Copyright Protection). It consists of a set of methods to embed robust labels into different types of images. Currently, the system supports gray-scaled, color, and binary images. These methods share an algorithm framework for both label writing and reading described below.

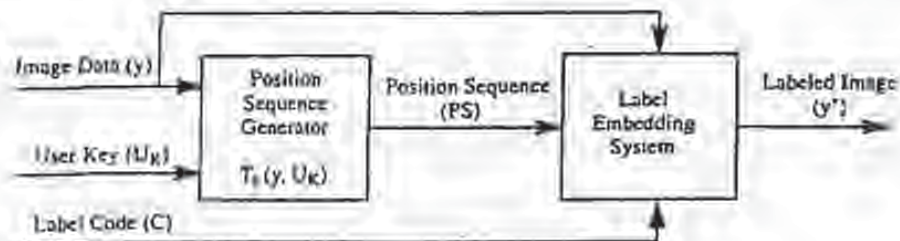


Figure 1. Write label

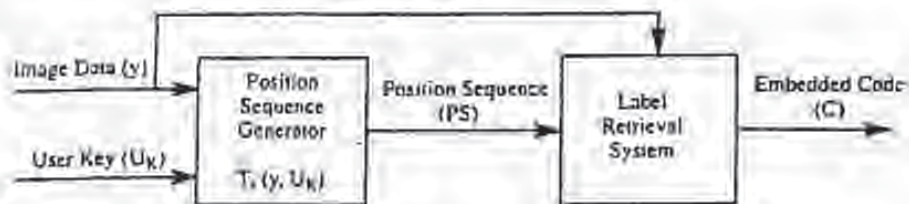


Figure 2. Read label

Algorithm 1(b): Framework (read).

- (1) If $i \geq n$, return.
- (2) Randomly select a distributed or a contiguous 6x8 block b , using the position sequence generation function $T_s(U_X, y)$ in Figure 2.
- (3) If b exists already in \mathcal{B} , then go to (2), otherwise add b to \mathcal{B} .
- (4) Call $check_read(b, c_i)$ to check whether b is a valid block; if this function returns False (i.e. the block b is an invalid block), go to (2).
- (5) Call $read(b)$ to retrieve a bit from the block b .
- (6) Increment i , and go to (1).

3 Robust Label Embedding Methods

3.1 JPEG-Based Label Embedding for Gray-Scaled and Color Images

In this subsection, we first introduce briefly the JPEG compression model, then describe the principle of the embedding methods based on the JPEG compression model. Finally, the algorithms for embedding labels into gray-scaled and color images are developed.

Suppose the source image composes three components: one luminance (Y) and two chrominance (I and Q). That is, each pixel in the image can be represented with a triple of 8-bit values (Y,I,Q). Each component is broken up into contiguous blocks. The JPEG compression consists of six steps: normalization, DCT transformation, quantization, zigzag scan, run-length encoding and Huffman coding steps. Since our method is applied after the quantization step, we only describe briefly the first three steps of the JPEG model. The detailed description of the JPEG model is available elsewhere [1].

The normalization step brings all image values into a range, e.g. between -128 and 127 for a 24-bit image. The DCT step applies the discrete cosine transform (DCT) to each 8x8 block, producing a new 8x8 block $\{10\}$. If we call the new block $Y(k,l)$, with $k,l \in 0..7$, the equation of the DCT is:

$$Y(k,l) = \frac{1}{8} \sum_i \sum_j C(i,k)C(j,l)y(i,j)$$

where

$$C(i,k) = A(k) \frac{\cos(2i+1)k\pi}{16} \quad A(k) = \frac{1}{\sqrt{2}} \text{ (for } k=0), A(k) = 1 \text{ (for } k \neq 0) \quad (1)$$

Each element of the new block is further quantized:

$$\hat{Y}_0(k,l) = \text{Round}\left(\frac{Y(k,l)}{q(k,l)}\right) \quad (2)$$

Equation (2) represents the entire lossy modelling process of the JPEG compression. The choice of the quantization table ($q(k,l)$) determines both the amount of compression and the quality of the decompressed image. The JPEG standard includes recommended luminance and chrominance quantization tables resulting from human factors studies. To obtain different compression quality, we typically use a quality factor to scale the values of these default quantization tables.

In the JPEG decompression process, each element of $Y_Q(k,l)$ is multiplied by $q(k,l)$ to recover an approximation of $Y(k,l)$. Finally, the image block $y(i,j)$ can be recovered by performing an inverse 2-D DCT (IDCT):

$$y(i,j) = \frac{1}{4} \sum_k \sum_l C(k,k)C(l,l)Y(k,l) \quad (3)$$

The basic principle of the JPEG-based embedding method is that quantized elements have a moderate variance level in the middle frequency coefficient ranges, where scattered changes in the image data should not be noticeably visible. The specific frequencies being used to embed the code will be 'hopped' in this range to increase the robustness of the signal and making it more difficult to find [5], [2]. A label bit is embedded through holding specific relationship among three quantized elements of a block. The relationships among them compose 8 patterns (combinations) which are divided into three groups: two of them are used to represent '1' or '0' for embedded codes (valid patterns), and the other represents *invalid patterns*. If too big modifications are needed to hold a desired valid pattern representing a bit, this block is *invalid*. In this case, the relationships among the three elements of the selected location set are modified to any of the invalid patterns to 'tell' the label-retrieval process that this block is invalid. The criterion for invalid blocks is specified by a parameter MD, i.e. the maximum difference between any two elements of a selected location set in order to reach the desired valid pattern.

| Set No. | (k_1,l_1) | (k_2,l_2) | (k_3,l_3) |
|---------|-------------|-------------|-------------|
| 1 | 2(0,2) | 9(1,1) | 10(1,2) |
| 2 | 9(1,1) | 2(0,2) | 10(1,2) |
| 3 | 3(0,3) | 10(1,2) | 11(1,3) |
| 4 | 10(1,2) | 3(0,3) | 11(1,3) |
| 5 | 9(1,1) | 2(0,2) | 10(1,2) |
| 6 | 2(0,2) | 9(1,1) | 10(1,2) |
| 7 | 9(1,1) | 16(2,0) | 2(0,2) |
| 8 | 16(2,0) | 9(1,1) | 2(0,2) |
| 9 | 2(0,2) | 9(1,1) | 16(2,0) |
| 10 | 9(1,1) | 2(0,2) | 16(2,0) |
| 11 | 10(1,2) | 17(2,1) | 3(0,3) |
| 12 | 17(2,1) | 10(1,2) | 3(0,3) |
| 13 | 10(1,2) | 3(0,3) | 17(2,1) |
| 14 | 3(0,3) | 10(1,2) | 17(2,1) |
| 15 | 9(1,1) | 16(2,0) | 17(2,1) |
| 16 | 16(2,0) | 9(1,1) | 17(2,1) |
| 17 | 10(1,2) | 17(2,1) | 18(2,2) |
| 18 | 17(2,1) | 10(1,2) | 18(2,2) |

Table 1. Possible location sets



Figure 3. Possible locations for embedding code in a block

| (k_1,l_1) | (k_2,l_2) | (k_3,l_3) | |
|-------------|-------------|-------------|------------------|
| H | M | L | patterns for '1' |
| M | H | L | |
| H | H | L | |
| M | L | H | patterns for '0' |
| L | M | H | |
| L | L | H | invalid patterns |
| H | L | M | |
| L | H | M | |
| M | M | M | |

Table 2. '1', '0' and invalid patterns. (H: High, M: Middle, L: Low)

Our statistic results of the possible locations holding the specific frequencies are illustrated in Figure 3 as shadowed areas within a 8x8-block. In Table 1, we give our statistic results of the best location sets

combined from these possible elements. The algorithms to write and read a label into and from an color or gray-scaled image are described in Algorithm 2(a)-(d).

Two parameters are provided for adjusting the robustness vs. modification visibility in an embedding process. The first one is the distance (D) between selected quantized frequency coefficients for representing an embedded bit. The default value of this distance is 1. The greater distance produces stronger robustness, but also may cause more serious modification visibilities. The second parameter is the quantization factor (Q) used to quantize the values selected for embedding code. The greater quantization factor results in less modifications to image data but weaker robustness against lossy JPEG compression. The default value of this quantization factor is 75%.

Algorithm 2(a): check_write(b, c_i)

- (1) A three-element location set of the block b is pseudo-randomly (from the user key and image data) selected from the possible location sets listed in Table 1. They are denoted as (k_1, l_1) , (k_2, l_2) and (k_3, l_3) .
- (2) The block b is locally DCT transformed and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q parameter. Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.
- (3) When $c_i=1$, if $\text{MIN}(|Y_Q(k_1, l_1)|, |Y_Q(k_2, l_2)|) + MD < |Y_Q(k_3, l_3)|$ where $|Y_Q(k_u, l_u)|$ is the absolute value of $Y_Q(k_u, l_u)$ with $u \in \{1, 2, 3\}$, MIN is an operation that returns the minimum value of two elements, and MD is the maximum modification distance, then b is an invalid block:
 - (i) modify them to any of the invalid patterns shown in Table 2,
 - (ii) de-quantize and inversely transform (IDCT) them, and write them back to the block b ,
 - (iii) return False.
- (4) When $c_i=0$, if $\text{MAX}(|Y_Q(k_1, l_1)|, |Y_Q(k_2, l_2)|) > |Y_Q(k_3, l_3)| + MD$ where MAX is an operation that returns the maximum value of two elements, and MD is the maximum modification distance, then b is an invalid block:
 - (i) modify them to any of the invalid patterns shown in Table 2,
 - (ii) de-quantize, inversely transform (IDCT) them, and write them back to the block b ,
 - (iii) return False.
- (5) For other cases, return True.

Algorithm 2(b): check_read(b, c_i)

- (1) A three-element location set of the block b is pseudo-randomly (from the user key and image data) selected from the possible location sets listed in Table 1. They are denoted as (k_1, l_1) , (k_2, l_2) and (k_3, l_3) .
- (2) The block b is locally DCT transformed and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q parameter. Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (3) If $|Y_Q(k_1, l_1)|$, $|Y_Q(k_2, l_2)|$ and $|Y_Q(k_3, l_3)|$ form any of the invalid patterns as illustrated in Table 2, return False, otherwise return True.

Algorithm 2(c): write(b, c_i)

Assume that a valid three-element location set of the block b has been pseudo-randomly selected. They are denoted as (k_1, l_1) , (k_2, l_2) , and (k_3, l_3) . The block b is locally DCT transformed, and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q . Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$, and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (1) When $c_i=1$, modify the $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ such that they satisfy the following conditions: $Y_Q(k_1, l_1) > Y_Q(k_3, l_3) + D$, and $Y_Q(k_2, l_2) > Y_Q(k_3, l_3) + D$
- (2) When $c_i=0$, modify the $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ such that they satisfy the following conditions: $Y_Q(k_1, l_1) + D < Y_Q(k_3, l_3)$, and $Y_Q(k_2, l_2) + D < Y_Q(k_3, l_3)$
- (3) $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ are de-quantized, inversely transformed (IDCT), and written back to the block b .

Algorithm 2(d): read(b)

Assume that a valid three-element location set of the block b has been pseudo-randomly selected. They are denoted as (k_1, l_1) , (k_2, l_2) , and (k_3, l_3) . The block b is locally DCT transformed, and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q . Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$, and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (1) If $Y_Q(k_1, l_1) > Y_Q(k_2, l_2) + D$ and $Y_Q(k_2, l_2) > Y_Q(k_3, l_3) + D$, return 1.
- (2) If $Y_Q(k_1, l_1) + D < Y_Q(k_3, l_3)$, and $Y_Q(k_2, l_2) + D < Y_Q(k_3, l_3)$, returns 0.
- (3) In other cases, the embedded bit in this block b has been damaged.

3.2. Black/White Rate-Based Label Embedding for Binary Images

The value of each pixel in a binary image is either '1' or '0'. This determines that, in general, there is no 'noise' space which can be used for embedding additional information. To do it, we must find appropriate image areas where modifications for embedding labels do not affect seriously the quality of the original image. Obviously, these areas are varied with individual images or at least with types of images.

The proposed method for binary images is based on the ratio of '1' and '0' in a selected block. Suppose '1' represent black bit and '0' represent white bit in the source binary image. Let $P_1(b)$ be the rate (percentage) of blacks in the selected block b :

$$P_1(b) = \frac{N_1(b)}{64} \text{ where } N_1(b) \text{ is the number of '1' in the block } b.$$

Since the sum of percentages of blacks and whites in a block is 100%, the rate (percentage) of whites in the block b is $P_0(b) = 100 - P_1(b)$. A bit is embedded into a block b in the following way: a '1' is embedded into the block b if $P_1(b)$ is greater than a given threshold, and a '0' is embedded into the block b if $P_1(b)$ is less than another given threshold. A sequence of contiguous or distributed blocks is modified by switching whites to blacks or vice versa until such thresholds are reached.

We have classified two categories of binary images on which the generic method described above can be applied. These binary images are identified by distribution feature of blacks and whites. The first type of binary images is dithered image in which the black and white are well interlaced. The second type of binary images is black/white sharply contrasted images in which there exist clear boundaries between black and white areas.

Two modification strategies are adopted for these two types of binary images, respectively. For dithered binary images, modifications are well-distributed throughout the whole block: the bit that has most neighbors with the same value (either black or white) is reversed. For sharply contrasted binary images, modifications are carried out at the boundary of black and white pixels: the bit that has most neighbors with the opposite value is reversed. At the borders of the contiguous block, the neighbor bits in the neighbor blocks are also taken into account in both approaches. Two examples of both modification strategies are illustrated in Figure 4 and 5, respectively.

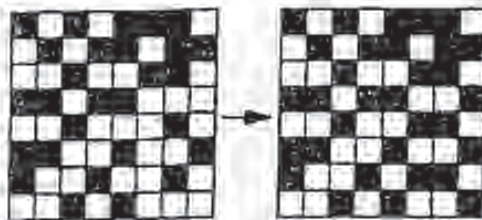


Figure 4. Well-distributed modifications

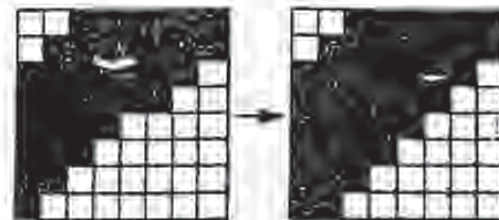


Figure 5. Modifications at black and white boundary

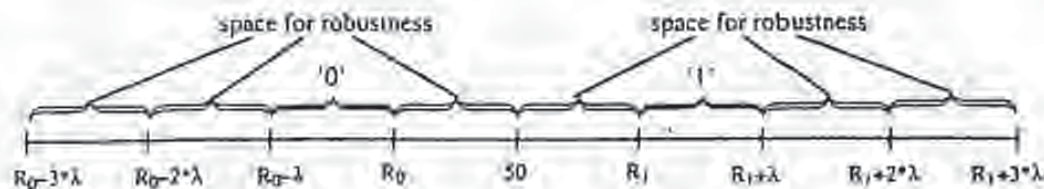


Figure 6. Achieve robustness in the black/white rate-based embedding method

Let R_1 be the threshold rate for '1'. Thus, the threshold rate for '0' is $R_0 = (100\% - R_1)$. Let λ be the robustness degree against image processing of labeled images. It represents the number of bits that can be altered after image processing without damage of embedded bits. For example, when λ is 5%, alternation (i.e. reversion from '1' to '0' or vice versa) of less than 4 bits in a block does not damage the embedded code. Our experiments have shown that the following values of them are the reasonable choices both in robustness of embedding code and the modification visibility:

$$R_1 = 55, R_0 = 45, \text{ and } \lambda = 5$$

The algorithms to write and read a label into and from a binary image are described in Algorithm 3(a)-(d).

Algorithm 3(a): check_write(b, c_i)

(1) If $P_1(b) > R_1 + 3 \cdot \lambda$ or $P_1(b) < R_0 - 3 \cdot \lambda$, return False.

- (2) When $c_i=1$, if $P_1(b) < R_0$, modify the block b such that

$$P_1(b) < R_0 - 3*\lambda,$$
and then return False.
- (3) When $c_i=0$, if $P_1(b) > R_1$, modify the block b such that

$$P_1(b) > R_1 + 3*\lambda,$$
and then return False.
- (4) For other cases, return True.

Algorithm 3(b): check_read(b, c_i)

- (1) If $P_1(b) > R_1 + 2*\lambda$ or $P_1(b) < R_0 - 2*\lambda$, return False.
- (2) For other cases, return True.

Algorithm 3(c): write(b, c_i)

Assume that a valid block b has been pseudo-randomly selected. A bit c_i is embedded into b by switching blacks to whites or vice versa using the different modification strategies described above in order to reach a specified threshold rate.

- (1) When $c_i=1$, modify the block b such that:

$$P_1(b) \geq R_1 \text{ and } P_1(b) \leq R_1 + \lambda.$$
- (2) When $c_i=0$, modify the block b such that:

$$P_1(b) \leq R_0 \text{ and } P_1(b) \geq R_0 - \lambda.$$
- (3) write the block b back to the image.

Algorithm 3(d): read(b)

Assume that a valid block b has been pseudo-randomly selected.

- (1) If $P_1(b) > 50$, return 1.
- (2) If $P_1(b) < 50$, return 0.
- (3) For other cases, the embedded bit in the block b has been damaged.

4 Conclusion

The 'SysCoP' has been implemented on UNIX platform, and provides a graphical interface, a set of UNIX commands and an API (Application Programming Interface). It currently supports JPEG, PPM, GIF, and TIFF image formats. Experiments have been carried out to demonstrate the robustness of our methods against image processing. For the gray-scaled and color images using the JPEG-based embedding method, three images were labeled, and then processed by JPEG compression, format conversions and color reduction. In general, the results are quite satisfactory and meet the basic requirements for embedding codes as copyright labels. Due to the space limitation of the paper, concrete results are omitted. For the binary images, a dithered TIFF binary image and a sharp contrasted TIFF binary image were used in our tests. They are labeled first with $R_1=55\%$ and the robustness degree (λ) 5%. The labeled TIFF images are then smoothed and converted to PBM. The embedded codes were not damaged in both labeled images after smoothing and conversions.

Our methods are still weak against physical damages (e.g. cut a pixel line, grab an area, etc.). Currently, we address this problem by allowing the user to specify 'valuable or sensitive' areas of :

image into which labels are (repeatedly) embedded. Thus, cutting a part which is not in these areas does not damage embedded labels.

The methods described in this paper for embedding robust copyright labels for images have been extended to support MPEG-1. Two additional attacks in embedding copyright labels into MPEG-1 videos have been identified: removal of frames and re-compression with different patterns. To be resistant against them, the copyright label is repeatedly embedded into each frame. Thus we ensure that the label can be retrieved from each I-frame regardless of re-compression with different patterns. Furthermore, we are developing new labeling methods for other digital media, i.e. structured electronic documents (e.g. PostScript, SGML documents) and audio data. In addition, a WWW (World Wide Web) image copyright labeling server incorporating the methods described in this paper is being developed.

Acknowledge We are grateful to Scott Burgett from GMI, USA, who initiated and completed the JPEG-based embedding method of 'SysCoP' during his visiting stay at the Fraunhofer-IGD in Darmstadt. We also want to thank Martin Clavier and Joachim Krumb for helping us in implementing the 'SysCoP' system.

References

- (1) J. BRASSIL, S. LOW, N. MAXEMCHUK, L. D'GORMAN. Electronic Marking and Identification Techniques to Discourage Document Copying. AT&T Bell Laboratories, Murray Hill, NJ, 1994.
- (2) S. BURGETT, E. KOCH, J. ZHAO, A Novel Method for Copyright Labeling Digitized Image Data, Technical Report of Fraunhofer Institute for Computer Graphics, Darmstadt, August, 1994. (Also submitted to IEEE Trans. on Communications, September, 1994).
- (3) A.K. CHOUDHURY, N.F. MAXEMCHUK, S. PAUL, H.G. SCHULZRINNE. Copyright Protection for Electronic Publishing over Computer Networks. AT&T Bell Laboratories, June 1994.
- (4) W. DIFFIE and M. HELLMAN. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.
- (5) R. C. DIXON. *Spread Spectrum Systems*, 2nd ed., Wiley, New York, NY, 1984.
- (6) B. KAHIN. The strategic environment for protecting multimedia. *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, 1994, pp. 1-8.
- (7) E. KOCH, J. RINDFREY, J. ZHAO. Copyright Protection for Multimedia Data. *Proceedings of the International Conference on Digital Media and Electronic Publishing* (6-8 December 1994, Leeds, UK).
- (8) K. MANTUSI and K. TANAKA. Video-Steganography: How to secretly embed a signature in a picture. *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, 1994.
- (9) W. NIBLACK, R. BARBER, W. EQUITZ, M. FLICKNER, E. GLASMAN, D. PETKOVIC, P. YANKER, C. FALOUTOS, G. TAUBIN. The QBIC Project: Querying Images By Content Using Color, Texture, and Shape. *SPIE* vol. 1908, 1993, pp. 173-187.
- (10) K.R. RAO and P. YIP. *Discrete Cosine Transform: Algorithms Advantages, Applications*. Academic Press, 1990.
- (11) G.K. WALLACE. The JPEG still picture compression standard. *Communications of the ACM*, vol. 34, no. 4, April 1991, pp. 30-40.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- IMAGE CUT OFF AT CORNERS
- UNREADABLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

HANDBOOK of APPLIED CRYPTOGRAPHY

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone



CRC Press

Boca Raton London New York Washington, D.C.

BEST AVAILABLE COPY

20-09-02A09:49 RCVD

Library of Congress Cataloging-in-Publication Data

Menezes, A. J. (Alfred J.), 1965-
Handbook of applied cryptography / Alfred Menezes, Paul van Oorschot,
Scott Vanstone.

p. cm. -- (CRC Press series on discrete mathematics and its
applications)

Includes bibliographical references and index.

ISBN 0-8493-8523-7 (alk. paper)

1. Computers--Access control--Handbooks, manuals, etc.
2. Cryptography--Handbooks, manuals, etc. I. Van Oorschot, Paul C.
II. Vanstone, Scott A. III. Title. IV. Series: Discrete
mathematics and its applications.

QA76.9.A25M463 1996

0005.872--dc21

96-27609
CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to provide reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all material or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the CRC Press Web site at www.crcpress.com

© 1997 by CRC Press LLC

No claim to original U.S. Government works
International Standard Book Number 0-8493-8523-7
Library of Congress Card Number 96-27609
Printed in the United States of America 5 6 7 8 9 0
Printed on acid-free paper

BEST AVAILABLE COPY

5.15 Algorithm FIPS 186 one-way function using SHA-1INPUT: a 160-bit string t and a b -bit string c , $160 \leq b \leq 512$.OUTPUT: a 160-bit string denoted $G(t, c)$.

1. Break up t into five 32-bit blocks: $t = H_1 \| H_2 \| H_3 \| H_4 \| H_5$.
2. Pad c with 0's to obtain a 512-bit message block: $X \leftarrow c \| 0^{512-b}$.
3. Divide X into 16 32-bit words: $x_0 x_1 \dots x_{15}$, and set $m \leftarrow 1$.
4. Execute step 4 of SHA-1 (Algorithm 9.53). (This alters the H_i 's.)
5. The output is the concatenation: $G(t, c) = H_1 \| H_2 \| H_3 \| H_4 \| H_5$.

5.16 Algorithm FIPS 186 one-way function using DESINPUT: two 160-bit strings t and c .OUTPUT: a 160-bit string denoted $G(t, c)$.

1. Break up t into five 32-bit blocks: $t = t_0 \| t_1 \| t_2 \| t_3 \| t_4$.
2. Break up c into five 32-bit blocks: $c = c_0 \| c_1 \| c_2 \| c_3 \| c_4$.
3. For i from 0 to 4 do the following: $x_i \leftarrow t_i \oplus c_i$.
4. For i from 0 to 4 do the following:
 - 4.1 $b_1 \leftarrow c_{(i+4) \bmod 5}$, $b_2 \leftarrow c_{(i+3) \bmod 5}$.
 - 4.2 $a_1 \leftarrow x_i$, $a_2 \leftarrow x_{(i+1) \bmod 5} \oplus x_{(i+4) \bmod 5}$.
 - 4.3 $A \leftarrow a_1 \| a_2$, $B \leftarrow b_1 \| b_2$, where b_i denotes the 24 least significant bits of b_i .
 - 4.4 Use DES with key B to encrypt A : $y_i \leftarrow \text{DES}_B(A)$.
 - 4.5 Break up y_i into two 32-bit blocks: $y_i = L_i \| R_i$.
5. For i from 0 to 4 do the following: $z_i \leftarrow L_i \oplus R_{(i+2) \bmod 5} \oplus L_{(i+3) \bmod 5}$.
6. The output is the concatenation: $G(t, c) = z_0 \| z_1 \| z_2 \| z_3 \| z_4$.

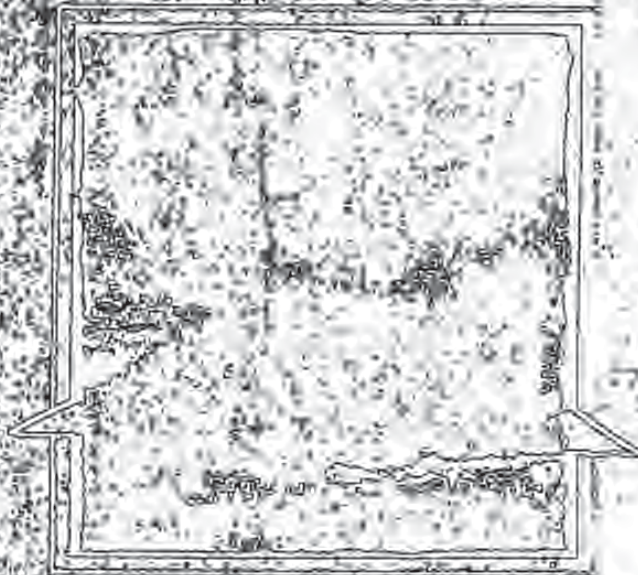
5.4 Statistical tests

This section presents some tests designed to measure the quality of a generator purported to be a random bit generator (Definition 5.1). While it is impossible to give a mathematical proof that a generator is indeed a random bit generator, the tests described here help detect certain kinds of weaknesses the generator may have. This is accomplished by taking a sample output sequence of the generator and subjecting it to various statistical tests. Each statistical test determines whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit; the conclusion of each test is not definite, but rather *probabilistic*. An example of such an attribute is that the sequence should have roughly the same number of 0's as 1's. If the sequence is deemed to have failed any one of the statistical tests, the generator may be *rejected* as being non-random; alternatively, the generator may be subjected to further testing. On the other hand, if the sequence passes all of the statistical tests, the generator is *accepted* as being random. More precisely, the term "accepted" should be replaced by "not rejected", since passing the tests merely provides probabilistic evidence that the generator produces sequences which have certain characteristics of random sequences.

§5.4.1 and §5.4.2 provide some relevant background in statistics. §5.4.3 establishes Golomb's randomness postulates. Specific statistical tests for randomness are described in §5.4.4 and §5.4.5.

BEST AVAILABLE COPY

APPLIED CRYPTOGRAPHY



Protocols, Algorithms, and Source Code in C

BRUCE SCHNEIER

BEST AVAILABLE COPY

Associate Publisher: Katherine Schowalter
Editor: Paul Farrell
Managing Editor: Beth Austin
Editorial Production & Design: Editorial Services of New England, Inc.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering professional services. If legal, accounting, medical, psychological, or any other expert assistance is required, the services of a competent professional person should be sought. ADAPTED FROM A DECLARATION OF PRINCIPLES OF A JOINT COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND PUBLISHERS.

In no event will the publisher or author be liable for any consequential, incidental, or indirect damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising from the use or inability to use the protocols and algorithms in this book, even if the publisher or author has been advised of the possibility of such damages.

Some of the protocols and algorithms in this book are protected by patents and copyrights. It is the responsibility of the reader to obtain all necessary patent and copyright licenses before implementing in software any protocol or algorithm in this book. This book does not contain an exhaustive list of all applicable patents and copyrights.

Some of the protocols and algorithms in this book are regulated under the United States Department of State International Traffic in Arms Regulations. It is the responsibility of the reader to obtain all necessary export licenses before implementing in software for export any protocol or algorithm in this book.

This text is printed on acid-free paper.

Trademarks

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc. is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Copyright © 1994 John Wiley & Sons, Inc. PRINTED IN THE UNITED STATES OF AMERICA

All rights reserved. Published simultaneously in Canada.

Reproduction or translation of any part of this work beyond that permitted by Section 107 or 108 of the 1976 United States Copyright Act without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to the Permissions Department, John Wiley & Sons, Inc.

Library of Congress Cataloging-in-Publication Data

Schneier, Bruce

Applied cryptography : protocols, algorithms, and source code in C
/ Bruce Schneier.

p. cm.

Includes bibliographical references and index.

ISBN 0-471-59756-2 (paper)

1. Computer security. 2. Telecommunication—security measures. 3. Cryptography. 4. Title

QA76.9.A25535 1993

005.8'2—dc20

93-2139

CIP

Printed in the United States of America
109876543

BEST AVAILABLE COPY

Applications of Subliminal Channel

The most obvious application of the subliminal channel is in a spy network. If everyone is sending and receiving signed messages, spies will not be noticed sending subliminal messages in signed documents. Of course, the enemy's spies can do the same thing.

Using a subliminal channel, Alice could safely sign a document under threat. She would, when signing the document, embed the subliminal message, saying, "I am being coerced." Other applications are more subtle. A company can sign documents and embed subliminal messages, allowing them to be tracked throughout the document's lifespan. The government can "mark" digital currency. A malicious signature program can leak the private key. The possibilities are endless.

Subliminal-Free Signatures

Alice and Bob are sending signed messages to each other, negotiating the terms of a contract. They use a digital signature protocol. However, this contract negotiation has been set up as a cover for Alice's and Bob's spying activities. When they use the digital signature algorithm, they don't care about the messages they are signing. They are using a subliminal channel in the signatures to send secret information to each other. The counterespionage service, however, doesn't know that the contract negotiations and the use of signed messages are just cover-ups.

The use of subliminal channels has led people to create subliminal-free signature schemes. These are digital signature schemes that cannot be modified to contain a subliminal channel. See [283,284].

4.1 UNDENIABLE DIGITAL SIGNATURES

The Alice Software Company distributes DEW (Do-Everything-Word™). To ensure that their software is virus-free, they include a digital signature. However, they want only legitimate buyers of the software, not pirates, to be able to verify the signature. At the same time, if copies of DEW are found containing a virus, there should be no way for the Alice Software Company to deny a valid signature.

Conventional digital signatures can be copied exactly. Sometimes this property is useful, as in the dissemination of public announcements. Other times they could be a problem. Imagine a digitally signed personal or business letter. If many copies of that document were floating around, each of which could be verified by anyone, this could lead to embarrassment or blackmail. The best solution is a digital signature that can be proven to be valid, but one that the recipient cannot show to a third party without the signer's consent.

Undeniable signatures, invented by David Chaum [207], are suited to these tasks. Like a normal digital signature, an undeniable signature depends on the signed document and the signer's private key. But unlike normal digital signatures, an undeniable signature cannot be verified without the signer's consent.

The mathematics behind this protocol can be found in Section 16.7, but the basic idea is simple:

BEST AVAILABLE COPY

Shakespeare, or a newsgroup on the Internet [871,872]. There are no keys involved; this is a restricted algorithm.

Gustavus Simmons invented the concept of a subliminal channel in a conventional digital signature algorithm [827]. Since the subliminal messages are hidden in what looks like normal digital signatures, this is a form of obfuscation. Walter sees signed innocuous messages pass back and forth, but he completely misses the information being sent over the subliminal channel. In fact, the subliminal-channel signature algorithm is indistinguishable from a normal signature algorithm, at least to Walter. Walter not only cannot read the subliminal message, but he also has no idea that one is even present. (Of course, any warden who gives his prisoners computers and high-speed modems deserves what he gets.) In general the protocol looks like this:

- (1) Alice generates an innocuous message, at random.
- (2) Using a secret key shared with Bob, Alice signs the innocuous message in such a way as to hide her subliminal message in the signature. (This is the meat of the subliminal channel protocol; see Section 16.6.)
- (3) Alice sends this signed message to Bob via Walter.
- (4) Walter reads the innocuous message and checks the signature. Finding nothing amiss, he passes the signed message to Bob.
- (5) Bob checks the signature on the innocuous message, confirming that the message came from Alice.
- (6) Bob ignores the innocuous message and, using the secret key he shares with Alice, extracts the subliminal message.

What about cheating? Walter doesn't trust anyone and no one trusts him. He can always prevent communication, but he has no way of introducing phony messages. Since he can't generate any valid signatures, Bob will detect his attempt in step (3). And since he does not know the shared key, he can't read the subliminal messages. Even more important, he has no idea that the subliminal messages are there. Signed messages using a digital signature algorithm look no different from signed messages with subliminal messages embedded in the signature.

Cheating between Alice and Bob is more problematic. In some implementations of a subliminal channel, the secret information Bob needs to read the subliminal message is the same information Alice needs to sign the innocuous message. If this is the case, Bob can impersonate Alice. He can sign messages purporting to come from her, and there is nothing Alice can do about it. If she is to send him subliminal messages, she has to trust him not to abuse her private key.

Other subliminal channel implementations don't have this problem. A secret key shared by Alice and Bob allows Alice to send Bob subliminal messages, but it is not the same as Alice's private key and does not allow Bob to sign messages. Alice does not have to trust Bob not to abuse her private key.

BEST AVAILABLE COPY

DIGITAL AUDIO CARRYING EXTRA INFORMATION

W. R. Th. van Kester, L. M. van de Kerkhof and F. F. M. Zoiderfeld

Philips Research Laboratories
P.O. Box 80000
5600 JA Eindhoven, The Netherlands

ABSTRACT

A new technique is proposed which enables the inaudible addition of extra information to an audio signal. Full compatibility with present-day transmission and reproduction systems is guaranteed, as the resulting signal remains in the same format. When reproducing the new signal on such equipment there will be no perceptible difference. The extra information, however, can be retrieved by the use of additional signal processing. The technique of adding and retrieving extra information is described and applications are presented. Special attention is given to the so-called 4:2:4 coding, as the technique presented offers a very promising scheme for such a coding.

INTRODUCTION

The proposed technique is based on the masking effect [1]. Masking is the psycho-acoustic phenomenon which deals with the insensitivity of the human ear to sounds in the presence of other, louder sounds. It is usually explained in terms of an upward shift in the hearing threshold, which is then referred to as the masking threshold. Masking is most effective for frequencies close to the frequency of the masking sound, but extends to both lower and higher frequencies, diminishing more rapidly to the lower than to the higher end. The same holds for the time characteristics: masking is strongest for sounds occurring simultaneously, but is also observed in the time spans shortly before and after the presentation of the masking sound.

A direct consequence of the masking effect is that it allows the inaudible addition of extra information to an audio signal. The inaudibility is guaranteed if the sound power level of the added signal is kept below the masking threshold.

In order to obtain a system carrying out such an addition, a method is required that adapts the extra information in the frequency and time structure of the audio signal in such a way that the masking rules known from psycho-acoustics are satisfied. Of course, the addition must be performed in such a way that the retrieval of the extra information is also possible. This paper proposes such a method.

The techniques on which the method is based are quite similar to those used in subband coding systems [2], see Fig. 1. The signals are filtered by a filter bank into subband signals, on which the addition operation is subsequently performed. After addition, the resulting subband samples are synthesized to a broadband signal. This signal will be perceived as the original audio signal. The extra information is retrieved by applying the retrieval operation to the subband signals, which have first been obtained by splitting the broadband signal.

The principle behind the addition and retrieval operation is the quantization of the (subband) samples. It is the quantizing that makes it possible to add another signal in such a way that it can also be recovered, by applying the same quantizing to the signal which has resulted after the addition; the extra information is identified as the "quantizing noise".

The resulting broadband signal can be represented in format according to present standards. So full compatibility is guaranteed and the signal can be transmitted and reproduced by the conventional systems. There will be no perceptible difference from the original audio signal if the power of the error signal is kept below the masking threshold. The error signal consists of two main components, namely the added signal and the error signal which is solely due to the applied quantization.

In order to receive the extra information as well, extra processing is required. This processing consists of filtering the broadband signal into subband signals again, quantizing these subband signals and specifying the quantization noise, which represents the information required.

In the next sections the method will be outlined in more detail. Subsequently, some applications will be presented. The concluding section summarizes the presented ideas.

ADDITION AND RETRIEVAL

The masking audio signal will be referred to as the main signal (M), the information to be added as the auxiliary signal (A). In order to clarify the addition and retrieval mechanism it is assumed that the auxiliary signal is itself an audio signal. Moreover, the auxiliary and main signal are assumed

CH2647-2/90/0000-1007 \$1.00 © 1990 IEEE

BEST AVAILABLE COPY

to exhibit some correlation. Based on these assumptions the method can be explained as follows:

Because the masking properties of a signal are dependent on both its time and frequency structure, the audio signals M and A are first filtered into subbands, see Fig. 1. To make a suitable choice of the bandwidths of these subbands a trade-off has to be made between benefiting from the masking effect and the resulting technical complexity [2]. The analyzing and synthesizing filters are required to be (nearly) perfect-reconstructing [3].

As in subband coding [2], the power of the main signal in each subband is estimated. Based upon these estimates, the maximal signal level which can be masked in each subband is determined. Next, the subband components of the main signal are quantized according to these calculated levels. The quantizing should be such that the resulting quantizing noise together with the added information will be masked by the main signal. The quantizing operation is described by

$$Q(\text{sample}) = \text{qstep} \cdot \text{ROUND}(\text{sample}/\text{qstep}) \quad (1)$$

where sample represents the value of the sample being quantized, $Q(\text{sample})$ its value after the quantizing, and qstep the step size according to which the sample is quantized. Clearly, if the signal has a large masking capability, a large value for qstep can be assigned. In fact, the quantizing is the principal step by which it is possible to add and retrieve information. After quantizing, the main signal's subband-samples can only be integer multiples of qstep . Consequently, the samples' values are allowed to be changed by adding any value in the range $(-\frac{1}{2}\text{qstep} \leq \Delta \leq \frac{1}{2}\text{qstep})$, as they can be recovered by applying the quantizing operation again. What is more, the added value can then be determined as well, as it appears as the difference between the changed and requantized value, see Fig. 2. Clearly, this value is going to represent the auxiliary signal.

The resulting subband signals are synthesized to a broadband signal prior to transmission. Because of its compatibility it can be reproduced by the equipment currently in use. There will be no perceptible difference. The extra information can be retrieved by adding extra processing circuitry to this equipment. This extra processing consists of filtering the signal into subband signals again and determining the added values by applying the quantizing operation Eq.(1). For the sake of clarity it should be noted that the "transmit" action in Fig. 3 also represents the synthesizing and analyzing filtering.

The quantizing can be interpreted as the addition of a noise signal with a power given by [4]

$$\frac{(\text{qstep})^2}{12} \quad (2)$$

Similarly, the addition representing the auxiliary signal contributes to the noise in the main signal. It is reasonable to

suppose that the upper bound of the power of this addition is also given by Eq.(2). As the addition and quantization noise are uncorrelated, a total power of at most twice the value expressed by Eq.(2) results as the noise power to be masked by the main signal.

The addition of the auxiliary signal to the main signal is to be performed by adding numbers with a value in the range $(-\frac{1}{2}\text{qstep} \leq \Delta \leq \frac{1}{2}\text{qstep})$. These numbers are obtained by attenuating the auxiliary signal sufficiently, see Fig. 2. The amount of attenuation depends on the strength of the auxiliary signal and on the available room qstep . As the main and auxiliary signal are correlated these two parameters are related as well, and the required attenuation factor can be obtained as follows.

When L levels are used to represent the main signal, L being an odd integer, the maximum absolute value of the main signal after quantization will be

$$\frac{L-1}{2} \text{qstep} \quad (3A)$$

So the largest possible value before quantization is given by

$$\frac{L}{2} \text{qstep} \quad (3B)$$

Assuming that the main and auxiliary signal are fully correlated, the values of the auxiliary signal samples will also range up to the maximum given by Eq.(3B). Consequently, the attenuation factor to be applied to the auxiliary signal results as

$$\gamma_{\text{min}} = \frac{\frac{\text{qstep}}{2}}{\frac{L}{2} \text{qstep}} = \frac{1}{L} \quad (4)$$

Because in practice the two signals are not fully correlated, some further attenuation, by a fixed amount of, for example, 0.80, should be applied to avoid quantize overload.

After attenuation (1) must be checked whether the resulting value is in the required range of a half qstep . If not, a clipping to $\frac{1}{2}\text{qstep}$ will be performed. Experiments have shown that quite a large number of clippings can be tolerated before they will become perceptible audibly. The reason for this is attributed to the masking properties of the auxiliary signal. Because the errors due to clipping are confined to the same frequency range and because they only occur at the large valued samples, they can be masked by the auxiliary signal.

In order to retrieve the auxiliary signal from a received (broadband) signal, first the filtering into subbands has to be applied. When, after quantizing the subband samples, the size of the added numbers are determined, these numbers have to be amplified to obtain the original strength of the auxiliary signal. The amplification factor is given by the in-

verse of Eq.(4), corrected for the amount of further applied oversampling. Synthesizing the resulting subband signals will finally lead to the retrieval of the auxiliary signal. Fig.3 depicts the total scheme of addition and retrieval in further detail.

DISCUSSION

In the foregoing it was assumed that the auxiliary signal was correlated with the main signal. For this case a scheme for the addition was presented. In the case of uncorrelated signals, however, it is still possible to add (and retrieve) both signals under the constraint that only one of them can be perceived. In that case, we consider the auxiliary signal as an arbitrary bit stream representing some information. It is, of course, apt to first apply a data-reduction algorithm [2] to the auxiliary signal before adding it to the main signal.

Depending on the room available at a certain moment, a number of bits can be added to the main signal. The available room is determined by q_{step} (Eq.(1)). The group of bits to be added at that instant are transformed into a number, e.g. '101' is transformed into '5'. Next, the number is scaled so that it fits into the range $(0, q_{step})$. So, in the given example a scaling by $q_{step}/8$ is to be applied. This scaling parameter directly indicates how the number of bits which can be added depends on the size of q_{step} . Finally, a shift over $-5q_{step}$ is applied, so that we arrive at a number which is in the range $(-5q_{step}, +5q_{step})$. The further processing continues as described in the previous section for correlated signals.

In the paper the filtering is assumed to be performed according to a subband scheme, as we believe that such a scheme offers the best results obtainable in a technical implementation. As far as the ideas described are concerned, however, the choice of the actual frequency-selective scheme is of no importance.

Concerning the filter banks there is a point which requires consideration. In order to reduce the system's complexity, multirate filter banks are used. Such filter banks show a time-variant behavior with a period of the largest down sampling factor. Perfect-reconstruction-type filter banks are designed in such a way that this time variance is not noticeable at the input and output terminals. Here, input and output terminals refer to the usual filter-bank configurations, which is the configuration in which the input and output signals are in the broadband format having the highest sample rate. In our case, however, the other configuration is used as well, i.e. the configuration of filter banks which synthesize subband signals at their input in a broadband signal and subsequently split this broadband signal into subband signals again. In fact, the "transmit" action in Fig.2 represents this configuration.

With respect to this new configuration, the filter banks are required to be (nearly) perfect-reconstructing as well. This requirement is automatically met by the perfect-reconstruction condition for the usual configuration. This can be seen by considering the cascade of an analyzing, a synthesizing and again an analyzing filter bank. Because the

filters are designed so that the two broadband signals in this cascade are equal, the subband signals at the input of the synthesizing filter bank should be equal to those at the output of the second analyzing filter bank.

The time-variant behavior should also remain unnoticeable in the new filter-bank configuration (i.e. synthesizing followed by analyzing). This is only achieved if we ensure that the total delay is an integer times the sampling period at the lowest sampling rate, or equivalently, when expressed in sampling periods at the highest sampling rate, if the total delay is an integer times the highest downsampling factor. In other words, it is necessary to synchronize the downsamplers in the analyzing filter bank at the retrieval (receiver) site with the upsamplers in the synthesizing filter bank at the addition (transmitter) site.

On the other hand, when no up- and downsampling is applied, the time-invariance condition will be satisfied, at the expense, however, of automatically fulfilling the perfect reconstruction demand. Because of the bandpass properties of the filters in the filter bank this demand can only be satisfied when the subband signals are sampled at their critical rate, because in this case the bandwidth of the bandpass filter matches that of any conceivable subband signal (Remind that due to the processing the spectrum of the subband samples is extended over the total available bandwidth given by the sampling rate).

APPLICATIONS

The applications of this new technique are manifold. It is convenient to make a classification of the information to be added according to its representation: if it is a number (correlated) audio signal or if it is simply representing data (bits). Different processing strategies are required in each case. Audio signals are to be divided into correlated and uncorrelated signals. As mentioned in the previous section, uncorrelated auxiliary signals are to be considered as a bit stream of data and processed accordingly. The processing of correlated signals was described in the main section of the paper. The data can be, for example, extra features (control data). Examples of correlated signals are an anechoic recording and a dummy-head recording.

A very convincing application of this new technique concerns the so-called 8-2-4 coding. Nowadays movies often have four audio channels. Up to now for use at home in TV sets the signal has been constrained to two channels, as the room available for transmission does not allow more. For this reason the original four signals are mixed into a stereo signal, thereby nullifying the 4-channel sound sensation. To overcome this problem, the mixing is usually performed by some kind of matrixing by which it is possible to retrieve some impression of the original four channels [5].

With the technique presented, however, it is now possible to generate a 2-channel signal which is fully compatible with the mixed stereo signal, but which can also be converted into the original 4-channel version. The following matrix can be used to mix the original four signals L , R , C and S

BEST AVAILABLE COPY

$$M_1 = L + \frac{1}{\sqrt{2}}(C + S), \quad (5A)$$

$$M_2 = R + \frac{1}{\sqrt{2}}(C + S), \quad (5B)$$

$$A_1 = \frac{1}{\sqrt{2}}(C + S), \quad (5C)$$

$$A_2 = \frac{1}{\sqrt{2}}(C - S). \quad (5D)$$

The signals M_1 and M_2 compose the new left and right stereo signals respectively. In addition, they each serve as a main signal to carry one of the (auxiliary) signals A_1 or A_2 . As expressed by Eqs.(5), the main and auxiliary signals are correlated, and consequently the described addition and retrieval algorithms for such signals can be applied.

Listening to the resulting signals produces the sensation that the pure M_1 and M_2 are being transmitted. By applying the necessary additional processing, the auxiliary signals A_1 and A_2 can be retrieved. By subsequently executing the inverse matrix operation of Eqs.(5) we will finally arrive at four signals which exhibit the same perceptual experience as the original four. Note that, besides the much better channel resolution obtainable with this coding scheme, the composition of the compatible stereo signal out of the four original signals is done in a much more attractive way than in other 4-2-4 coding schemes [5,6].

The performance of a real-time version of such a 4-2-4 coding system confirmed our expectations, demonstrating its power as well as the improvement obtainable compared with the mixing procedures in use until now.

SUMMARY

A new technique, based on the masking effect, is proposed which enables the inaudible addition of extra information to an audio signal. It opens the way to a whole new area of extensions for audio and/or video with audio, while remaining compatible with present-day standards.

As a major application of this new technique a new 4-2-4 coding scheme is presented, having an increased channel resolution. The scheme offers full compatibility with present 2-channel transmission and reproduction systems, while through the incorporation of extra processing it also provides the possibility of reproducing the original 4-channel sound sensation.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to Dr. W.F. Druyvesteyn, who first came up with the idea of information addition, and to Dr. R.N.J. Veldhuis, who offered the basic algorithms for its realization. His careful reading of the manuscript was of great assistance and was greatly appreciated.

REFERENCES

- [1] E. Zwicker, R. Feldtkeller, *Das Ohr als Nachrichtenempfänger*, S. Hirzel Verlag, Stuttgart, 1967.

- [2] R.N.J. Veldhuis, M. Breuwer and R. van der Waal, *Subband coding of digital audio signals*, Philips J. Res. 44 (1989) 329-343.
- [3] M. Yetterli und D. LeGall, *Perfect reconstruction FIR filter banks: some properties and factorizations*, IEEE Trans. ASSP 37 (1989) 1057-1071.
- [4] N.S. Jayanti and P. Moll, *Digital coding of waveforms*, Prentice-Hall, Englewood Cliffs, NJ, 1984.
- [5] S. Julstrom, *A high-performance surround sound process for home video*, J. Audio Eng. Soc. 35 (1987) 536-549.
- [6] J.M. Eargle, *Multichannel stereo matrix systems: an overview*, J. Audio Eng. Soc. 19 (1971) 552-559.

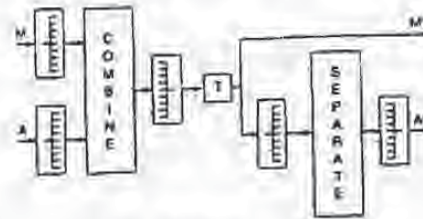


Fig. 1. General block diagram

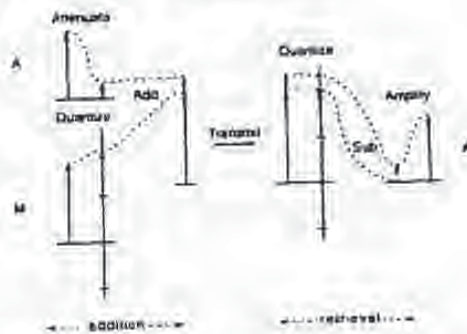


Fig. 2. The process of 'addition' and 'retrieval'

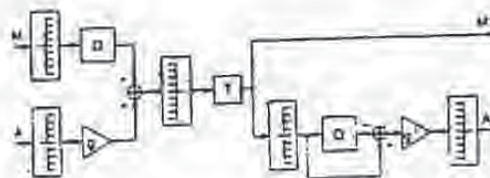


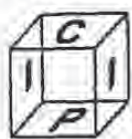
Fig. 3. Total scheme

3A 688

12

PROCEEDINGS

ICIP-94



Volume II of III

November 13 - 16, 1994
Austin Convention Center
Austin, Texas

Sponsored by

The Institute of Electrical and Electronics Engineers Signal Processing Society



IEEE

SER. REC. LIBRARY
FEB 08 1995
U.C. DAVIS



IEEE Computer Society Press
Los Alamitos, California

Washington • Brussels • Tokyo

BEST AVAILABLE COPY

K 4188



IEEE Computer Society Press
 10662 Los Vaqueros Circle
 P.O. Box 3014
 Los Alamitos, CA 90720-1264

Copyright © 1994 by The Institute of Electrical and Electronics Engineers, Inc.
 All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyright Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and this paper. It reflects the authors' opinions and, in the interests of timely dissemination, are published as presented, without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society Press, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Press Order Number 6950-02

Library of Congress Number 94-78171

IEEE Catalog Number 94CH35708

ISBN 0-8186-6950-0 (paper)

ISBN 0-8186-6951-9 (microfiche)

ISBN 0-8186-6952-7 (case)

Additional copies may be ordered from:

IEEE Computer Society Press
 Customer Service Center
 10662 Los Vaqueros Circle
 P.O. Box 3014
 Los Alamitos, CA 90720-1264
 Tel: +1-714-831-8380
 Fax: +1-714-831-4641
 Email: cs.books@compjnet.org

IEEE Service Center
 445 Hoes Lane
 P.O. Box 1331
 Piscataway, NJ 08855-1331
 Tel: +1-908-981-1393
 Fax: +1-908-981-9667

IEEE Computer Society
 13, Avenue de l'Aquilon
 B-1200 Brussels
 BELGIUM
 Tel: +32-2-770-2198
 Fax: +32-2-770-8505

IEEE Computer Society
 Daikoku Building
 2-10-1 Minami-Aoyama
 Minato-ku, Tokyo 107
 JAPAN
 Tel: +81-3-5409-3118
 Fax: +81-3-5408-3323

Editorial production by Bob Werner
 Printed in the United States of America by Braun-Brumfield, Inc.



The Institute of Electrical and Electronics Engineers, Inc.

K 4189

A DIGITAL WATERMARK

R.G.van Schyndell(*), A.Z.Tirkel(+), C.F.Osborne(*)

(*) Department of Physics, Monash University, Clayton, 3168, Australia.

(+) Scientific Technology, 21 Walrab St, E. Brighton, 3187, Australia.

ABSTRACT

This paper discusses the feasibility of coding an "undetectable" digital watermark on a standard 512x512 monochrome image with an 8 bit gray scale. The watermark is capable of carrying such information as authentication or authorization codes, or a legend essential for image interpretation. This capability is envisaged to find application in image logging, copyright enforcement, counterfeit protection, and controlled access. Two methods of implementation are discussed. The first is based on bit plane manipulation of the LSB, which offers easy and rapid decoding. The second method utilizes linear addition of the water mark to the image data, and is more difficult to decode, offering inherent security. This linearity property also allows some image processing, such as averaging, to take place on the image, without corrupting the water mark beyond recovery. Either method is potentially compatible with JPEG and MPEG processing.

1. INTRODUCTION

The art/science of hiding messages is known as steganography [1]. Conventional techniques involve the encryption of a copyright message on one colour of a composite image. The method described in this paper relies on the manipulation of the LSB of any colour or monochrome image, as a message which is undetectable to the eye. The embedded message is retrieved and can be removed from the modified image in order to recover the original information. The desirable properties of an electronic water mark are undetectability and accurate recovery of the hidden message. In general, the problem of embedding an invisible watermark and its subsequent extraction falls into the category of matched or adaptive filtering [2]. The authors have developed a simple modification of such a scheme. In order to render the watermark undetectable, encoding with *m*-sequences was chosen, because of their balance, random appearance and good auto-correlation properties (a single peak with no sidelobe), which simplify the recovery process [3]. In practice, extended *m*-sequences were employed, being commensurate with the image size (2^m) and exhibiting a null in autocorrelation around the main peak [4]. Two dimensional analogues such as Costas Arrays were studied, but were rejected because of their sparse nature [5]. For simplicity, we have chosen to encode the water mark by the choice of *m*-sequence phase. (An alternative method could use the choice of *m*-sequence to determine the data bytes). This paper demonstrates the feasibility of such encoding and the accuracy of the message extraction.

2. M-SEQUENCES

M-Sequences can be formed from starting vectors by a Fibonacci recursion relation, which can be implemented by linear shift registers. They are of maximal length (2^m-1) for a vector of length *m*. The sequences thus formed (or the polynomials by which they can be generated) form a finite field called Galois Field. The autocorrelation function and spectral distribution of *m*-sequences resemble that of random Gaussian noise. The cross-correlation of *m*-sequences has been examined mathematically and empirically in [6], [7] and [8]. Certain families of sequences (maximal cross-correlation) have been known to possess desirable cross-correlation properties [9]. Images encoded with *m*-sequences of one bit Gaussian noise are statistically indistinguishable from each other and only visually distinguishable from the original if the image contains large areas with a small information variation. In many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence its sacrifice is of limited significance. The exact choice of code depends on the amount of data to be embedded, the error involved in image transmission, and the degree of security required [10]. The Monash group has performed extensive analysis of *m*-sequence codes and their correlations [3]. The vulnerability of *m*-sequences to cracking is characterised by their span (2^{*m*}), which is the dimension of the matrix which must be diagonalised in order to determine the shift register configuration [3]. In the case of the linear addition of the *m*-sequence to the image LSB, the code cracker must know the image content without errors in order to determine the encoding sequence. The span of these sequences can be increased by forming compound codes (Gold or Kasami) or by performing non-linear mappings, such as in the GMLV sequences [2]. The number of available sequences varies according to the operations performed. Also, it is possible to utilise other sequences of the de Bruijn type, such as Legendre sequences, based on residues, and extremely difficult to crack [11].

3. METHODS OF INCORPORATING THE WATER MARK

Our experiments were conducted on 512x512 8 bit gray scale images encoded on a line by line basis with *m*-sequences 2^m pixels long. The first method involves the embedding of the *m*-sequence on the LSB of the image data. The original 8 bit gray scale image data is capable of compression to 7 bits by adaptive histogram manipulation. This process is followed by a compensating mapping

K 4190



reflect the dynamic range, the resulting image is practically indistinguishable from the original. The above process enables the LSB to carry the watermark information. The watermark can be detected by comparing the LSB in pixels with a stored watermark. The watermark message can be carried by the choice of sequence (or its complement) and its position. A watermark equivalent of the streamer is shown in Fig. 1. The second method uses LSB addition for embedding the watermark. As a result, the decoder is more complex, as shown in Fig. 2. The decoding process makes use of the unique and optimal auto-correlation function of m-sequences. The process requires the examination of the complete bit pattern, and in current implementation, must therefore be performed offline, which is its principal disadvantage. However, it is intrinsically more secure, since a potential code breaker has to perform the same operations, without any a-priori knowledge. The decoding process is not completely error free, due to partial correlation of the image data with the encoding sequence. This may be suppressed by a deliberate compression of the image dynamic range followed by a compensating mapping of the lookup table, which leads to gray scale quantization effects. Analysis of the image histogram indicates that a 3 bit dynamic range compression (from 8 bits down to 5 bits) should permit acceptable detection to be successful. Alternatively the application of a longer sequence of length 2^{10} or better filtering or detection algorithms should have a similar effect. Since the auto-correlation peak is typically very sharp, superimposed on a significant, but slowly varying background it is possible to employ simple filtering techniques to extract it. Various length impulse response filters were tested in single and multi-pass configurations. The differential filter (with kernel $[-1, -1, 3, -1, -1]$) was found to yield optimum results for 512×512 images with a $m=31$ sequence. The separation of the image autocorrelation histogram into image and message peaks shown in Fig. 3(a) and (b) demonstrate the feasibility of using thresholding on the autocorrelation values as a simple and rapid technique of message detection. The possibility of false positives and false negatives was also investigated in terms of the effect the image content has on the auto-correlation function. The effects of adding two distinct messages to the same image each encoded using a different m-sequence and then added to the image was investigated in terms of their effect on each other and their recovery ability. Such an image could contain two watermarks: one for the hospital, and one for the radiologist. Fig. 4 shows some images in which the water mark has been added. The composite image of Fig. 4(a) has been changed so that of Fig. 4(b) with the addition of the water mark, with a enlarged detail shown in 4(c). The cross-correlation after filtering of the image is shown with (above) and without (below) the watermark in Fig. 4(d). The peaks are visible as a series of single white dots in the lower right portion of the figure, whose position determines the message length (in this case the message is "radiocctAABBCC" repeated four times). This suggests that the water mark is undetectable only in circumstances where low-level gaussian noise is expected. Typically this does not include computer generated images.

4. APPLICATIONS

The objectives of this project are to investigate the feasibility of embedding undetectable watermarks for the purposes of image integrity verification, tagging and copyright infringement protection and controlled image access. The anticipated applications include medical images, commercial photographs and videos, sensitive documents such as patents, artwork, and computer generated images.

5. FUTURE WORK

The authors are investigating LMS adaptive filter extraction algorithms to determine an optimum technique with minimal image dependence. We will explore the effects on the watermark due to cropping and distortions such as skew, rotations, translations etc. and nonuniformities against these. These may include bit-swapping or diagonal raster folding of sequences into m-arrays [17]. These operations are facilitated by our choice of extended m-sequences of length 2^p . The desirability of unique-residual watermarks could be a function of the application. Some implementations may be better served by retaining a distorted watermark as evidence of the illegal act! This aspect requires further study.

6. CONCLUSIONS

This paper examines the feasibility of embedding a digital water mark on test images. The main problems found with adding the water mark is in retaining the dynamic range of the original image and the auto-correlation output. The paper discusses a method which would avoid the sacrifice of the LSB for the insertion of the sequence, and the ramifications on image processing and compression. The techniques used and contemplated for watermark coding and detection are all compatible with hardware implementation in standard (i.e. programmable gate array IC's) such implementation would be capable of on-line, real time algorithm execution.

7. ACKNOWLEDGEMENT

The authors would like to express their gratitude to Mr. G.A.Rankin for his assistance in developing a program to generate and analyze the sum and cross-correlations of m-sequences and related codes, which has proved invaluable in this project.

8. REFERENCES

- [1] E.Sapwater and K.Wood "Electronic Copyright Protection", Photo-Electronic Imaging, vol 37, No.6, (1994), p.16-21.
- [2] B.Widrow, "Adaptive Signal Processing", Englewood Cliffs, N.J. Prentice Hall, 1985.
- [3] M.K. Simon, J.K.Omura, R.A.Scholtz, & K.Levin, "Spread Spectrum Communications" Volume III, Potomac Md. Computer Science Press, 1983.



K 4191

[4] U.-C. G. Felby "Auto- and Cross-correlation Properties for Extended m-Sequences and Related Sequences" IEEE USTA Symposium, Dohi, Fouad, July 4-6, 1994, p.406-410.
 [5] S.W. Golomb, H. Taylor "Construction and Properties of Costas Arrays" Proc. IEEE, vol.72, p.1143-1163, Sept 1984.
 [6] Sarwate D.V., Pursley M.B. "Cross-correlation Properties of Pseudorandom and Related Sequences" Proc. of the IEEE vol.68, no 5, May 1980, pp 393-419.
 [7] Nish Y. "Multi-valued Cross-correlation Functions Between Two Maximal Linear Recursive Sequences" Ph.D. Dissertation, Department of Electrical Engineering, University of Southern California 1972.
 [8] A.Z. Tirkel, N.R.A. McC, C.F. Osborne, G.A. Rankin "Cross-Correlation Properties of M-Sequences" Paper Submitted to IEEE Transactions on Information Theory.
 [9] A.Z. Tirkel, C.F. Osborne, N. McC, G.A. Rankin, A. McAndrew "Maximal Connected Sets - Application to Microcell EDMA" International Journal of Communication Systems, 1994, vol 7, p.29-32.
 [10] A.Z. Tirkel, G.A. Rankin, R.H. van Schyndel, W.J. Ho, N.R.A. McC, C.F. Osborne "Electronic Water Mark" DOCTA-91 Macquarie University, Sydney, December 1991, p.666-672.
 [11] S. Kishiyoshi, T. Ozawa, M. Ham, "Property of the Legendre Subsequence" Communications on the Theory, ICCS-USTTA '92, Singapore, vol 3, p.1214-1228.
 [12] P.J. McWilliams and N.J.A. Sloane "Pseudorandom Sequences and Arrays" Proc IEEE(76), vol 64, p.1713-1729.

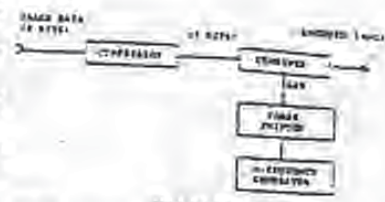


FIG 2 (a) ADDITIVE ENCODER



FIG 2 (b) ADDITIVE DECODER



FIG 2 (a) ADDITIVE ENCODER



FIG 2 (b) ADDITIVE DECODER

K 4192

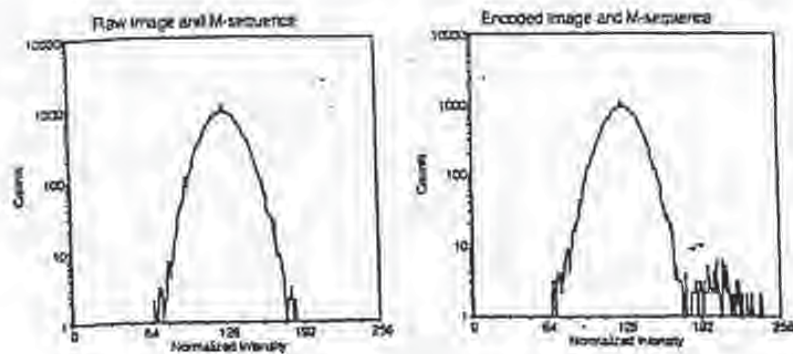


Fig. 3 (a)

Fig. 3(b)

Fig. 3 Histograms of the Cross-correlation of the Raw and Encoded Images with the Watermark M-Sequence

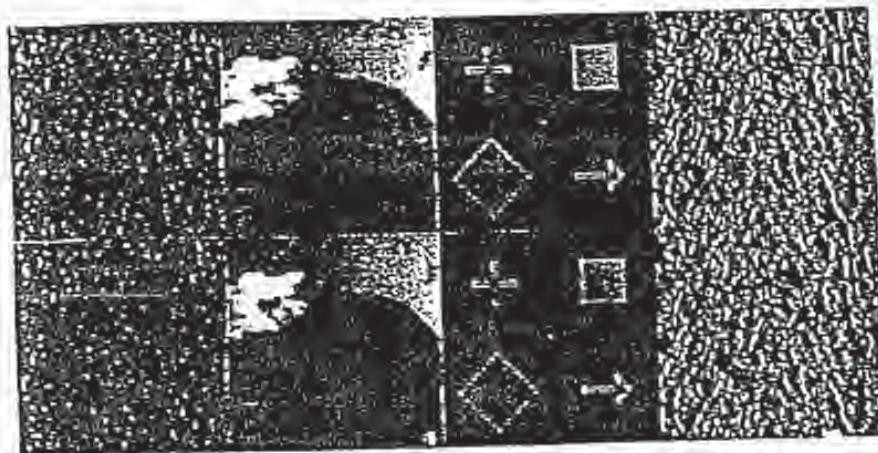


Fig. 4 (a) Upper - Unencoded Composite Image

Fig. 4 (b) Lower - Composite Image with Watermark (Undetectable)



Fig. 4(c) Detail of Binary Test Image Showing the Watermark (Enhanced Contrast)

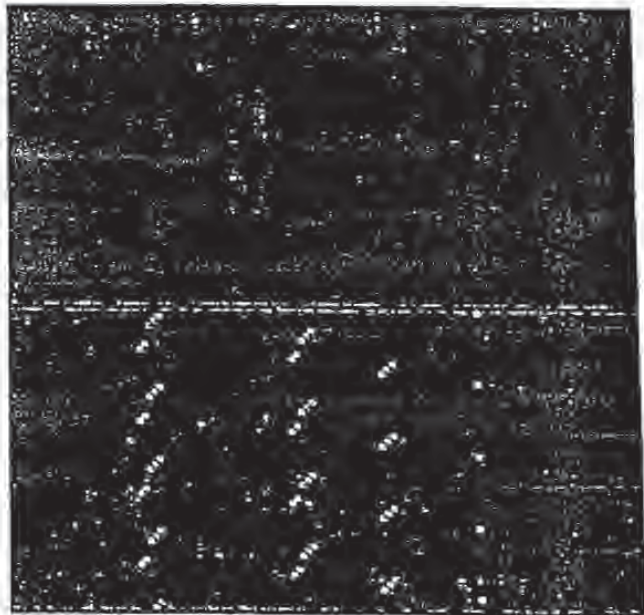


Fig. 4(d) M-Sequence Cross-Correlation with Raw Image (Upper), Encoded Image (Lower)
(Watermark Message Reads "asbbccAABBCC")

50

K 4194

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- EXCESSIVE DARK SPOTS
- UNREADABLE OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAYSCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

Ross Anderson (Ed.)

Information Hiding

First International Workshop
Cambridge, U.K., May 30 - June 1, 1996
Proceedings



(1)

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

BEST AVAILABLE COPY

12. E. Koch, J. Rindfery, and J. Zhao, Copyright protection for multimedia data. In *Proc. of the Int. Conf. on Digital Media and Electronic Publishing*, 1994.
13. E. Koch and J. Zhao, Towards robust and hidden image copyright labeling. In *Proceedings of 1993 IEEE Workshop on Nonlinear Signal and Image Processing*, June 1993.
14. F. T. Leighton and S. Micall, Secret-key agreement without public-key cryptography. In *Proceedings of Crypto*, 1993.
15. J.S. Lim, *Two-Dimensional Signal Processing*. Prentice Hall, Englewood Cliffs, N.J., 1990.
16. H. M. Mory and J.-J. Quinquere, Cryptology for digital tv broadcasting. *Proc. of the IEEE*, 82(5):644-657, 1994.
17. K. Matsui and K. Tanaka, Video-steganography. In *IMA International Property Privacy Proceedings*, volume 1, pages 187-206, 1994.
18. H. L. Picholtz, D. L. Schilling, and L. D. Milstein, Theory of spread spectrum communications - a tutorial. *IEEE Trans. on Communications*, pages 855-884, 1982.
19. W. F. Schreiber, A. E. Lippman, E. H. Adelson, and A. N. Murzavski, Reversible compatible colorant definition television system. Technical Report 3, MIT, 1955, United States Patent, 1991.
20. K. Tanaka, Y. Nakamura, and K. Matsui, Embedding secret information into a digital multi-level image. In *Proc. 1990 IEEE Military Communications Conference*, pages 216-220, 1990.
21. L. P. Turner, Digital data security system. Patent IPN W3 89/08915, 1989.
22. B. G. van Schriemel, A. Z. Tinker, and C. F. Osleron, A digital watermark. In *Int. Conf. on Image Processing*, volume 2, pages 86-90, 1994.

Modulation and Information Hiding in Images

Joshua R. Smith and Barrett A. Chaffin

[jrs, barrett]@media.mit.edu
Physics and Media Group
MIT Media Lab
20 Ames Street
Cambridge, MA 02139
USA

Abstract. We use concepts from communication theory to discuss information hiding schemes: the amount of information that can be hidden, its perceptibility, and its robustness to removal can be modeled using the quantization channel capacity, signal-to-noise ratio, and decoding margin. We then introduce new information hiding schemes whose parameters can easily be adjusted to trade off capacity, imperceptibility, and robustness as required in the application. The theory indicates the most appropriate feasible parameter settings. We also introduce a technique called *protection* for increasing resistance to JPEG compression. Analogous techniques are presumably possible whenever a model of anticipated distortion is available.

1 Introduction

In this paper, we discuss schemes for imperceptibly encoding extra information in an image by making small modifications to large numbers of its pixels. Potential applications include copyright protection, embedded or "in-band" captioning and indexing, and secret communication.

Ideally, one would like to find a representation that satisfies the conflicting goals of not being perceivable, and being difficult to remove, accidentally or otherwise. But because these goals do conflict, because it is not possible to simultaneously maximize robustness and imperceptibility, we will introduce a framework for quantifying the tradeoffs among these conflicting figures of merit useful for characterizing information hiding schemes: (1) capacity (the number of bits that may be hidden and then recovered) (2) robustness to accidental removal, and (3) imperceptibility. We will then present new information hiding schemes that can be tailored to trade off these figures of merit as needed in the particular application. For example, capacity may be more important in a captioning application, robustness may be most desired for copyright protection schemes, and imperceptibility might be favored in a secret communication

1.1. Information theoretic view of the problem

We view an image in which extra information has been embedded as an approximately continuous (in amplitude) two-dimensional, low-dimensional with large average noise power. The noise is the original unmodified image, which we will refer to as the cover image, and the signal is the set of small modifications introduced by the hider. The modifications occur in the embedded information. We will refer to the modified, distributed image as the stego-image. From this point the convention suggested at the Information Hiding Workshop, *cover* is the original image of view, any scheme for transmitting over a continuous channel. That is, any modulation scheme is a particular information hiding scheme, and concepts used to analyze these schemes, such as channel capacity, rate of signal points to noise power, and jamming margin can be invoked to quantify the trade-offs between the amount of information that can be hidden, the visibility of that information, and its robustness to removal.

1.2. Relationship to other approaches

In our framework, it becomes obvious why *cover image cover image* hiding schemes such as those presented in [CKLS] and [N0198] have high robustness to distortion. In cover image schemes, the extractor is required to have the original unmodified cover image, so that the original cover image can be subtracted from the stego-image before extraction of the embedded message. Because the cover image is subtracted off before decoding, there is no noise due to the cover image itself; the only noise that must be resisted is the noise introduced by distortion such as compression, printing, and scanning. While the image-crowd hiding schemes must respect the same information theoretic limits as ours, the noise in their case is very small, since it arises only from distortion to the stego-image.

In our view, image-crowd schemes are of limited interest, because of their narrow range of practical applications. Since the embedded information cannot be accessed by one who possesses the original, the embedded information cannot be used to extract and display a caption or "property of warning embedded in a downloaded image. The need to identify the original image before extraction also precludes oblivious, batch extraction. One might desire a web crawler or search engine to automatically find all illegal copies of any one of the many images belonging to, say, a particular photo archive, or all images with a certain embedded caption, but this is not possible with cover image-crowd schemes (at least not without involving computer vision). Finally, even assuming that the cover image has been identified and subtracted out, the proof value of such a watermark is questionable at best, since an "original" can always be constructed a posteriori in *any* image appear to contain any watermark. The only practical application of cover image-crowd schemes we have been able to identify is fingerprinting or tracing [16], in which many apparently identical copies of the cover image are distributed, but the owner wants to be able distinguish

The hiding methods presented in this paper are oblivious, meaning that the message can be read with no prior knowledge of the cover image. Other oblivious schemes have been proposed [W0301, Cor03], but the information-theoretic limits on the problem have not been explicitly considered. We make comparisons between our hiding schemes and those other oblivious schemes later in the paper.

In the next section, we will estimate the amount of information that can be hidden (with optimal robustness) in an image as a function of signal-to-noise ratio. The bulk of the paper is a derivation of some new hiding schemes that fall short but are within a small constant factor of the theoretical hiding capacity in the implementation of these schemes presented in this paper, we have chosen capacity over robustness, but we could have done otherwise. In the conclusion, we return to the discussion of modeling the trade-offs between hiding capacity, perceptibility, and robustness using the quantities channel capacity, signal-to-noise, and process gain.

2. Channel Capacity

By Nyquist's theorem, the highest frequency that can be represented in our cover image is $\frac{1}{2} \frac{1}{\text{pixel}}$. The band of frequencies that may be represented in the image ranges from $-\frac{1}{2} \frac{1}{\text{pixel}}$ to $+\frac{1}{2} \frac{1}{\text{pixel}}$, and therefore the bandwidth W available for information hiding is $2 \times \frac{1}{2} \frac{1}{\text{pixel}} = \frac{1}{\text{pixel}}$.

For a channel subject to Gaussian noise, the channel capacity, which is an upper bound on the rate at which communication can reliably occur, is given by [SW04]

$$C = W \log_2(1 + \frac{S}{N})$$

Since the bandwidth W is given in units of $\frac{1}{\text{pixel}}$ and the base of the logarithm in 2, the channel capacity has units of bits per pixel. For some applications (particularly print) it might be desirable to specify the bandwidth in units of millimeter⁻¹, in which case the channel capacity would have units of bits per millimeter.

This formula can be rewritten to find a lower bound on the $\frac{S}{N}$ required to achieve a communication rate C given bandwidth W . Shannon proved that this lower bound is in principle tight, in the sense that there exist ideal systems capable of achieving communications rate C using only bandwidth W and signal-to-noise $\frac{S}{N}$. However, for practical systems, there is a tighter, empirically determined lower bound, given a desired communication rate C , and an available bandwidth W , a message can be successfully received if the signal-to-noise ratio is at least some small threshold factor α above the Shannon lower bound. The threshold α is greater than 1 and typically around 3. [Sho65]

$$\frac{S}{N} \geq \alpha \left(2^{C/W} - 1 \right)$$

The information hiding, $\frac{S}{N} < 1$, so $\log_2(1 + \frac{S}{N})$ may be approximated as $\frac{S/N}{1 + S/N}$ or about $1/4 \frac{S}{N}$ [Sho65]. Thus $\frac{S}{N} \geq \frac{4}{3} \alpha \frac{C}{W}$. So in the low signal-to-noise regime

equivalent to information hiding, channel capacity goes linearly with signal-to-noise.

The average noise power of two example cover images was measured to be 002 (in units of squared amplitude). For signal powers L, A , and n (amplitude²), the channel capacity figures are 1.6×10^{-3} bits per pixel, 0.1 and n (amplitude²), the and 1.4×10^{-3} bits per pixel, in an image of size 320×320 , the upper bound on the number of bits that can be hidden and reliably recovered is then 32000. In our cover image of this size, then, using gain factors of 1, 2, and 3 (up to 6 of amplitude), the Shannon bound is 160 bits, 600 bits, and 1400 bits. With a bandwidth factor of $n = 3$, we might realistically expect to hide 30, 210 or 450 bits using these signal levels.

3 Modulation Schemes

In the modulation schemes we discuss in this paper, each bit b_i is represented by some basis function ϕ_i multiplied by either positive or negative one, depending on the value of the bit. The modulated message $S(x, y)$ is added pixel-wise to the cover image $N(x, y)$ to create the stego-image $I(x, y) = S(x, y) \oplus N(x, y)$. The modulated signal is given by

$$S(x, y) = \sum_{i=1}^n b_i \phi_i(x, y)$$

The basis functions will always be chosen to be orthogonal to each other, so that embedded bits do not equivocate:

$$\langle \phi_i, \phi_j \rangle = \sum_{x,y} \phi_i(x, y) \phi_j(x, y) = n \delta_{ij}^2$$

where n is the number of pixels and δ^2 is the average power per pixel of the carrier.

In the ideal case, the basis functions are also uncorrelated with (orthogonal to) the cover image N . In reality, they are not completely orthogonal to N ; if they were, we could hide our signal using arbitrarily little energy, and still recover it later.

$$\langle \phi_i, N \rangle = \sum_{x,y} \phi_i(x, y) N(x, y) \approx 0$$

For information hiding, basis functions that are orthogonal to typical images are needed; image coding has the opposite requirement: the ideal is a small set of basis functions that approximately spans image space. These requirements come in to conflict when an image holding hidden information is compressed: the ideal compression scheme would not be able to represent the carrier (bases) used for hiding at all.

The basis functions used in the various schemes may be organized and compared according to properties such as total power, degree of spatial spreading (or localization), and degree of spatial frequency spreading (or localization). We will now explain and compare several new image information hiding schemes, by

3.1 Spread Spectrum Techniques

In the spectrum-spreading techniques used in RF communications [Davis, SOSI, 04], spread-to-noise is traded for bandwidth: the signal energy is spread over a white frequency band at low SNR so that it is difficult to detect, intercept, or jam. Though the total signal power may be large, the signal to noise ratio in any band is small; this makes the signal when spectrum has been spread difficult to detect in RF communications, and, in the context of information hiding, difficult for a human to perceive. It is the fact that the signal energy resides in all frequency bands that makes spread RF signals difficult to jam, and embedded information locally that makes spread RF signals difficult to jam, and embedded information difficult to remove from a cover image. Compression and other degradation may have been distributed everywhere, some of the signal should remain. Thirdly, if the key used to generate the carrier is kept secret, then in the context of other wireline communications or data hiding, it is difficult for eavesdroppers to decode the message.

Three schemes are commonly used for spectrum spreading in RF communications: direct spread, frequency hopping, and chirp. In the first, the signal is modulated by a function that alternates pseudo-randomly between $+1$ and -1 , as multiples of a time constant called the chiprate. In our application, the elements in the pixel matrix. This pseudo-random carrier contains components of all frequencies, which is why it spreads the modulated signal's energy over a large frequency band. In frequency hopping spread spectrum, the transmitter rapidly hops from one frequency to another. The pseudo-random "key" in this case is the sequence of frequencies. As we will see, this technique can also be generalized to the spatial domain. In chirp spreading, the signal is modulated by a chirp, a function whose frequency changes with time. This technique could also be used in the spatial domain, though we have not yet implemented it.

3.2 Direct-Spectrum Spread Spectrum

In these schemes, the modulation function consists of a constant, integral-valued gain factor G multiplied by a pseudo-random block ψ of $+1$ and -1 values. Each block ψ has a distinct location in the (x, y) plane. In both variants of direct spread spectrum we have considered, the blocks ψ are nonoverlapping (and therefore mutually orthogonal); they tile the (x, y) plane without gaps. The cover image basis functions ϕ do not overlap in the x and y coordinates, so we do not need to worry about interference and can write the total power

$$P = \sum_{x,y} \sum_{\psi} G^2 \psi(x, y)^2 = \sum_{x,y} \sum_{\psi} (G \psi(x, y))^2 = (G^2 N)^2 = n G^2$$

(The definition holds in general, but the first equation only holds if the ψ tile the (x, y) plane without overlaps. Non-integral values of power can be implemented by "dithering": choosing step values

$$p \in \{-G\}, \{-G+1\}, \dots, \{-1\}, \{0\}, \{1\}, \dots, \{G-1\}, \{G\}$$

with probability $p(p)$ such that the average power $E^2 = \sum_y p(p)^2$.

The embedded image is recovered by demodulating with the original weighting function. A TRUE (+) bit appears as a positive correlation value; a FALSE (-) bit is indicated by a negative correlation value. We have found the median of the maximum and minimum correlation values to be an effective decision threshold, though it may not be optimal for this scheme. In work at least one value of the embedded image must be TRUE and one FALSE, in the version of direct sequence data hiding presented in [Cor95], a similar problem is avoided by including 0(0) at the beginning of each line.

A more sophisticated scheme would be to use a "differential" representation in which each bit is hidden in two pixels and modulated with $(-1)^i$ to represent FALSE and $(1)^i$ to represent TRUE. Then to recover the message, each bit can be demodulated twice, once with $(-1)^i$ and once with $(1)^i$. Whichever correlation value is higher gives the bit's value. This dual rate scheme also has advantages for carrier recovery.

Bender et al.'s Patchwork algorithm [BEN91] for data hiding in images can be viewed as a form of spread spectrum in which the pseudo-random carrier is sparse (is mostly 0s) and with the constraint that its integral amplitude be zero enforced by explicit construction, rather than enforced statistically as in ordinary spread spectrum schemes.

In the Patchwork algorithm, a sequence of random pairs of pixels is chosen. The brightness value of one member of the pair is increased, and the other decreased by the same amount, δ ; in our terminology, this leaves the total amplitude of the image (and therefore the average amplitude) unchanged. To demodulate, they find the sum $S = \sum_{i=1}^n a_i - b_i$, where a_i is the first pixel of pair i , and b_i is the second pixel of pair i . Notice that because addition is commutative, the order in which the pixel pairs were chosen is irrelevant. Thus the set of pixels at which single changes are made can be viewed as the non-zero entries in a single two-dimensional carrier $\phi(x, y)$. Bender et al. always modulate this carrier with a coefficient $b = 1$, but $b = -1$ could also be used. In this case, the recovered value of δ would be negative. If the same pixel is chosen twice, in the original formulation of the Patchwork algorithm, the result is still a carrier $\phi(x, y)$ with definite power and bandwidth. This Patchwork can be viewed as a special form of spread spectrum (with extra constraints on the carrier), and evaluated quantitatively in our information-theoretic framework.

Pully Spread Version We have implemented a "fully spread" version of direct sequence spread spectrum by choosing a different pseudo-random ϕ_i for each value of i . This fully spreads the spectrum, as the second figure in the second column of Figure 2 shows. The figure shows both space and spatial frequency representations of the carrier using the modulated pseudo-random carrier, and the sum of the two, the spreading.

To extract the embedded message (to demodulate), we must first recover the carrier phase. If the image has only been cropped and translated, this can be accomplished by a two-dimensional search, which is simple but effective.

The point at which the cross-correlation of the step-weights and the carrier is maximized gives the relative carrier phase. We have implemented this brute force carrier phase recovery scheme, and found it to be effective. Rotation or scaling enable this to overcome with more general scenarios.

Once the carrier has been recovered, we project the message onto each basis vector ϕ_i :

$$a_i \ll D_i \phi_i \gg = \sum_{x,y} D(x,y) \phi_i(x,y)$$

and then threshold the a_i values. We have used the median of the maximum and minimum a_i values as the threshold value. Note that for this to work, there must be at least one $b_i = -1$ and one $b_i = +1$. Above we discussed more sophisticated schemes that avoid this problem. Figure 2 shows the original input to be embedded, the demodulated signal recovered from the step-weights, the threshold value, and the recovered original input.

Third Version This scheme is identical to the "fully spread" scheme, except that the basic pseudo-random sequence is used for each ϕ_i . The ϕ_i differ from one another only in their location in the (x, y) plane. Unlike the fully spread version, which is effectively a one-time pad, some information about the embedded text is recoverable from the modulated carrier alone, without a priori knowledge of the unmodulated carrier. This information appears as the interference in the spatial frequency plane of the modulated carrier visible in Figure 3. If a different carrier were hidden, the interference would look different. One advantage of this third scheme is that carrier recovery requires less computation, since the scale of the search is just the size of one of the ϕ_i files, instead of the entire (x, y) plane. Given identical transmit power, this scheme seems to be slightly more robust than the "fully spread" scheme.

These two spread spectrum techniques are resistant to JPE(G)G, if the modulated carrier is given enough power (or more generally, as long as the jamming margin is made high enough). With carrier recovery, the two direct sequence schemes are resistant to translation and some cropping. However, unlike the frequency hopping scheme that we will describe below, the direct sequence schemes functions are fairly localized in space, so it is possible to lose some bits to cropping.

Fourth Version In addition to simply increasing the signal to improve compression immunity, Figure 4 illustrates a trick, called *pre-rotation*, for increasing the robustness of the embedded information when it is known that the image will be, for example, JPEG compressed. We generate the pseudo-random carrier, then JPEG compress the carrier by itself (before it has been modulated by the embedded information and added to the cover image), and uncompress it before modulating. The idea is to run the compression routine to filter out in advance

all the power that would otherwise be lost later in the course of compression. From the gain can be increased if necessary to compensate for the power lost to compression. The new JPEGed carrier is invariant to further JPEGing using the same quality factor (except for small numerical artifacts).² Figure 4 shows both the space and spatial frequency representations of the JPEG compressed carrier. Note the suppression of high spatial frequencies. Using the same power levels, we achieved error-free decoding with this scheme, but had several errors using the usual fully spread scheme without the pre-distortion of the carrier. These anomalies in this are probably possible whenever the information carrier has a model of the type of distortion that will be applied. Note that the removal of pre-distortion cannot be applied to our next scheme, or to the version of direct sequence spread spectrum in [Conf5], because in these schemes carriers overlap in space and therefore interfere.

3.3 Frequency Hopping Spread Spectrum

This scheme produces perceptually nice results because it does not create hard edges in the space domain. However, its computational complexity, for both encoding and decoding, is higher than that of the direct sequence scheme.

Each bit is encoded in a particular spatial frequency, which bit of the sub-carrier message is represented by which frequency is specified by the pseudo-random key. In our first implementation of frequency hopping spread spectrum, however, we have skipped the pseudo random key, and instead chosen a fixed block of 16 low spatial frequencies, one spatial frequency for each bit. One advantage of the frequency hopping scheme over the direct sequence technique is that each bit is fully spread spatially; the bits are not spatially localized at all. This means that the scheme is robust to cropping and translation, which only induce phase shifts.

An apparent disadvantage of the frequency hopping scheme is that because the functions overlap in the space domain, the time to compute the modulated carrier appears to be kXY , where k is the number of bits, instead of just XY . The time required for the direct sequence scheme. However, the Fast Fourier Transform (more precisely, a Fast Discrete Cosine Transform) can be used to implement this scheme, reducing the time to $XY \log XY$. This is a savings if $\log_2 XY \ll k$. In our example, $\log_2 320 \times 320 = 16.6$ and $k = 100$, so the FFT is indeed the faster implementation.

Figure 5 illustrates the frequency hopping modulation scheme. The results shown in figure 6, are superior to the direct sequence schemes both perceptually

² By compressing the carrier separately from the image, we are breaking the JPEG algorithm as an operator that obeys a superposition principle, which it does in an approximate sense defined in the Appendix.

³ It should be apparent from the description of JPEG compression in the Appendix that the output of the JPEG operator (or more precisely, the operator consisting of JPEG followed by inverse JPEG, which maps an image to an image) is an eigenfunction with in fact a fixed point of that operator, ignoring small numerical artifacts.

and in terms of robustness to accidental removal. There is little need to threshold the output of the demodulator in this case. However, summing and decoupling require significantly more computation than:

This scheme never needs "spatial JPEGing" with no pre-distortion, as illustrated in figure 7.⁴

A disadvantage of this scheme for some purposes is that it would be relatively easy to intentionally remove the embedded message, by applying a spatial filter at the appropriate frequency. A more serious implementation of the scheme would separate the frequencies from one another, to make this sort of filtering operation more difficult. The main disadvantage of this scheme relative to the direct sequence scheme is that, even using the FFT, its computational complexity for encoding and decoding is greater ($XY \log XY$ rather than XY).

4 Discussion

We have suggested that information and communication theory are useful tools both for analyzing information hiding, and for creating new information hiding schemes. We showed how to estimate the signal-to-noise needed to hide a certain number of bits given bandwidth W . A shortcoming of our channel capacity estimate is that we used the capacity formula for a Gaussian channel, which is not the best model of the "noise" in a single hopper as a player at any of the frequency domain plots in the figures will reveal. The Gaussian channel has the same power at each frequency, but already these images do not, especially after compression. A more refined theory would use a better statistical model of the image channel, and would therefore be able to make better estimates of the signal-to-noise needed to hide a certain number of bits. This would also lead to better hiding schemes, since the signal energy could be distributed more effectively.

The scheme we have called "frequency hopping" is superior perceptually, and in terms of robustness to accidental removal, to the direct sequence schemes which we experimented. Direct sequence may be less vulnerable to intentional removal, and wins in terms of computational complexity.

Assuming that the Gaussian channel approximation discussed above is not too misleading, our capacity estimates suggest that there exist significantly better schemes than we have presented, capable of hiding several hundred bits in an image in which we hid our hundred. Hybrid modulation/encoding schemes such as

⁴ All the JPEG compression reported here was done in Plotinus using the "high quality" setting.

⁵ In fact, it is not possible to pre-distort in the frequency hopping scheme because the basic functions overlap; the resulting interference pattern depends strongly on the particular values of the bits being encoded. There is no single pattern into which we can project the superposition to recover the embedded data, we must (silently) project it onto a sequence of vectors, or (more sophisticated) use the FFT in other than the idea of pre-distortion, does not apply, at least not in the same way it did to the non-overlapping direct sequence schemes.

treble-tapping over a remaining route toward higher hiding densities, that better models of channel noise (the noise due to cover images themselves, plus channel) would lead immediately to better capacity estimates, and better hiding schemes.

In all the practical examples in this paper, we have tried to hide as much information as possible using a given signal-to-noise. However, varying signal-to-noise and bandwidth fixed, communication rate can instead be traded for robustness to jamming. The formulas known as jamming margin and processing gain in spread spectrum communication theory are helpful in capturing the nature of robustness.

Processing gain is the ratio $\frac{W}{B}$ of available bandwidth W to the bandwidth B actually needed to represent the message. Jamming margin, the useful measure of robustness, is the product of signal-to-noise and processing gain. If the actual signal-to-noise ratio is $\frac{S}{N}$, then the jamming margin or relative signal-to-noise ratio $\frac{S}{N}$ after demodulation is given by $\frac{S}{N} = \frac{W}{B} \frac{S}{N}$. So robustness may be increased either by increasing signal-to-noise (at the cost of perceptibility, as we will explain in more detail below), or by decreasing the size of the embedded message (the capacity), which increases the processing gain. For example, in the case of our direct sequence schemes, the processing gain increases when we hide fewer bits because each bit can be represented by a larger block. The Dvorkovskii hiding scheme referred to earlier sacrifices communication rate entirely (hiding just one bit) in order to buy as much robustness as possible.

Signal-to-noise ratio provides a rough estimate of perceptibility, because, all other things being equal, the higher the signal-to-noise, the more visible the modulated carrier will be. However, keeping signal-to-noise constant, some carriers—particularly those with mid-range spatial frequencies, on experience as far suggests—will be more perceptible than others. So the real test, instead of perceptibility is simply signal-to-noise ratio; a plausible refinement might be the integral over all spatial frequencies of the signal-to-noise as a function of frequency weighted by a model of the frequency response of the human visual system. Methods for quantifying visibility to humans might be a new theoretical avenue to explore, and developing systematic methods for minimizing the visibility of hidden signals is certainly a challenge to information hiding practice. The pre-distortion technique demonstrated in this paper can be viewed as a first step in this direction, in the sense that successful compression schemes comprise implicit, algorithmic models of the human visual system (the ideal compression scheme would encompass a complete model of the human visual system). It will be interesting to watch the development of information hiding schemes and their co-evolutionary "arms race" with compression methods in the challenging environment of the human visual system.

A. Approximate superposition property for JPEG operator

An operator \mathcal{O} always superimposes if $\mathcal{O}(f+g) - (\mathcal{O}f) - (\mathcal{O}g) = 0$. Each coefficient generated by the JPEG operator f is called $-1 \leq J(f+g) - (Jf) + J(g) \leq 1$. In other words, JPEGing a pair of images separately and then adding them yields a set of coefficients each of which differs by no more than one quantization level from the corresponding coefficient found by adding the images first and then JPEGing them (using the same compression parameters in both cases).

The proof is simple. For a gray scale image, the unquantized JPEG coefficients S_{ij} are found by expanding each 8×8 block in a cosine basis. The final quantized coefficients n_{ij} are found by dividing each S_{ij} by a quantization factor q_{ij} (where each q_{ij} is greater than zero, since the purpose of the JPEG experiment is to decrease the size), and rounding toward zero [10]:

$$n_{ij} = \left\lfloor \frac{S_{ij}}{q_{ij}} \right\rfloor$$

The error expansion in a linear operation, and therefore always superposition, as (as long as $q_{ij} > 1$) we need only show that for any real numbers f and g , $-1 \leq J(f+g) - (Jf) - (Jg) \leq 1$. Without loss of generality, we may take f and g to be non-negative and less than one, since the integer parts f' and g' of f and g satisfy $J(f+g) - (Jf) - (Jg) = 0$. So, for each n_{ij} and p_{ij} , $0 \leq f+g < 2$, $0 - 0 - 0 = 0$. If $1 \leq f+g < 2$ then $J(f+g) - (Jf) - (Jg) = 1 - 0 - 0 = 1$. Since $f+g < 2$, these are the only two cases. The case of f and g negative is analogous, yielding a discrepancy of either -1 or 0 . The discrepancy in the case that f and g have opposite sign is less than in the same sign case. Therefore each n_{ij} coefficient produced by the JPEG operator satisfies our approximate superposition principle, $-1 \leq J(f+g) - (Jf) - (Jg) \leq 1$. Since each n_{ij} coefficient has a discrepancy of $+1$, 0 , or -1 , each S_{ij} has a discrepancy of $\pm q_{ij}$, 0 , or $-q_{ij}$. Thus the total power of the deviation from superposition (in either the spatial frequency or pixel representation, by Parseval's theorem) is bounded above by $\sum_{ij} q_{ij}^2$. This explains why JPEGing the carrier separately from the cover image is a reasonable preliminary task.

Note that the more aggressive the compression (the larger the q_{ij} values), the larger the discrepancy, or deviations from superposition.

Acknowledgments

This research was performed in the laboratory of Neil Erdemliou. The authors thank him for his advice and support. The second author thanks Joe Anzalone for his support. We thank Walter Bender, Don Grubb, and the crew at the Future Consortium for introducing us to the problem of data hiding. We acknowledge the other members of the Physics and Media groups, especially Joe Paradise and Tom Zimmerman, for helpful conversations about multitone techniques. Maggie Orth made useful suggestions about the proof of the superresolution principle.

This work was supported in part by the MIT Media Lab's crew in the Future Consortium, a Motorola Fellowship, the Hewlett-Packard Corporation, Deric Corporation, MirraSoft, Compuq Computer Corporation, and the MIT Media Lab's Things That Think consortium.

References

[1] W. Bender, D. Grubb, and N. Erdemliou, "Technique for data hiding. In *Proceedings of the SPIE*, page 2430-2440, San Jose, CA, February 1991.

[2] M.F. Barnsley and L.P. Hunt, *Fractal Image Compression*. AE Peters, Ltd. Wellesley, Massachusetts, 1993.

[3] F.M. Boland, J.J.K. O'Ruanaith, and G. Denzelsberg, "Watermarking digital images for copyright protection. In *Proceedings, IEEE International Conference on Image Processing and its Applications*, Edinburgh, 1995.

[4] J. Cox, J. Killian, T. Leighton, and T. Shanon, "A secure, robust watermark for multimedia. This volume.

[5] *Digimarc Corporation*. Identification/authentication coding method and apparatus. U.S. Patent Application, June 1995.

[6] R.C. Dinn, *Spread Spectrum Systems with Commercial Applications*. John Wiley and Sons, New York, 1984.

[7] R. Pflumm, *Talks at Intel Labs*. This volume.

[8] T.J. Shepard, *Decentralized Channel Management in Scalable Multitone Spread-Spectrum Packet Radio Networks*. PhD thesis, Massachusetts Institute of Technology, July 1995.

[9] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, *The Spread Spectrum Communications Handbook*. McGraw-Hill, New York, 1994.

[10] G.E. Shannon and W.W. Weaver, *The Mathematical Theory of Communication*. The University of Illinois Press, Urbana, Illinois, 1949.

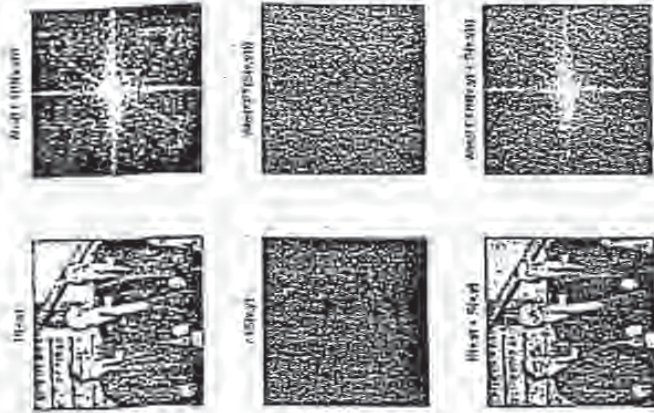


FIG. 1. "Fully Spread" version of direct sequence spread spectrum. The left column shows (from top to bottom) the three representations of the cover image, the individual carrier, and the spreading. The right column is the spatial frequency representation of the same three functions. The cover image has a bit of gray scale (0 - 255), and the power per pixel of this particular cover image, that is, the mean power per pixel, is 102.5. The carrier alternates between +2 and -2 in this figure, so the signal power per pixel is $2^2 = 4$. We have added a constant ϵ to the carrier to map the values into a positive gray scale.



FIG. 2. Demodulation of Fully Spread Scheme. Top: (0,1) bit input data from 10 to 1000. Second: demodulated values after demodulation. Third: threshold value. Bottom: Original input recovered by comparing demodulated values to threshold.

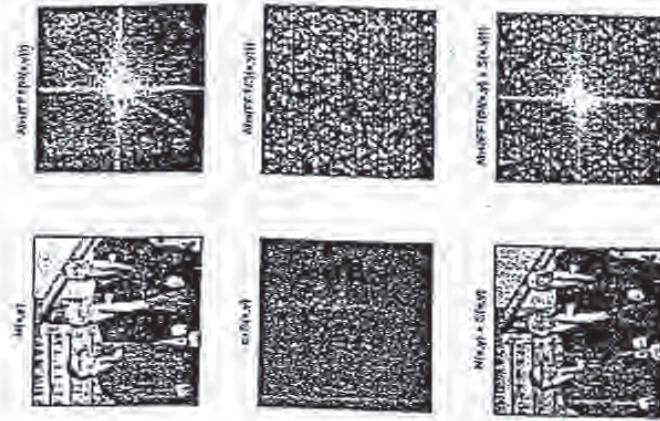


Fig. 3. Titled version of spread spectrum modulation scheme. Note the information in the spatial frequency view of the modulated carrier. As is the fully spread scheme, the noise power per pixel (the average power of the cover image) is 0.02, and the carrier ranges between +2 and -2, for a signal power of 1 per pixel.

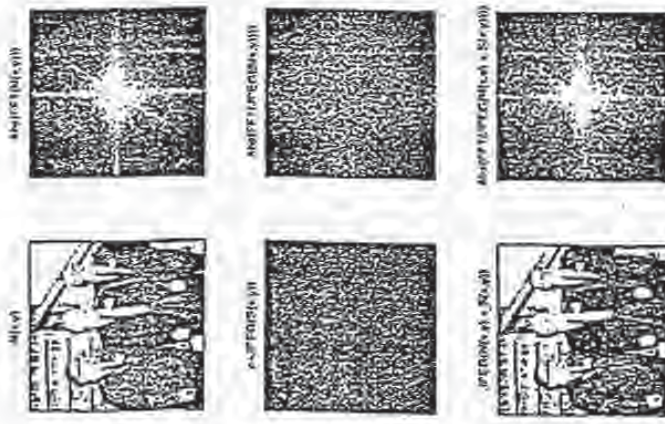


Fig. 4. Prediction of carrier for JPECC compression to compensate for distortion from anticipated JPECC compression. The usual direct receiver carrier has been compressed and resampled before being used in modulator and demodulator. JPECC compression of the same quality factor will not alter the carrier further. The original average carrier power was 16; after JPECCing the carrier by itself, the average carrier power dropped to 8.8.

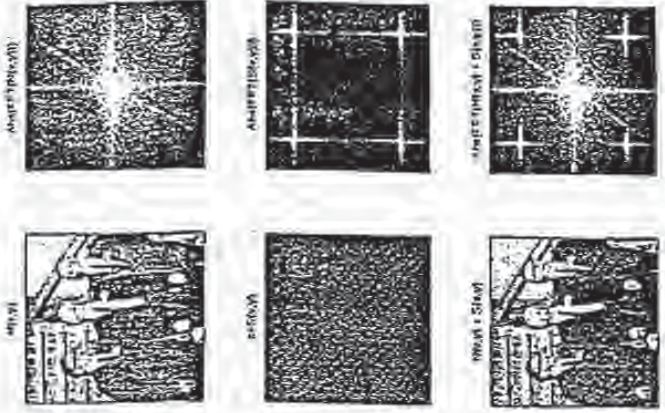


Fig. 5. Frequency hopping spread spectrum. Average signal power = 0.1 (units of amplitude squared), and average noise power = 0.02.



Fig. 6. Demodulation of Frequency hopping spread spectrum.



Fig. 7. Frequency hopping spread spectrum, with JPEG(100) step-impulse. The step-image S was created, JPEGed at high quality, uncompression, and then demodulated. To estimate the amount of signal lost in compression, we measured the average power of $\text{jpeg}(N + S) - N$ and found its value to be 5.6; the power in the carrier S was 0.1, as Figure 5 showed. The carrier shown for illustration purposes in the figure, labeled $e_s + \text{JPEG}(S(x, y))$, is in fact $\text{JPEG}(N + S) - N$. The carrier used to create the step-image was in fact $S(x, y)$.

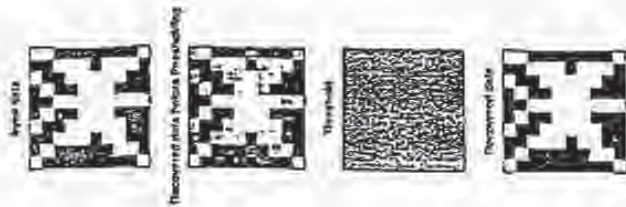


Fig. 8. Demodulation of Frequency Hopping spread spectrum, with jittered PRNG-image. The compression took its toll: contrast this output figure with the one from figure 6, which was so robust it needed no thresholding.

Watermarking Document Images with Bounding Box Expansion

Jack Brezina and Larry O'Grady

ljb|log|@bell-labs.com

Bell Laboratories
710 Mountain Ave.
Murray Hill, NJ 07972 USA

Imperceptible displacements of text objects has been shown to be a successful technique for hiding data in document images. In this paper we extend our earlier work to show how the height of a bounding box enclosing a group of text words can be used to increase the density of information hidden on a page. We present experimental results which show that bounding box expansions as small as 1/100 inch can be reliably detected, even after the distortions introduced by noisy image reproduction devices such as plain paper copiers. Digital watermarks based on this technique can be used with electronically disseminated documents for applications including copyright protection, authentication, and tagging.

1. Introduction

Traditional publishers seek access to the vast numbers of potential information consumers connected to computer networks such as the Global Internet. However, many information providers remain reluctant to distribute their intellectual property electronically, in part due to their concerns about the unauthorized redistribution of their copyrighted materials. We have previously proposed a collection of techniques to discourage unauthorized copying of document images [1]. These techniques use digital watermarks created by imperceptible displacements of text objects in document images. Many other research groups are also successfully studying the use of digital watermarks in various media, including text, color image, audio and video [2, 3, 4, 5, 6, 7, 8, 9, 10]. In addition, a number of software companies have initiated efforts to pursue commercial applications of watermarks [11, 12, 13, 14, 15].

In this paper we introduce a new scheme to watermark binary document images containing text. Each document recipient receives either a paper or electronic document containing a set of marks constituting a unique fingerprint [16]. Each mark corresponds to the expansion of the height of a logical "bounding box" enclosing a group of adjacent characters (i.e. a text block) on a line. A bounding box is the smallest rectangle that encloses the block. We show how to encode documents imperceptibly with bounding box expansions, and demonstrate that this hidden information can be reliably recovered from degraded document images.

In the next section we briefly review our previous approaches to watermarking document images. Section 3 details our new approach to encoding and decoding documents with bounding box expansions. We also discuss troublesome image effects that characterize "noisy" document reproduction devices, as well as our approach to circumventing these distortions. Section 4 presents experimental results that show that

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- EXCESSIVE LIGHT HEAVING
- DARK COLOURS, ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAYSCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

675

2

Digital Signature of Color Images using Amplitude Modulation

Martin Kutler

Signal Processing Laboratory, EPFL
1015 Lausanne Switzerland

Frédéric Jordan

Signal Processing Laboratory, EPFL
1015 Lausanne Switzerland

Frank Bosen

Signal Processing Laboratory, EPFL
1015 Lausanne Switzerland

ABSTRACT

Watermarking techniques, also referred to as digital signature, sign images by introducing changes that are imperceptible to the human eye but easily recoverable by a computer program. Generally, the signature is a number which identifies the owner of the image. The locations in the image where the signature is embedded are determined by a secret key. Doing so prevents possible pirates from easily removing the signature. Furthermore, it should be possible to retrieve the signature from an altered image. Possible alterations of signed images include blurring, compression and geometrical transformations such as rotation and translation. These alterations are referred to as attacks. A new method based on amplitude modulation is presented. Single signature bits are multiply embedded by modifying pixel values in the blue channel. These modifications are either additive or subtractive, depending on the value of the bit, and proportional to the luminance. This new method has shown to be resistant to both classical attacks, such as filtering, and geometrical attacks. Moreover, the signature can be extracted without the original image.

Keywords: Watermarking, digital signature, copyright, color image, geometrical attack, steganography

1. INTRODUCTION

The emergence of digital imaging and of digital networks has made duplication of original artwork easier. In order to protect these creations, new methods for signing and copyrighting visual data are needed. Watermarking techniques, also referred to as digital signature, sign images by introducing changes that are imperceptible to the human eye but easily recoverable by a computer program. Generally, the signature is a number which identifies the owner of the image. The locations in the image where the signature is embedded are determined by a secret key. Doing so prevents possible pirates from easily removing the signature. Furthermore, it should be possible to retrieve the signature from an altered image. Possible alterations of signed images include blurring, compression and geometrical transformations such as rotation and translation. These alterations are referred to as attacks.

BEST AVAILABLE COPY

Several watermarking algorithms have been developed in the past. Van Schyndel et al.¹ and Bender et al.² proposed a straightforward technique to sign gray scale images by adding a watermark image to the original image. A modification of the dithering rule was suggested by Matsui and Tanaka.³ Another approach is based on the modification of DCT coefficients within a JPEG or an MPEG encoder.⁴

The main drawback of these early techniques is the lack of robustness to attacks. More recently, a spread spectrum technique has led to significant improvements.⁵ Although it resists to filtering, it is vulnerable to geometrical attacks such as rotation, translation and image composition.

A new method based on amplitude modulation is presented. Single signature bits are multiply embedded by modifying pixel values in the blue channel. These modifications are either additive or subtractive, depending on the value of the bit, and proportional to the luminance. This new method has shown to be resistant to both classical and geometrical attacks. Moreover, the signature can be extracted without the original image.

This paper is structured as follows. Section 2 gives an overview of the new method. First the single embedding and retrieval of a single bit is described. This process is then generalized to multiple embedding of the same bit and to embedding of multiple bits. Section 3 describes how robustness to geometrical attacks is achieved. Section 4 shows some results and finally some conclusions are drawn in section 5.

2. ALGORITHM OVERVIEW

The main requirements for a digital signature are both invisibility to the human eye and robustness to alterations. To comply with the first requirement the signature is embedded in the blue channel, which is the one the human eye is least sensitive to. Also, changes in regions of high frequencies and high luminance are less perceptible, and thus favored. Robustness is achieved by embedding the signature several times at many different locations in the image.

First the single embedding and retrieval of a single bit is described. This process is then generalized to multiple embedding of the same bit and to embedding of multiple bits.

2.1. Single bit embedding

Let s be a single bit to be embedded in an image $I = (R, G, B)$, and $p = (i, j)$ a pseudo-random position within I . This position depends on a secret key K , which is used as a seed to the pseudo-random number generator. The bit s is embedded by modifying the blue channel B at position p by a fraction of the luminance $L = 0.299R + 0.587G + 0.114B$ as:

$$B_{ij} \leftarrow B_{ij} + (2s - 1)L_{ij}q \quad (1)$$

where q is a constant determining the signature strength. The value q is selected such as to offer best trade-off between robustness and invisibility.

2.2. Single bit retrieval

In order to recover the embedded bit, a prediction of the original value of the pixel containing the information is needed. This prediction is based on a linear combination of pixel values in a neighborhood around p . Empirical results have shown that taking a cross-shaped neighborhood gives best performance. The prediction B_{ij} is thus

These differences are then averaged:

$$\bar{\delta} = \frac{1}{|I|} \sum_i \delta_i \quad (5)$$

where $|I|$ is the number of pixels contained in image I .

The sign of the average difference $\bar{\delta}$ determines the value of the multiple embedded bit.

2.4. Extension to an m -bit signature

The extension to an m -bit signature $S = (s_0, \dots, s_{m-1})$ is straightforward: let p_1, \dots, p_n be the n positions selected for the multiple embedding of a single bit. For each of these positions a signature bit is randomly selected and embedded.

Given an $m-2$ bit string to be embedded, 2 bits are added to the string to form an m -bit signature. These two bits are always set to 0 and 1, respectively. There are two reasons to do so:

1. it allows to define a threshold τ which improves signature retrieval
2. it defines a geometrical reference which is used to counter geometrical attacks, such as rotation, cropping, translation

These items are further described in the next sections.

2.5. Adaptive threshold

Considering each difference δ^i that is used for information retrieval, the left graph in figure 2 clearly shows that the sign of δ^i is a very good decision function. However, the right graph suggests that after an attack, this is not so anymore. Therefore the decision function needs to be adapted. Since it is known that the two first bits of the signature have values 0 and 1, respectively, this information can be used to compute an adaptive decision threshold. This threshold is defined as the average between δ^0 and δ^1 :

$$\bar{\delta}^i = \begin{cases} 1 & \text{if } \delta^i > \frac{\delta^0 + \delta^1}{2} \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

3. ROBUSTNESS TO GEOMETRICAL ATTACKS

In order to resist to geometrical attacks, it is required for the recovering algorithm to be able to determine what operation (translation, rotation) has been applied to produce the tampered image. To estimate this transform, a reference is needed. The two first bits of the signature can fulfill this requirement. Since these bits always have the same value, a known pattern is hidden within the image. By looking for this pattern the transform can be found.

Let G be the transform applied to the signed image to obtain the tampered image J : $J = G(I)$. For now, it is assumed that the transform G is affine. Let (i, j) be the position of a pixel in I . The corresponding pixel in J

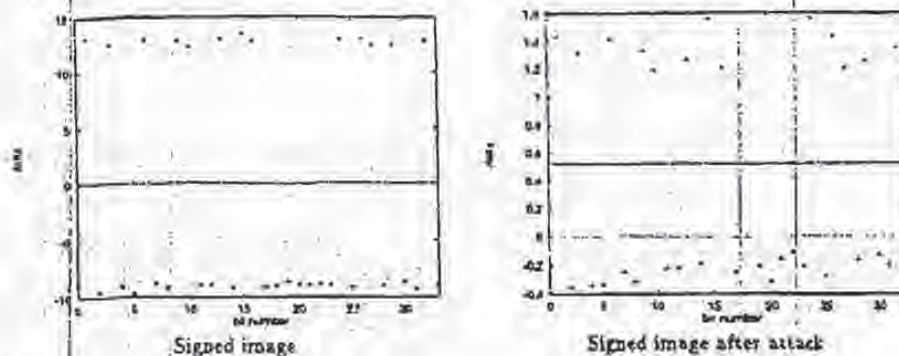


Figure 2: Behavior of δ^1 (δ) before and after an image attack (low pass filtering)

is at position (\tilde{i}, \tilde{j}) and is related to (i, j) by:

$$\begin{pmatrix} \tilde{i} \\ \tilde{j} \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & d \\ c & e & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} i \\ j \\ 1 \end{pmatrix} \quad (7)$$

where a, \dots, e are the transform parameters.

In order to retrieve the signature, the inverse G^{-1} of G is needed. By applying G^{-1} to J the image I is recovered and the signature can then be extracted.

The transform G^{-1} can be found by looking for the pattern created by the two first bits of the signature. Let H be an estimation of G^{-1} , and I_H the image obtained by applying H to J . Let's first suppose that H is equal to G^{-1} . The two first bits of the signature can clearly be retrieved from I_H . Also, the confidence of the retrieval is very high, that is the difference between δ^1 and δ^0 is maximum. Suppose now that H is slightly different from G^{-1} . The signature can still be retrieved but the difference between δ^1 and δ^0 is smaller than before. This difference gets smaller as the divergence between H and G^{-1} grows.

The difference can thus be used as an optimization criterion $q(H)$ defined as $q(H) = \delta^1(I_H) - \delta^0(I_H)$. As mentioned before $q(H)$ is maximal for $H = G^{-1}$. However the function $q(H)$ is not a smooth function. Optimization methods such as gradient descent would thus not be suitable. In this case full search methods have to be used.

The search can be sped up a lot if the nature of the transform G is given. For instance if it is known that the transform is a pure translation or rotation, the search space is greatly reduced.

4. RESULTS

To confirm the invisibility of the embedding process, an image (640 by 480 pixels, 24-bit color) with blue tones has been signed (see figure 3). For this particular image, the parameters have been set as follows: the signature S is 34 bit long and its value is the 32-bit number 1234567890 augmented by the two constant bits 0 and 1, the embedding density ρ is 0.55, the embedding strength is given by $\alpha = 0.1$, and the size of the crossed-shape window

if $r = 3$.

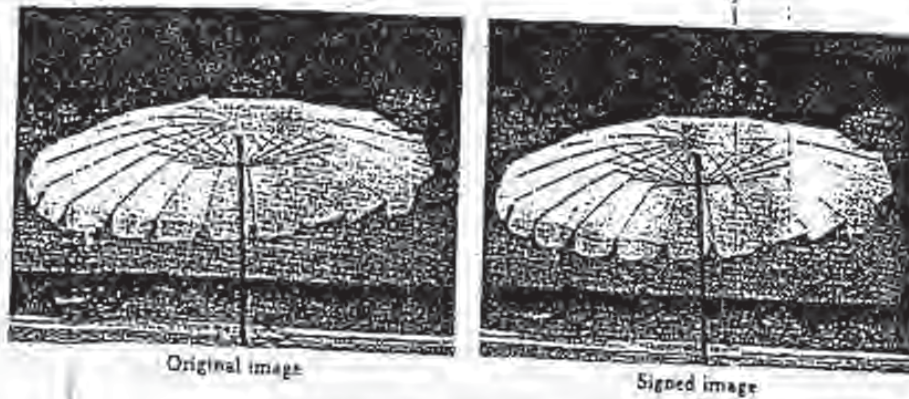


Figure 2: Invisible embedding of information

To verify the robustness of the proposed method, the signed image has been attacked in several ways, namely:

- blurring
- JPEG encoding/decoding
- rotation
- composition with another image

The next sections describe more precisely each of these attacks. Although in this document comprehensive results are only provided for these four attacks, the method has also shown to be resistant to other attacks including pixel spreading, pixelizing, color quantization, translation, cropping, and despeckling (median filtering).

4.1. Blurring

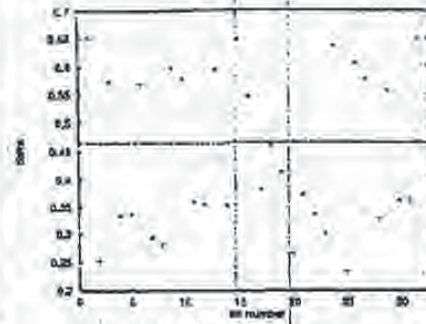
Figure 4 shows the signed image after blurring. The blurring function is as follows. Each color value is replaced by the average value of pixels within a 5 by 5 neighborhood.

The graph on the right hand side of figure 4 clearly indicates that the strength of the signature is much lowered by the attack. The average absolute difference between the I^s and the threshold τ goes down from about 10 before the attack (see figure 2) to about 0.1 after the attack.

Although the signature is correctly retrieved after the blurring, the limits of the proposed method appear. Indeed the I^s lies very close to the threshold and blurring the image even more would probably result in an erroneous signature retrieval. However the image quality would then also be much lower.



Blurred image



Retrieval quality

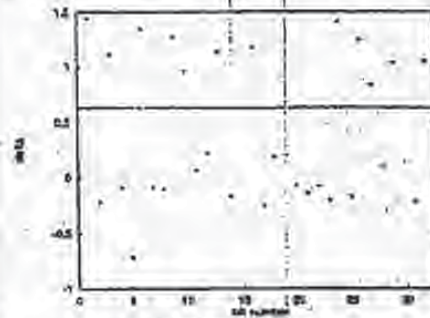
Figure 4: Simple image attack: blurring

4.2. JPEG encoding

Figure 5 shows the signed image after a JPEG encoding/decoding cycle. The quality factor for JPEG compression was set to 75 percent, which is the default value. Again the average absolute difference between the I^k and the threshold r is much lower than before the attack. However each I^k clearly lies on one of the sides of the threshold, and the signature can thus be correctly retrieved with great confidence.



Image after JPEG compression/decompression



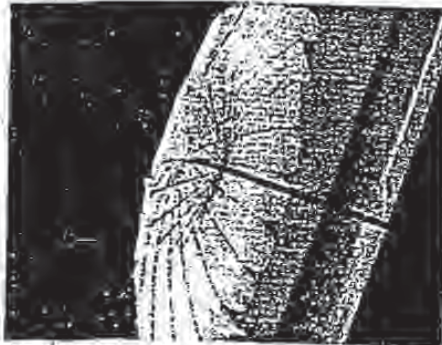
Retrieval quality

Figure 5: JPEG attack

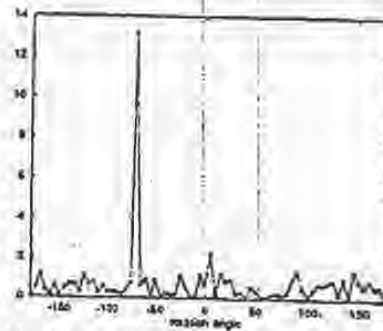
4.3. Rotation

To test the robustness of the proposed method against geometrical attacks, the signed image has been rotated to the left by an angle of 70 degrees (see figure 6). Considering that it is known that the attack is purely rotational, $q(H)$ is computed for every H defined as a rotation between 0 to 360 degrees, with increments of 5 degrees. The graph in figure 6 shows how the value $q(H)$ is affected by the angle. Clearly the optimum lies at -70 degrees, that

is, the amount by which the signed image was rotated. The signature can thus accurately be retrieved. Although a full search technique is used, the retrieval is still quite fast. Less than 20 seconds¹ were needed to do so.



The signed image rotated 70 degrees to the left



Searching for the transform: $q(H)$ as a function of the rotation angle

Figure 6: Geometrical attack: rotation

4.4. Composition with another image

Figure 7 shows an example of image composition. Given two signed images, each being signed with a different key, a third one is created by taking some pixels from the first one and some from the second one. This procedure can also be seen as a mixture of cropping and translation.

In this case, the algorithm is able to correctly retrieve both signatures given the appropriate keys.

5. CONCLUSION

A novel technique for image watermarking has been presented. The signing process has shown to be unnoticeable to the human eye. It has also been demonstrated that the signature is immune to a variety of attacks, including filtering, compression, and geometrical transforms. The resistance to the latter kind of attack without the need for the original image is the main improvement brought by this new method.

The proposed algorithm could be improved in several ways. First, all color channels could be exploited. The strength of the signature in each channel would be proportional to the sensitivity of the human eye to it. Also, robustness could be improved with the use of optimal error correcting codes. The current algorithm already features a primitive error correcting code based on the multiplicity of the embedding. However, it is well known that redundancy codes are far from optimality.

The authors would like to thank Vincent Vaerman for providing the images.

¹On a Sun Ultra 1 workstation

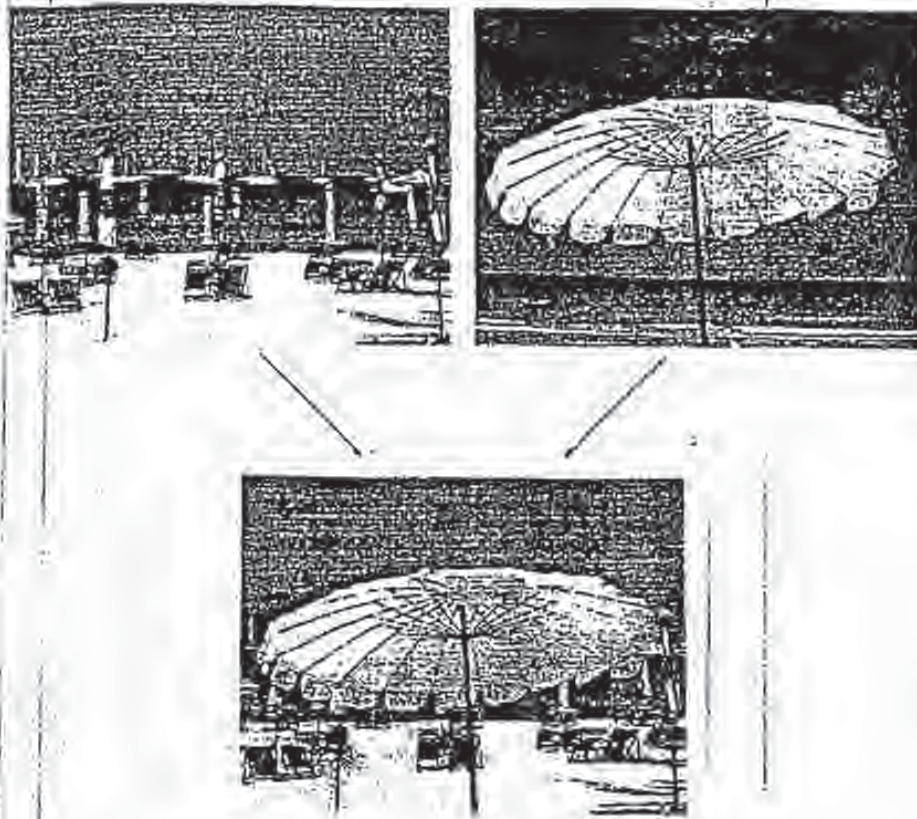


Figure 7: Composition example

6. REFERENCES

- [1] W. Bender, D. Gruhl, and N. Marmorato. Techniques for data hiding. In *SPIE*, volume 2420, February 1995.
- [2] S. Burgetts, E. Koch, and J. Zhao. A novel method for copyright labelling digitized image data. *IEEE Transactions on Communications*, September 1994.
- [3] J. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical Report 95-10, NEC Research Institute, 1995.
- [4] K. Matsui and E. Tanaka. Video-steganography: How to secretly embed a signature in a picture. *Journal of the Interactive Multimedia Association Intellectual Property Project*, 1(1):187-206, January 1994.
- [5] R.G. van Schyndel, A.Z. Tuzel, and C.F. Coborn. A digital watermark. In *1st IEEE International Conference on Image Processing*, volume 2, pages 85-90, 1984.

This document is copyrighted by SPIE. Additional copies, for internal or personal use only, are authorized subject to payment of a copying fee of \$6.00 per copy, payable to the Copyright Clearance Center (CCC), 222 Rosewood Drive, Danvers, MA 01923.

Other copying for republication, resale, advertising, or any form of systematic or electronic reproduction requires permission in writing from SPIE.

The CCC fee code for this paper appears on the first page of the document.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

IMAGE IS UNREADABLE

IMAGE IS UNRELIABLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

694

(3)

Using fractal compression scheme to embed a digital signature into an image

Joan Puare, Fred Jordan

Swiss federal institute of technology
Signal Processing Laboratory
CH-1015 Lausanne
Switzerland
Email: jordan@ltsig3.epfl.ch
Tel.: +41 21 693 70 89
FAX: +41 21 693 70 90

ABSTRACT

With the increase in the number of digital networks and recording devices, digital images appear to be a material, especially still images, whose ownership is widely threatened due to the availability of simple, rapid and perfect duplication and distribution means. It is in this context that several European projects are devoted to finding a technical solution which, as it applies to still images, introduces a code or Watermark into the image data itself. This Watermark should not only allow one to determine the owner of the image, but also respect its quality and be difficult to remove. An additional requirement is that the code should be retrievable by the only mean of the protected information. In this paper, we propose a new scheme based on fractal coding and decoding. In general terms, a fractal coder exploits the spatial redundancy within the image by establishing a relationship between its different parts. We describe a way to use this relationship as a means of embedding a Watermark. Tests have been performed in order to measure the robustness of the technique against JPEG conversion and low pass filtering. In both cases, very promising results have been obtained.

Keywords: digital signature, watermarking, image, copyright protection, security, fractal compression, IFS (Iterated Function Systems), FVT (Fractal Vector Technique), compression, internet

1. Introduction

1.1. The context

The last decades have seen exceptional developments in the field of multimedia systems. Hence, people's needs will probably become very dependent on this phenomenon, and in order that the true potentials of these systems be properly exploited, some security mechanisms for privacy and intellectual rights must be given.

In the case of the protection of still images, finding a general solution is particularly difficult. The increasing number of digital networks and recording devices makes it very easy to create, distribute and copy such material. For these reasons, the demand for technical solutions against piracy is rapidly increasing among creators of multimedia information.

1.2. Several approaches

Different approaches have been already presented, they all intend to face mainly format conversions, low pass filtering and data compression. Whereas some works are based on the direct modification of the pixels' luminance [1,2,3,7], some others make use of a predicted coding scheme [5] or a JPEG compression scheme [6]. In [4], the mark is embedded in the LSB (Least Significant Bit) of the pixels' values and in [8], the use of a frequency modulation is done. Also, some techniques have been developed for video data, which is the case of [9].

1.3. Our proposal

In the following we propose a novel approach to Watermarking, based on the fractal theory of iterated transformations. For an image to sign we will construct its 'fractal code' in such a way that the decoded one includes a signature. Therefore, the signing algorithm consists of a coding-decoding process and retrieving the signature will be performed as a fractal coder. A signature thus obtained will have the important characteristic of being undetectable without the appropriate key.

Through this paper, some general concepts related to fractal coding techniques will be first explained, followed by their practical applications to our coder and decoder. Afterwards, we will introduce the signing and retrieving techniques as well as some results, focusing mainly on their robustness against JPEG compression and Blurring (3x3 kernel) attack. Finally, new ideas and possible improvements to be performed will be discussed.

II. Fractal Image Coding

II.1. Some general concepts

The fractals theory has proved to be suitable in many fields and particularly interesting in various applications of image compression. First important advances are due to M. F. Barnsley who introduces for the first time the term of Iterated Function Systems (IFS) [10,11,12,13] based on the self-similarity of fractal sets. Barnsley's work assumes that many objects can be closely approximated by self-similarity objects that might be generated by use of IFS simple transformations. From this assumption, the IFS can be seen as a relationship between the whole image and its parts, thus exploiting the similarities that exist between an image and its smaller parts.

At that point, the main problem is how to find these transformations or, what is the same, how to define the IFS. There is, in fact, a version of the IFS theory, the Local Iterated Function Systems theory, that minimizes the problem by stating that the image parts do not need to resemble the whole image but it is sufficient for them to be similar to some other bigger parts in it.

It was Arnaud E. Jacquin who developed an algorithm to automate the way to find a set of transformations giving a good quality to the decoded images [14]. In Fractal coding methods based on Jacquin's work, the main idea is to take advantage of the fact that different parts of the image at different scales are similar. As a matter of fact, they are block-based algorithms that intend to approximate blocks of a determined size with contractive transformations applied on bigger blocks. However, in theory the shape of the segments to encode is nonrestricted.

II.2. The basic theory

The main idea of a fractal based image coder is to determine a set of contractive transformations to approximate each block of the image (or a segment, in a more general sense), with a larger block.

Some basic aspects of the theory are given in the lines below (a clear and brief explanation can be found in [15] and [16]):

Let's consider a metric space (E, d) where d is a given metric and E might be the space of the digital images. We can talk of a contractive transformation $B: E \rightarrow E$, when:

$$d(B(x), B(y)) \leq \alpha d(x, y), \quad \forall x, y \in E, \quad 0 \leq \alpha < 1$$

In this case, exists a point x^* such that:

$$B(x^*) = x^*$$

$$\lim_{n \rightarrow \infty} B^n(x) = x^*, \forall x \in E$$

This point is called a fixed point.

An IFS consists of a complete metric space (E, d) and a number of contractive mappings B_i defined on E . The fractal transformation associated with an IFS is defined as:

$$B(E) = \bigcup_{i=1}^N B_i(E)$$

where E is any element of the space of non-empty compact subsets of E .

If B_i is contractive for every i , then B is contractive and there is a fixed point for which:

$$A = B(A) = \bigcup_{i=1}^N B_i(A)$$

and

$$\lim_{n \rightarrow \infty} B^n(E) = A$$

A is called the *attractor* of IFS and the transformations are usually chosen to be affine.

Once B is determined, it is easy to get the decoded image by making use of the Contraction Mapping Theorem: the transformation B is applied iteratively on any initial image until the succession of images does not vary significantly.

However, given a set M , how to find a contractive transformation B such that its attractor A is close to M ?

To answer this question we have to apply to the *Collage Theorem*:

For a set M and a contraction B with attractor A :

$$h(M, A) \leq \frac{h(M, B(M))}{1 - s}$$

Where h is the *Hausdorff Distance*.

That is to say that we can guarantee that M and A will be sufficiently close if we can make M and $B(M)$ close enough.

In terms of B_i , and combining the two following expressions:

$$B(M) = M; \quad B(M) = \bigcup_{i=1}^N B_i(M)$$

we get

$$\bigcup_{i=1}^n B_i(M) = M$$

So, if we make a partition of M :

$$M = \bigcup_{i=1}^n m_i$$

then, m_i can be closely approximated by applying a contractive affine transformation B_i on the whole M :

$$m_i = B_i(M)$$

The theory of IFS was extended to Local IFS where each part of the image is approximated by applying a contractive affine transformation on another part of the image:

$$m_i = B_i(D_i)$$

where D_i is the bigger part from which m_i is approximated.

III. Algorithm description

The main idea to automate the searching of a Local IFS relies on a partition of the image in blocks of a fixed size, called *Range Blocks*. These blocks are then approximated from larger blocks, called *Domain Blocks*. The transformations normally applied on the Domain Blocks are contracting and luminance scaling and shifting. Some other isometric transformations are sometimes used.

We have used an algorithm based on Jacquin's work as the first step of the signing technique. In the following, a brief explanation of it is given.

III.1. Coder

Let O denote the image we want to encode. Let also O_r denote a partition of O in $n \times n$ blocks referred to as *Range Blocks (Rb)*. Similarly, O_d will denote another partition of O , this time in $2n \times 2n$ blocks or *Domain Blocks (Db)* in steps of $n \times n$ pixels. The goal of the encoding algorithm is to establish a relationship between O_r and O_d in such a way that any Rb can be expressed as a set of transformations to be applied on a particular Db. The transformations that have been considered are *Contraction*, *Isometric transformation* (one out of eight), *Luminance Scaling* and *Luminance Shifting*. For each Rb in O_r , denoted as Rb_i , the code will consist of a vector V_i and the appropriate transformations T_i , in such a way that:

- V_i has its origin in Rb_i and points to the correspondent Db_j , which now becomes its *Matching block (Mb_j)*.

- T_i if applied on Mb_j minimizes the Mean Square Error (MSE) with respect to Rb_i .

- The couple (V_i, T_i) is the best solution (in the sense of the MSE) within a local area surrounding Rb_i in which we search for Mb_j .

The region of O_d where the search of Mb_j is performed is commonly taken as a square region surrounding the Rb_i . We will name this region LSR (Local Searching Region). The use of such a shape in the Matching Block determination might be justified from spatial redundancies considerations and that is essentially true. But that does not mean that other shapes can not give more than acceptable results on the Ranges Blocks approximation. Next figure shows the square surrounding region and a possible alternative:



Fig. 1: (a) A square LSR and (b) an alternative solution.

As we will describe further down, the assumption of this property will allow to make of this point the basis of our Watermarking proposal.

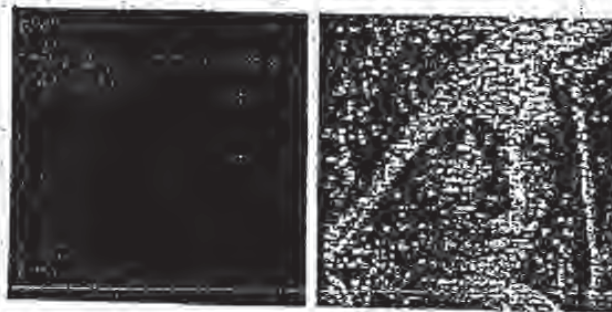
III.2. Decoder

Let's consider an initial image S with the only constraint that it has to be of the same size as O . As before, we consider a $n \times n$ -partition S_i in R_b , and a $2n \times 2n$ partition S_d in D_b . The decoding algorithm takes for each R_b -its Matching Block (pointed by V_i), applies on it the transformations (defined by T_i) and places the result back on R_b . These operations are performed for every R_b of S_i , and through some iterations (typically four). After each iteration a new image Q_i is obtained and it turns out that Q_i converges to O , according to the *Collage Theorem*. An important point is that the solution (V_i, T_i) obtained for O remains exactly the same for Q_i . That is to say that for every Range Block the same Matching Block as before is found. We will also take advantage of this point to embed the signature by a properly choice of the vectors V_i .

Figure 2 shows some iterations for image Lena, when S_0 has been taken as a black image, n being equal to 4.

Figure 3, on the other hand, shows some iterations for image Lena, S_0 being a black image and n equal to 8.

It can be observed a better quality when $n=4$, above all in those parts of great detail. However, for $n=4$ the compression rate is much lower than for the case $n=8$. Therefore, there is choice to be made between quality and rate of compression. An intermediate solution might combine 4×4 -Rangeblocks with 8×8 -Rangeblocks. A quadtree based algorithm might achieve this compromise.



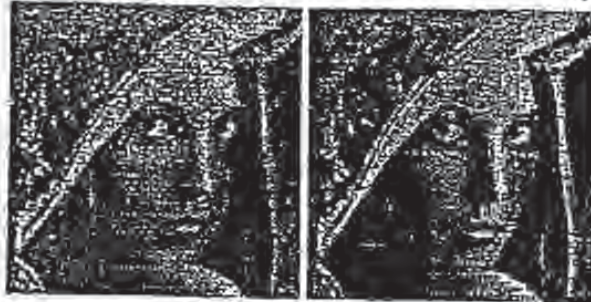


Fig. 2 Iterations 1,2,4 of a code for "Lena" applied on a gray image ($n=4$).

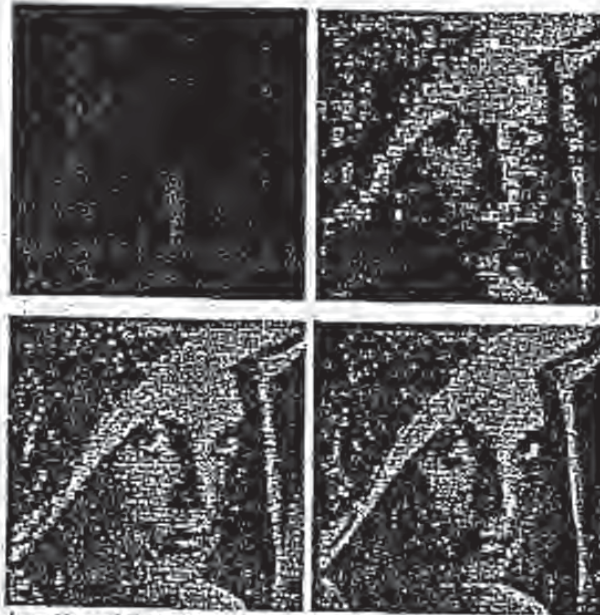


Fig. 3. Iterations 1,2,4 of a code for "Lena" applied on a gray image ($n=3$).

III.J. Signer

Signing an image consists of a coding-decoding process with variable searching regions. Let's consider two different LSR, A and B (Fig. 4), and a third one, C, defined as their union (a different choice of the regions could have been made, perhaps as a function of the characteristics of the image). Let also $S=(s_0, \dots, s_{31})$ be a 32-bit signature. We will embed every bit with a redundancy U . The coding process is as follows:

- For each bit s_i , U Range Blocks are randomly chosen and denoted by $\{Rb_i\}$. The random function used to get the blocks makes use of a 'seed' that should only be known by the user.
- If $s_i = 1$, $\{Rb_i\}$ is coded by searching for $\{Mb_i\}$ in regions $\{A_i\}$.
- If $s_i = 0$, $\{Rb_i\}$ is coded by searching for $\{Mb_i\}$ in regions $\{B_i\}$.
- The rest of Rb_i are coded by searching for Mb_i in $\{C_i\}$. Note that this would be the case for all Range Blocks in a non-signed image.

Then the decoding is performed as described above. The resulting image contains the signature.



Fig. 4: A range Block, its LSR, and its LSR_u. LSR_u is defined as their union.

III.4. Retriever

The whole fractal code of an image can be expressed as the union of every Range Block single code:

$$m = \bigcup_j (V_j, T_j)$$

Likewise, for an image Q obtained after an iterative application of μ on any initial image, we consider its fractal code π . Since, in Q , every Range block is not just an approximation to a transformed Domain Block but it is exactly a transformed Domain Block, it turns out that $\pi = \mu$.

Thus, we will be able to identify the signature by simply accessing the Range Blocks of Q defined by the 'seed' used when signing, recoding them and checking the values of V_j .

The rule to decide if a Range Block has been signed with a zero or a one, is the following one:

- If V_j belongs to region A_j , then a one has been embedded.
- If V_j belongs to region B_j , then a zero has been embedded.

In normal conditions, there ought to be a number of U recognition of bit one for those bits one in the signature, and of U recognition of bit zero for those bits zero in the signature.

To make the final decision there is a need of a threshold. It is going to be defined as the mean of the results obtained for bits two and three of the signature. Thus, they are always being embedded as a one and a zero respectively.

IV. Results

This section is divided in two parts. First one concerns the case for $n=4$, and second one the case for $n=8$. In both, the robustness to JPEG compression and to low pass filtering (3x3-kernel blurring) is discussed, as well as the quality of the signed images against the original and the non signed but fractal encoded.

All tests have been performed by embedding a 32-bits signature in 'Lena' image (256x256), then applying the retriever. The chosen signature has a value of one in even bits and zero in odd bits. The redundancy U is equal to 50 for the case $n=4$, and equal to 25 for the case $n=8$.

The LSRs have been defined as follows:

$$LSR_A \quad k \neq 6; \quad l \neq 6;$$

$$LSR_B \quad |k| \leq 5; \quad |l| \leq 5;$$

Where (k,l) are the coordinates of vector V.

Moreover, we have defined a parameter P as the ratio between the number of vectors found in region A and the redundancy U. Since each bit equal to one has been embedded in LSR A, parameter P will be equal to one for those bits. Parameter P will be equal to 0 for bits equal to 0 (which have been embedded in LSR B).

Finally, we need to have a new parameter to express the reliability of the retrieved signature. Let's name it by σ :

$$\sigma(\%) = \frac{\sum |P_i - \xi|}{1 * \xi} * 100, i = 0, \dots, l$$

where ξ is the threshold value and l is the length of the signature.

IV.1. Case n=4

Figure 5 shows, for a 'n' equal to 4, the original image 'Lena', the decoded image of 'Lena' with no signature, and the decoded image of 'Lena' with the signature. Both, the Peak to Signal Noise Ratio (PSNR) between original and signed image and that between original and non-signed image present a value higher than 31.5 dB.

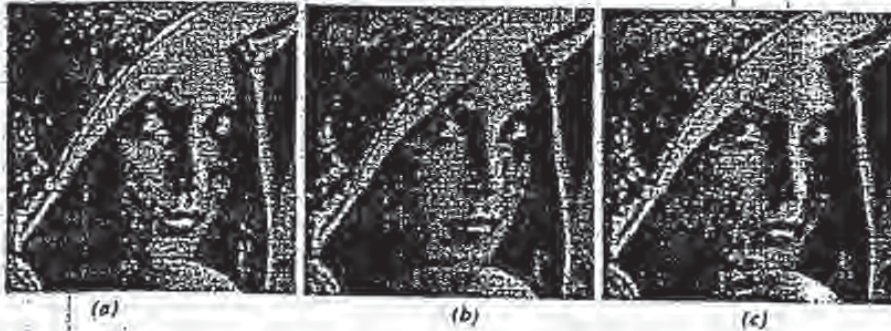


Fig. 5 : (a) Original 'Lena' image; (b) decoded image of 'Lena' with no signature; (c) decoded image of 'Lena' with the signature (n=4)

We have tested the robustness against JPEG compression qualities of 90, 75 and 50 %. Table 1 shows the results:

| | No JPEG | JPEG 90% | JPEG 75% | JPEG 50% |
|--------------------|---------|----------|----------|----------|
| P mean (even bits) | 0.985 | 0.672 | 0.457 | 0.351 |
| P mean (odd bits) | 0.00 | 0.099 | 0.18 | 0.219 |

| | | | | |
|--------------------------|------|------|------|------|
| Threshold ξ | 0.5 | 0.39 | 0.34 | 0.31 |
| Reliability σ (%) | 98.5 | 73.5 | 40.8 | 21.4 |
| Bits correctly retrieved | 32 | 32 | 32 | 29 |

Table I

IV.2. Case $n=8$

Figure 6 shows the original image 'Lena', the decoded image of 'Lena' with no signature, and the decoded image of 'Lena' with the signature. The PSNR between the original image and the non signed image presents a value of 25.82 dB (eighth iteration) whereas that between the original one and the signed decoded is equal to 25.40 dB (eighth iteration).

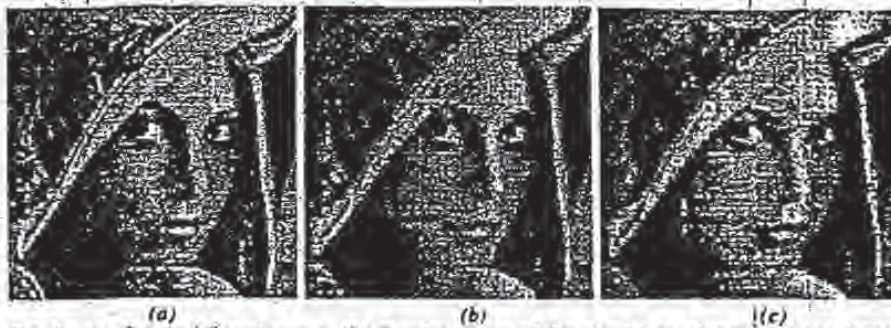


Fig. 6 : (a) Original 'Lena' image; (b) decoded image of 'Lena' with no signature; (c) decoded image of 'Lena' with the signature ($n=8$)

As before, we show in next table the behavior against JPEG compression. The same rates of quality have been tested:

| | No JPEG | JPEG 90% | JPEG 75% | JPEG 50% |
|--------------------------|---------|----------|----------|----------|
| P mean (even bits) | 0.992 | 0.962 | 0.887 | 0.797 |
| P mean (odd bits) | 0.00 | 0.002 | 0.035 | 0.097 |
| Threshold ξ | 0.5 | 0.52 | 0.48 | 0.46 |
| Reliability σ (%) | 99.25 | 92.3 | 88.8 | 77.2 |
| Bits correctly retrieved | 32 | 32 | 32 | 32 |

Table II

Table III shows the results when we have performed the tests of Table II but with a previous blurring on the signed image.

| | $n=4$ JPEG | JPEG 10% | JPEG 75% |
|--------------------------|------------|----------|----------|
| P_{mean} (even bits) | 0.662 | 0.642 | 0.567 |
| P_{mean} (odd bits) | 0.105 | 0.085 | 0.143 |
| Threshold ξ | 0.40 | 0.36 | 0.36 |
| Reliability σ (%) | 69.7 | 77.4 | 62.1 |
| Bits correctly retrieved | 32 | 32 | 32 |

Table III

V. Conclusions and Future Works

We have presented an algorithm which succeeds in making digital signature functionality by modifying fractal features of the image.

The presented results show a good behavior for JPEG compression when $n = 4$. In that case, the algorithm has proved to be able to retrieve correctly the signature up to a JPEG quality of 75 % with a reliability of 40.8 %. When the quality went down to a value of 50 %, the number of badly recognized bits of the signature was of only three, though the reliability was, in that case, of 21.4 %.

When $n = 8$, the robustness against JPEG compression has turned out to be pretty high even for a quality of 50 % (reliability equal to 77.2 %). The method would have probably proved to be robust to higher compression rates though at these stages JPEG images may become damaged.

Concerning low pass filtering, the tests that have been performed for $n = 4$, showed some weakness against blurring convolutions. But for $n = 8$, the technique appeared to be very robust, even when the blurring attack was followed by a JPEG compression. When the compression rate was of 75%, we were able to retrieve the signature with a good reliability ($\sigma = 62.1$ %).

For the case $n = 4$, the quality of the decoded images may be sufficient for some applications. However, the low complexity of the technique suggests that this quality can still be improved. On the other hand, new improvements ought to combine both cases, $n=4$ and $n=8$, in order to get either a good robustness against JPEG compression and low pass filtering and an acceptable level of quality. A quadtree-based algorithm seems promising as a mean to achieve this compromise. Indeed, a more advanced version of the actual work should take into account the statistics of the blocks where the signature is embedded.

A feature of this technique is that it does not allow, once the image has been decoded, to find out the location of the signature (in fact, it does not allow to determine whether a signature has been embedded or not). Since a Local Iterated Function Systems based algorithm looks for a set of transformations able to give a good approximation to the image to encode, it does not matter what these transformations are if the approximation is good enough. What the algorithm does, in fact, is to distinguish between different set of transformations by giving to one of them the feature of constituting a signature. Related to the last point would be the fact that we let totally opened the choice of searching regions shapes. The optimization of these shapes might increase the robustness of the signature as well as the retrieving reliability.

We think also that the *Fractal Vector Technique (FVT)* might be suitable in systems where images broadcasting needs a rate of compression similar to the one given by the fractal coding. Experiences have not shown great differences in quality between the decoded images either containing a signature or not. In effect, the degradation of the images comes mainly from the nature of the fractal method, not from the introduction of a watermark.

Finally, fractal compression scheme extracts several other parameters that might also be used to sign the image.

VI. References

- [1] J. Piate, F. Jordan, Two New Approaches to Digital Image Signature, *Diploma Project March 1996*.
- [2] C. de Soja, F. Jordan, Enhancement of a watermarking algorithm in order to increase resistance to JPEG compression, *Diploma Project March 1995*.
- [3] T. H. Kasbalis, J. Piate, Applying Signatures on Digital Images.

- [4] O. Bruyndonckx, J.-J. Quisquater and B. Macq. Spatial Method for Copyright Labeling of Digital Images.
- [5] Kineo Matsui, Kiyoshi Tanaka. Video-Steganography: How to Secretly Embed a Signature in a Picture.
- [6] S. Burgett, E. Koch, S. Zhao, A Novel Method for Copyright Labeling Digitized Image Data.
- [7] R. G. Van Schyndel. A Digital Watermark.
- [8] Ingemar J. Cox, Joe Kilian, Tom Leighton, Talal Shamooh. Secure Spread Spectrum Watermarking for Multimedia. *NEC Research Institute, Technical Report 95 - 10*.
- [9] T. Vynno, F. Jordan, Embedding a Digital Signature in a Video Sequence using Motion Vectors. *Submitted to ICIP 96*.
- [10] M. F. Barnsley. *Iterated function systems*. In R. L. Devaney, L. Keen, K. T. Alligood, J. A. Yorke, M. F. Barnsley, B. Branner, J. Harrison, and P. J. Holmes, editors, *Chaos and Fractals: The Mathematics Behind the Computer Graphics*. American Mathematical Society, 1989.
- [11] M. F. Barnsley. *Methods and apparatus for image compression by iterated function systems*. United States Patent Number 4, 941, 193, 1990.
- [12] M. F. Barnsley and S. Demko. Iterated function systems and the global construction of fractals. *Proceedings of the Royal Society of London*, A399: 243-275, 1985
- [13] M. F. Barnsley and L. P. HUD. *Fractal Image Compression*. AK Peters, Ltd., Wellesley, Massachusetts, 1993.
- [14] Jacquiri A. Image Coding Based on a fractal Theory of Iterated Contractive Image Transformations. *IEEE Transactions on image processing*, Vol1, pp 18-30. January 1992.
- [15] L. Torres, M. Kunt, Video Coding, The second Generation Approach.
- [16] Fisher, Y., *Fractal Image Compression: Theory and Application*. Spinger Verlag Edition, New York, 1995.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- EXACT COPY OF TOP BOTTOM OR SIDES
- EXACT COPY OF BACKSIDE
- BACKSIDE OR UNREADABLE FLAT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

693

6

Proceedings

INTERNATIONAL CONFERENCE ON
IMAGE PROCESSING

September 16 - 19, 1996

Lausanne, Switzerland

Sponsored by

The IEEE Signal Processing Society

Volume III of III

BEST AVAILABLE COPY

TRANSPARENT ROBUST IMAGE WATERMARKING

Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik

Department of Electrical Engineering
University of Minnesota, Minneapolis, MN 55455 USA
email: mswanson, binzhu, tewfik@ee.umn.edu

ABSTRACT

We propose a watermarking scheme to hide copyright information in an image. The scheme employs visual masking to guarantee that the embedded watermark is invisible and to maximize the robustness of the hidden data. The watermark is constructed for arbitrary image blocks by filtering a pseudo-noise sequence (author id) with a filter that approximates the frequency masking characteristics of the visual system. The noise-like watermark is statistically invisible to deter unauthorized removal. Experimental results show that the watermark is robust to several distortions including white and colored noises, JPEG coding at different qualities, and cropping.

1. INTRODUCTION

Digital images facilitate efficient distribution, reproduction, and manipulation over networked information systems. However, these efficiencies also increase the problems associated with copyright enforcement. To address this issue, digital watermarks (i.e., author signatures) are under investigation. Watermarking is the process of encoding hidden copyright information in an image by making small modifications to its pixels. Unlike encryption, watermarking does not restrict access to an image. Watermarking is employed to provide solid proof of ownership. To be effective, the watermark must be [1, 2]: perceptually invisible within the host media; statistically invisible to thwart unauthorized removal; readily extracted by the image owner; and robust to incidental and intended signal distortions incurred by the host image, e.g., filtering, compression, re-sampling, re-touching, cropping, etc.

In this paper, we introduce a novel watermarking scheme for images which exploits the human visual system (HVS) to guarantee that the embedded watermark is imperceptible. Our watermark is generated by filtering a pseudo-noise sequence (author id) with a filter

that approximates the frequency masking characteristics of the HVS. The image watermark is constructed by computing watermarks for individual image blocks. The blocks may be $n \times m$ or may be defined in terms of image objects/regions. This helps deter pirating of image objects. Furthermore, the noise-like watermark is statistically invisible. We include experimental results which indicate that the watermark is readily extracted and robust to common signal processing operations.

2. PREVIOUS WORK

The most common watermarking approaches modify the least significant bits (LSB) of an image based on the assumption that the LSB data are insignificant. Two LSB techniques are described in [3]. The first replaces the LSB of the image with a pseudo-noise (PN) sequence, while the second adds a PN sequence to the LSB of the data. Another LSB data hiding method called "Patchwork" [1] chooses n pairs (a_i, b_i) of points in an image and increases the brightness of a_i by one unit while simultaneously decreasing the brightness of b_i . Several executable software packages (e.g., Stego, S-Tools) based on LSB approaches are also available. However, any approach which only modifies the LSB data is highly sensitive to noise and is easily destroyed. Furthermore, image quality may be degraded by the watermark. Other watermarking approaches include [4, 5, 6].

A method similar to ours is presented in [7], where the authors hide data by adding fixed amplitude pseudo-noise to the image. The approach presented here employs masking to vary the amplitude of the hidden data. Specifically, the tolerable error levels obtained using masking provide us with the maximum amount the image data may change. Pseudo-noise techniques are also used in [2], where the N largest frequency components of an image are modified by Gaussian noise. However, the scheme only modifies a subset of the frequency components and does not take into account the HVS. The watermark we propose here embeds the maz-

This work was supported by AFOSR under grant AF/F49620-94-1-0461.

This document is copyrighted by the American Institute of Electrical and Electronics Engineers, Inc. All rights reserved. This document is intended solely for the personal use of the individual user and is not to be disseminated broadly.

0-7803-3268-7/95/00.00 © 1995 IEEE

NOT LISTED WITH CCC

211

BEST AVAILABLE COPY

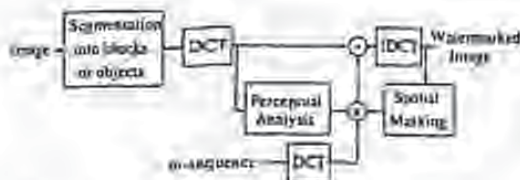


Figure 1: Diagram of new watermarking technique.

imum amount of information throughout the spectrum. Since more data is embedded, this scheme is guaranteed to be more robust to modifications than a technique which only modifies a subset of the image data.

3. WATERMARK GENERATION

In Fig. 1, we show our watermarking technique. The initial step consists of segmenting the image into blocks. Using a traditional approach, the blocks may be $n \times n$ (e.g., 8×8 like JPEG). An option at this stage is to segment the image into blocks of objects and texture regions. In either case, blocking the image adds detection robustness to cropping and localized signal processing operations. Upon applying a discrete cosine transform (DCT) to each block, a frequency mask is computed for each block in a manner similar to low bit rate coding algorithms [6]. The resulting perceptual mask is scaled and multiplied by the DCT of a maximal length pseudo-noise sequence (author id). Note that a different pseudo-noise sequence is used for each image block. This watermark is then added to the corresponding DCT block. The watermarked image is obtained by assembling the inverse DCT's of each block. Spatial masking is used to verify that the watermark is invisible and to control the scaling factor.

Pseudo-noise (PN) sequences form the signatures in our watermarking scheme because of their noise-like characteristics, resistance to interference, and their good auto-correlation properties. PN sequences are periodic noise-like binary sequences generated by length m linear shift registers [9]. Furthermore, the period N autocorrelation function has peaks equal to 1 at 0, N , $2N$, etc., and is approximately equal to $1/N$ elsewhere. These periodic peaks allow the author to synchronize with the embedded watermark during the detection process.

Visual masking models are used to modify the author signature. Visual masking refers to a situation where a signal raises the visual threshold for other signals around it. Both frequency and spatial masking are employed by our watermarking scheme. Our frequency masking model is based on the observation that a mask-

ing grating raises the visual threshold for signal gratings around the masking frequency [10]. The model we use [11] expresses the contrast threshold at frequency f as a function of f , the masking frequency f_m and the masking contrast c_m :

$$c(f, f_m) = c_0(f) \cdot \text{Max}\{1, (k(f/f_m)c_m)^{\alpha}\},$$

where $c_0(f)$ is the detection threshold at frequency f . To find the contrast threshold $c(f)$ at a frequency f in an image, we first use the DCT to transform the image into the frequency domain and find the constant at each frequency. Then we use a summation rule of the form $c(f) = [\sum_{f_m} c(f, f_m)^{\beta}]^{1/\beta}$. If the contrast error at f is less than $c(f)$, the model predicts that the error is invisible to human eyes.

After adding the watermark in the frequency domain, spatial masking is checked. The spatial model is used to verify that the watermark designed with the frequency masking model is invisible for local spatial regions. The model used here is similar to our image coding model [11] which gives the tolerable error level for each coefficient. Each watermark coefficient is compared with the tolerable error level obtained to assure that it is invisible. A visible watermark is rescaled via a weighting factor.

4. WATERMARK DETECTION

The watermark should be extractable even if common signal processing operations are applied to the host image. This is particularly true in the case of deliberate unauthorized attempts to remove it. For example, a pirate may attempt to add noise, filter, code, re-scale, etc., an image in an attempt to destroy the watermark. As the embedded watermark is noise-like and its location (based on multiple blocks) is unknown, a pirate has insufficient knowledge to directly remove the watermark. Furthermore, a different m -sequence is used for each block to further reduce unauthorized watermark removal by cross-correlation. Therefore, any destruction attempts are done blindly. Unlike other users, the author has copies of the original signal S and the signature. Detection of the watermark is accomplished via hypotheses testing:

$$\begin{aligned} H_0: X &= R - S = N && \text{(No watermark)} \\ H_1: X &= R - S = W' + N && \text{(Watermark)} \end{aligned}$$

where R is the potentially pirated signal, W' is the potentially modified watermark, and N is noise. The correct hypothesis is obtained by applying a correlating detector on X with W and comparing with a threshold. In some cases, e.g., spatial rescaling, a generalized likelihood ratio test must be applied.

To illus
grayscale
into 8
image

W,
eral d
iques
color
grated
to the
the w
noise
pled
was r
effici
pothe
lator
water

D
endir
hpp
rupt
nific
still
a pit
imat
decy
JPE
imag
the
ses
We
ing
mal
pres
nois
and
and
wh

scri
(un
len
wit
nifi
ter
as
po
bu
m
di

5. EXPERIMENTAL RESULTS

To illustrate our watermarking technique, the 256 x 256 grayscale (8-bit) image shown in Fig. 2 was segmented into 8 x 8 blocks and watermarked. The watermarked image is shown in Fig. 3. The images appear identical.

We tested the robustness of the watermark to several degradations. To model perceptual coding techniques, we corrupted the watermark with worst case colored noise which follows the image mask. We generated colored noise with SNR of 10dB and added it to the image with (hypothesis H_1) and without (H_0) the watermark. The watermarked image with colored noise is shown in Fig. 4. The hypothesis test was applied to each block in the image. This testing process was repeated 250 times. The normalized correlation coefficients indicate easy discrimination between the hypotheses as shown in Fig. 5. In particular, the correlation coefficient for the image with and without the watermark was approximately 0 and 1 respectively.

To further degrade the watermark, we applied JPEG coding at 0.38 bpp (10% quality, c.f. Fig. 5) and 1.32 bpp (50% quality) to each of the images already corrupted with colored noise. Note that the image is significantly degraded at 0.38 bpp, yet the watermark is still easily detected as shown in Fig. 6. It is unlikely a pirate would do so much irreparable damage to the image. Setting a decision threshold of 0.15 results in no decision errors. In Fig. 7, we show the result of applying JPEG coding at different quality factors to the noisy image with and without the watermark. It is clear that the correlation coefficient values for the two hypotheses are well separated for all JPEG coding qualities. We also investigated cropping robustness by determining the minimum number of image blocks required to make a confident decision on whether the watermark is present in an image ($P_D = 1$ and $P_F < 10^{-4}$). Each noisy image in the above tests was randomly cropped and tested. The results indicate that only 0.4%, 2%, and 15% of the image is needed for a confident decision when coded at 8 bpp, 1.32 bpp, and 0.38 bpp.

For comparison, we implemented the system described in [2]. For JPEG coding at 10%, we obtained (unnormalized) correlation coefficients using their system of 5.09 and 3.34 for the same test image with and without the watermark, respectively. The ratio is significantly smaller than ours. While testing their system, we were unable to reproduce the detection results as claimed in [2]. This may be the result of special post-processing operations they implement. The robustness of our watermarking scheme to re-sampling, multiple watermarking, vector quantization, and other distortions is described in [12].

6. REFERENCES

- [1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding," Tech. Rep., MIT Media Lab, 1994.
- [2] J. Cox, J. Killian, T. Leighton, and T. Shanon, "Secure Spread Spectrum Watermarking for Multimedia," Tech. Rep. 95-10, NEC Research Institute, 1995.
- [3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," in *Proc. 1997 IEEE Int. Conf. on Image Proc.*, vol. II, (Austin, TX), pp. 86-90, 1994.
- [4] I. Pitas and T. Kaskalis, "Applying Signatures on digital images," in *Nonlinear Signal Processing Workshop, Thessaloniki, Greece*, pp. 460-463, 1995.
- [5] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *Nonlinear Signal Processing Workshop, Thessaloniki, Greece*, pp. 452-455, 1995.
- [6] O. Bruyndonckx, J.-J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in *Nonlinear Signal Processing Workshop, Thessaloniki, Greece*, pp. 456-459, 1995.
- [7] J. R. Smith and B. O. Comiskey, "Modulation and Information Hiding in Images" to appear *1996 Workshop on Information Hiding*, University of Cambridge, UK.
- [8] N. Jayant, J. Johnston, and R. Safranek, "Signal Compression Based on Models of Human Perception," *Proc. of the IEEE*, vol. 81, pp. 1385-1422, oct 1993.
- [9] S. Haykin, *Communication Systems, 3rd Edition*, New York, NY: John Wiley and Sons, 1994.
- [10] G. E. Legge and J. M. Foley, "Contrast Masking in Human Vision," *J. Opt. Soc. Am.*, vol. 70, no. 12, pp. 1458-1471, 1980.
- [11] B. Zhu, A. Tewfik, and O. Gerek, "Low Bit Rate Near-Transparent Image Coding," in *Proc. of the SPIE Int. Conf. on Wavelet Apps. for Dual Use*, vol. 2491, (Orlando, FL), pp. 173-184, 1995.
- [12] A. H. Tewfik, M. D. Swanson, B. Zhu, K. Hamdy, and L. Boney, "Transparent Robust Watermarking for Images and Audio." To be submitted *IEEE Trans. on Signal Proc.*, 1996.



Figure 2: Original 256x256 grayscale image.

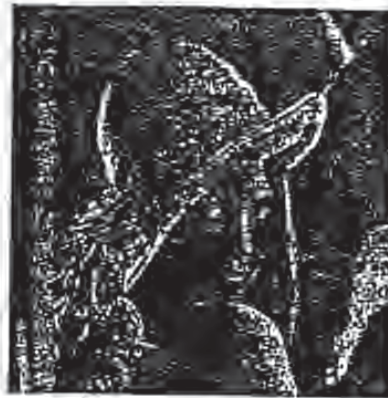


Figure 3: Watermarked image using 8x8 blocks.



Figure 4: Watermarked image with colored noise (SNR 10dB).



Figure 5: JPEG coded version of watermarked image at 0.38bpp (10% quality).

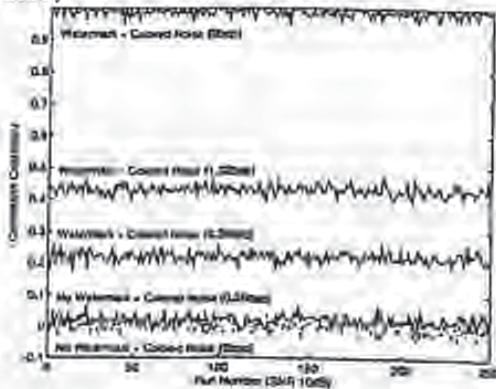


Figure 6: Watermark detection after adding colored noise with and without JPEG coding.

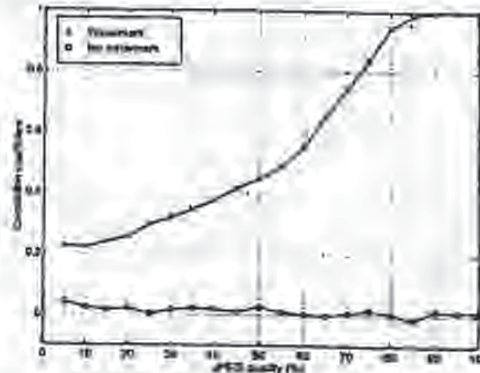


Figure 7: Watermark detection after JPEG coding at different qualities.

Signal
inform
ing di
effect
in thi
digi
to sub
previ
topice

The f
ing a
ing d
digi
impo

1.

2.

3.

4.

The
vide
on i
pers
gna

1996 IEEE DIGITAL SIGNAL PROCESSING WORKSHOP
PROCEEDINGS

SEPTEMBER 1 - 4 , 1996

HOTEL ALEXANDRA, LOEN, NORWAY



Cosponsored by: ABB Technology NERA
Telecommunications Group

BEST AVAILABLE COPY

Robust Data Hiding for Images *

Mitchell D. Swanson

Bin Zhu

Ahmed H. Tewfik

Department of Electrical Engineering, University of Minnesota, Minneapolis, MN 55455
e-mail: mswanson, binzhu, tewfik@ee.umn.edu

ABSTRACT

Data hiding is the process of encoding extra information in an image by making small modifications to its pixels. To be practical, the hidden data must be perceptually invisible yet robust to common signal processing operations. This paper introduces two schemes for hiding data in images. The techniques exploit perceptual masking properties to embed the data in an invisible manner. The first method employs spatial masking and data spreading to hide information by modifying image coefficients. The second method uses frequency masking to modify image spectral components. By using perceptual masking, we also increase robustness of the hidden information. Experimental results of data recovery after applying noise and JPEG coding to the hidden data are included.

1. INTRODUCTION

We introduce two robust schemes to hide information, e.g., labels, into an image by modifying perceptually irrelevant portions of image data. By exploiting the human visual system (HVS), our techniques embed a large amount of data into an image while guaranteeing that the hidden data are perceptually invisible. In particular, the data are hidden by modifying image coefficients according to masking levels based on the HVS. Information may be hidden throughout the image or confined to particular image objects and regions. The first scheme we introduce spreads the data to be hidden with a pseudo-noise sequence and then modifies them using spatial masking. The second data hiding scheme modifies the DCT coefficients of image blocks according to their frequency masking characteristics. In both schemes, masking characteristics are used to maintain high bit rates and robustness of the hidden data. We include experimental results which indicate the robustness of the data hiding techniques to common signal processing operations.

To be useful, the embedded data must be (1, 2): perceptually invisible within the host media; readily extracted by its intended audience; high bit-rate for practical applications; and robust to manip-

ulation and signal processing operations on the host image, e.g., filtering, re-sampling, compression, noise, cropping, etc. Hiding information in images may be used, e.g., to supplement an image with additional information, add copyright protection (i.e., digital watermarks), or verify image integrity. We consider here the generic problem of embedding supplementary information into image data with the goal of recovering the information bits without access to the original image. In such a scenario, the author of the hidden information supplies a public key which allows users to recover the hidden data. The hidden information may be text, audio, or image data. For example, text captions may be used to label faces and buildings in an image. A short audio clip may associate a train whistle with an image of a locomotive.

Note that embedding information directly into image data has several advantages over storing the data in an image header or a separate file. Specifically, header data are easily lost when the format of a file is changed or the image is cropped. Separate files also need to be transmitted when the image is transmitted and are difficult to maintain during cropping operations. Separate files and image headers also require additional storage. Hiding data directly into the image data resolves these problems.

2. PREVIOUS WORK

Several data hiding techniques have been proposed. The most common approaches modify the least significant bits (LSB) of an image based on the assumption that the LSB data are insignificant. In [3], two such techniques are described. The first replaces the LSB of the image with a pseudo-noise (PN) sequence, while the second adds a PN sequence to the LSB of the data. However, any approach which only modifies the LSB data is highly sensitive to noise and is easily destroyed. Another LSB data hiding method called "Patchwork" [1] chooses n pairs (a_i, b_i) of points in an image and increases the brightness of a_i by one unit while simultaneously decreasing the brightness of b_i . Several executable software packages (e.g., Stego, S-Tools) based on LSB approaches are also available [4]. A data hiding method similar to our frequency hiding method is proposed in [2], where the N largest frequency components of an image are modified by a PN sequence. How-

*This work was supported by AFOSR under grant AF/F49620-94-1-0161.

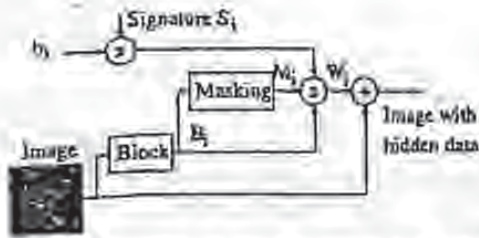


Figure 1. Diagram of spread spectrum data hiding technique.

ever, the scheme only modifies a subset of the frequency components and does not take into account the HVS. A method similar to our spatial hiding scheme is presented in [5], where the authors hide data in an image using spread spectrum techniques. Our approach employs spatial masking to maximize the amount of data hidden in the image.

3. SPATIAL AND FREQUENCY DOMAIN MASKING

We use masking models based on the HVS to ensure that the hidden data are perceptually invisible. Visual masking refers to a situation where a signal raises the visual threshold for other signals around it. Masking characteristics are used in high quality low bit rate coding algorithms to further reduce bit rates [6].

Our frequency masking model is based on the knowledge that a masking grating raises the visual threshold for signal gratings around the masking frequency [7]. The model we use [8] expresses the contrast threshold at frequency f as a function of f , the masking frequency f_m and the masking contrast c_m . To find the contrast threshold $c(f)$ at a frequency f in an image, we first use the DCT to transform the image into the frequency domain and find the contrast at each frequency. If the contrast error at f is less than $c(f)$, the model predicts that the error is invisible to human eyes.

Spatial masking refers to the situation that an edge raises the perceptual threshold around it. The model used here is similar to our image coding model [8] which is based on a model proposed by Girod [9]. In our approach, the upper channel of Girod's model is linearized under the assumption of small perceptual errors. The model gives the tolerable error level for each pixel in the image.

4. SPATIAL DATA HIDING

In Fig. 1, we show our first data hiding technique which uses spatial masking to shape hidden data. The first step consists of selecting arbitrarily sized image blocks B_i to embed the data. Note that the data may be embedded throughout the image or localized to specific regions and objects (e.g., the face outlined with a black box). This allows the author to associate image features with specific captions.

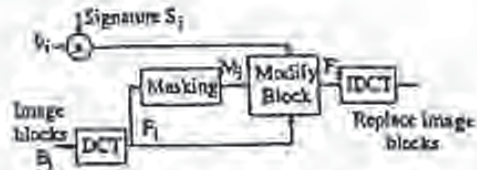


Figure 2. Diagram of frequency data hiding technique.

The message bits b_i are first spread using a pseudo-noise (PN) author signature S_i . As with spread spectrum communication systems, the PN sequence spreads the data spectrum, increases noise resistance, and hides the data. Spatial masking is then computed for the image blocks. The masking blocks M_i (i.e., tolerable error levels) are used to modify the hidden data $W_i = h_i(B_i + S_i)$, where $*$ is element-wise multiplication. The hidden data W_i are then added to the image. The masking blocks M_i shape the hidden data to guarantee invisibility and increase robustness.

As the hidden data are noise-like, they may only be extracted by a receiver that knows the PN signature S_i . A conventional receiver with access to S_i may be used to detect the hidden data. Specifically, the received image data blocks B_i are projected onto the author signature S_i weighted by the estimated image mask M_i and then thresholded to obtain an estimate of the data bit. In this way, image coefficients which are modified the most are given the most weight when the hidden data is recovered. Note that if the image has been cropped or translated, signature synchronization can be obtained using a two dimensional search. In some cases, e.g., spatial rescaling, a generalized likelihood ratio test must be applied.

5. FREQUENCY DATA HIDING

Our second data hiding approach is based on the frequency masking characteristics of the image data. The scheme is shown in Fig. 2. Again, blocks B_i are selected to hide the data b_i which are first spread by signature S_i . A discrete cosine transform (DCT) is applied to each block to form a DCT block F_i . A perceptual analysis stage is then applied to each DCT block to form frequency masking blocks M_i . A bit b_i is hidden in block F_i by modifying the DCT coefficients according to the equation

$$F_i'(j, k) = \left(\left\lfloor \frac{F_i(j, k)}{M_i(j, k)} \right\rfloor + \frac{1}{4} b_i S_i(j, k) \right) M_i(j, k),$$

where $\lfloor \cdot \rfloor$ denotes the rounding operation. The original image blocks B_i are replaced by the inverse DCT's of the modified blocks F_i' . Spatial masking is applied to the modified image to verify that the hidden data are invisible.

Given the image with (possibly modified) hidden data blocks F_i' , the data bit b_i may be recovered

ered by forming the difference

$$\hat{b}_i = \sum_{j,k} M_i'(j,k) \operatorname{sgn} \left(\frac{F_i''(j,k)}{M_i'(j,k)} - \left[\frac{F_i'(j,k)}{M_i'(j,k)} \right] \right)$$

where M_i' is the frequency mask estimated by the receiver times the signature S_i , i.e., $M_i' = M_i^{est} * S_i$, and $\operatorname{sgn}(\cdot)$ is the sign value. Again, the bit decision for block B_i is weighted by the mask M_i' . Unlike spatial data hiding, the bit error rate (BER) of this scheme is zero when no distortion is present in the received image. We can derive a simple expression for the upper bound on the BER when zero mean Gaussian noise with variance σ^2 is added to the signal. Without loss of generality, assume that $b_i = 1$. A decision error occurs for coefficient $F''(j,k)$ whenever the magnitude of a noise sample $|w(j,k)|$ falls in one of the intervals

$$\left[\frac{(2n+1)M(j,k)}{4}, \frac{(2n+3)M(j,k)}{4} \right] = I_n$$

for $n = 0, 1, 2, \dots$. Using the complementary error function $\operatorname{erfc}(\cdot)$, we may write the probability of error for coefficient $F''(j,k)$ as

$$P_e(F''(j,k), \sigma) = 2 \sum_{n=0}^{\infty} \operatorname{erfc} \left(\frac{I_n}{\sigma} \right)$$

For σ fixed, $P_e(F''(j,k), \sigma)$ decreases as $M(j,k)$ increases. Hence the receiver places more weight on coefficients with large masking values. The overall probability of error for bit b_i is a weighted combination of the $P_e(F''(j,k), \sigma)$ in block B_i .

6. PREPROCESSING HIDDEN DATA

To add further robustness to the hidden data, the data hiding techniques introduced here may be modified to take into account certain signal processing operations. If it is known that a JPEG coder will be applied to the image, for example, we can modify each data hiding procedure appropriately. In the spatial data hiding case, the signature-masking product is computed and then compressed/decompressed using a JPEG coder at an estimated quality factor Q . The decompressed product can then be modified to compensate for energy losses. In the frequency hiding scheme, the mask M_i may be preprocessed using the JPEG quantization table by substituting a new mask $\hat{M}_i = Q * M_i$ for M_i .

7. RESULTS

We illustrate our data hiding techniques on the 256×256 grayscale image shown in Fig. 3. Using each scheme, we embedded the text "We are investigating data hiding in multimedia systems" (432 bits) in the image by converting the text into bits and embedding each bit in an 8×8 image block. The text "Lens, 123 Main Street" (168 bits) is

also hidden in blocks about the face object in the image (outlined by the block box in Fig. 3). The image with the hidden data is shown in Fig. 4.

In Fig. 5 we show a plot of BER for differing levels of white noises using spatial data hiding. Note that since the signature and noise are approximately uncorrelated, the BER remains constant for all noise levels. The BER of the scheme for JPEG coding at different quality settings is shown in Fig. 6. Preprocessing of the signature-mask product at a quality of 80% was used.

A plot of BER for differing levels of white noises using frequency data hiding is shown in Fig. 7. Note that this scheme performs better in low noise conditions and worse in high noise conditions than the spatial technique. Similarly for the plot of BER versus JPEG coding at different quality settings shown in Fig. 8. The frequency scheme works well under high quality coding conditions yet degrades more rapidly than spatial data hiding when the coding becomes too lossy. JPEG preprocessing at a quality of 70% was used.

REFERENCES

- [1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding," Tech. Rep., MIT Media Lab, 1994.
- [2] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," Tech. Rep. 95-10, NEC Research Institute, 1995.
- [3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," in *Proc. 1994 IEEE Int. Conf. on Image Proc.*, vol. 11, (Austin, TX), pp. 86-90, 1994.
- [4] E. Milbrandt, "Steganography Info and Archive." Available at URL <http://indynia.wupui.edu/~emilbran/stego.html>.
- [5] J. R. Smith and B. O. Comiskey, "Modulation and Information Hiding in Images" to appear *1996 Workshop on Information Hiding*, University of Cambridge, UK.
- [6] N. Jayant, J. Johnston, and R. Safranek, "Signal Compression Based on Models of Human Perception," *Proc. of the IEEE*, vol. 81, pp. 1385-1422, oct 1993.
- [7] G. E. Legge and J. M. Foley, "Contrast Masking in Human Vision," *J. Opt. Soc. Am.*, vol. 70, no. 12, pp. 1458-1471, 1980.
- [8] B. Zhu, A. Tewfik, and O. Gerek, "Low Bit Rate Near-Transparent Image Coding," in *Proc. of the SPIE Int. Conf. on Wavelet Apps. for Dual Use*, vol. 2491, (Orlando, FL), pp. 173-184, 1995.
- [9] B. Girod, "The Information Theoretical Significance of Spatial and Temporal Masking in Video Signals," in *Proc. of the SPIE Human Vision, Visual Processing, and Digital Display*, vol. 1077, pp. 178-187, 1989.



Figure 3. Original 256x256 grayscale image.

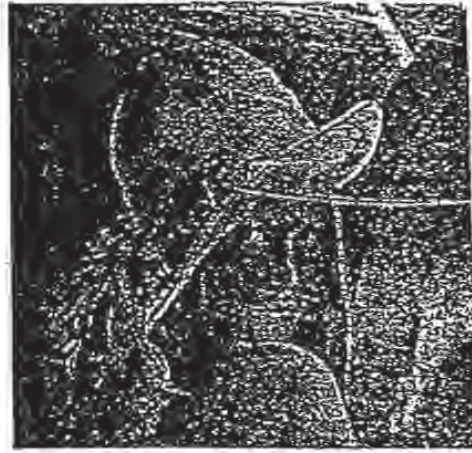


Figure 4. Image with hidden data.

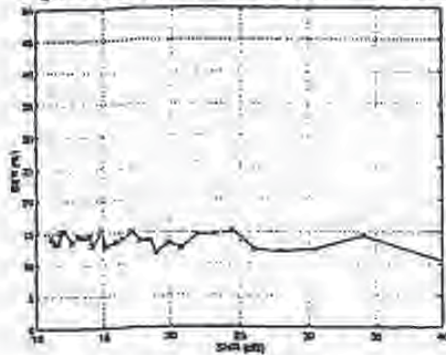


Figure 5. Bit error rate versus SNR using spatial data hiding.

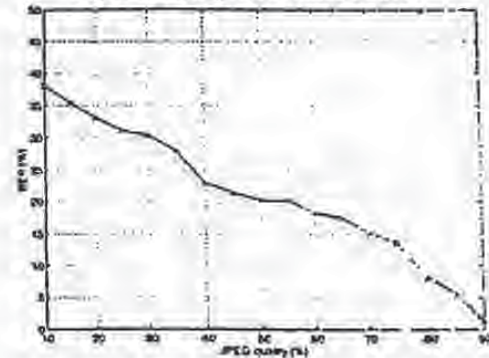


Figure 6. Bit error rate versus JPEG coding at different qualities using spatial data hiding.

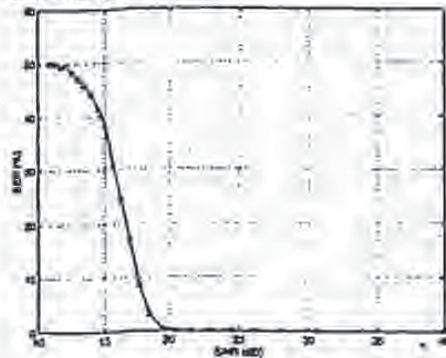


Figure 7. Bit error rate versus SNR using frequency data hiding.

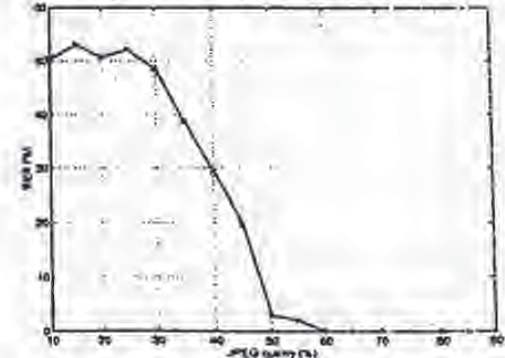


Figure 8. Bit error rate versus JPEG coding at different qualities using frequency data hiding.

9

Klaus Brunnstein, Peter Paul Sint

**Intellectual Property Rights
and New Technologies**

Proceedings of the KnowRight'95 Conference

R.Oldenbourg Wien München 1995

BEST AVAILABLE COPY

EMBEDDING ROBUST LABELS INTO IMAGES FOR COPYRIGHT PROTECTION

NOTICE: This material may
be subject to copyright
protection by its owner.

Jian Zhao & Eckhard Koch

Fraunhofer Institute for Computer Graphics
Wilhelminenstr. 7, 64283 Darmstadt, Germany

Email: {zhao, ekoch}@igd.fhg.de

Abstract

This paper describes a set of novel steganographic methods to secretly embed robust labels into image data for identifying image copyright holder and original distributor in digital networked environment. The embedded label is undetectable, unremovable and unalterable. Furthermore it can survive processing which does not seriously reduce the quality of the image, such as lossy image compression, low pass filtering and image format conversions.

1 Introduction

The wide use of digitally formatted audio, video and printed information in network environment has been slowed down by the lack of adequate protection on them. Developers and publishers hesitate to distribute their sensitive or valuable materials because of the easiness of illicit copying and dissemination [3],[6],[7].

Compared to ordinary paper form information, digitized multimedia information (image, text, audio, video) provides many advantages, such as easy and inexpensive duplication and re-use, less expensive and more flexible transmission either electronically (e.g. through the Internet) or physically (e.g. as CD-ROM). Furthermore, transferring such information electronically through network is faster and needs less efforts than physical paper copying, distribution and update. However, these advantages also significantly increase the problems associated with enforcing copyright on the electronic information.

Basically, in order to protect distributed electronic multimedia information, we need two types of protections. First, the multimedia data must contain a label or code, which identifies it uniquely as property of the copyright holder. Second, the multimedia data should be marked in a manner which allows its distribution to be tracked. This does not limit the number of copies allowed (vs. copy protection), but provides a mean to check the original distributor. In order to prevent any copyright forgery, misuse and violation, the copyright label must be unremovable and unalterable, and furthermore survive processing which does not seriously reduce the quality of the data. This requires that first the label must be secretly stored in a multimedia data, i.e. the locations for embedding this label are secret, second the label must be robust even if the labeled multimedia data has been processed incidentally or intentionally.

This paper describes a set of novel steganographic methods to secretly embed robust labels into image data for copyright protection in open networked environment. The label embedded in the image can be assigned or generated in a way that it is able to identify the copyright holder and the original purchaser (distributor).

Steganographic method is a technique embedding additional information into a data by modifying the original data without affecting the quality of the data. Many steganographic methods have been proposed to aim at storing additional information to identify or label formatted electronic documents [1], images, video [8], and audio data. However, they are far away from the requirements in protecting multimedia information in a networked environment, because although some of them provide secret locations for label embedding, none of them is able to prevent attacks on the embedded information by simple image processing, i.e. they do not adequately address the possibilities of using data compression, low pass filtering and/or simply changing the file format to remove an embedded code.

The discussion begins with a general framework for copyright label embedding. Then two specific methods are developed: one is based on the JPEG compression model for embedding labels in gray-scaled and color images, and the other is based on the black/white rate for binary images. Finally, these methods are tested experimentally and the future work is discussed.

2 Robust Label Embedding Framework

The system developed along the methods presented in this paper is called 'SysCoP' (System for Copyright Protection). It consists of a set of methods to embed robust labels into different types of images. Currently, the system supports gray-scaled, color, and binary images. These methods share an algorithm framework for both label writing and reading described below.

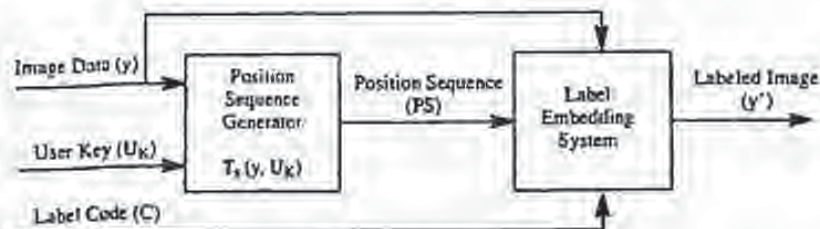


Figure 1. Write label

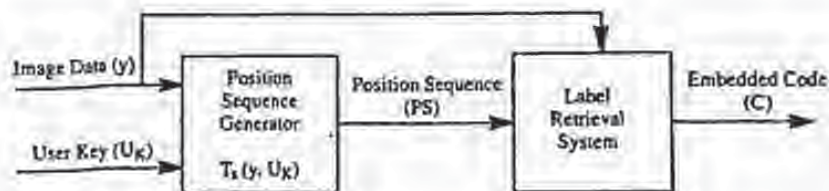


Figure 2. Read label

The framework, as shown in Figure 1 for label writing and Figure 2 for label reading, is composed of two steps. The first step generates a pseudo random position sequence for selecting blocks where the code is embedded. This step is denoted as a function $T_1(y, U_K)$ where y is the image data to be labeled, and U_K is the user-supplied secret key. The second step simply embeds or retrieves the code into or from the blocks specified in the position sequence. The methods for embedding or reading code depend on types of images, and will be described individually in the next section.

The function $T_1(y, U_K)$ firstly extracts some features from the image data and then use them together with the user secret key as the seeds for position sequence generation [4]. Ideally, the features of the image data used here must meet the following requirements:

- they must be robust against simple image processing that does not affect the visual quality of the image, and
- they must be image-dependent, i.e. the image can be identified, uniquely in an ideal case, by these features extracted from the image data.

However, to achieve the contradictory requirements above, in fact, is a very hard work. Much research has been done in related fields for other purposes, e.g. content-based image retrieval, image segment and pattern recognition, which can be found in many literature (e.g. [9]). Currently, we only use the width and height of an image for the position generation in the function $T_1(y, U_K)$.

Before describing the framework, we introduce some terminology. A block of an image consists of 8×8 pixels. In this framework, it is either a contiguous or a distributed block. A contiguous block is a 8×8 square in an image component. A distributed block is a collection of 8×8 pixels each of which is selected randomly from the whole image space. The purpose of distributed block is to prevent or discourage attackers from detecting embedding locations by comparing different labeled images. A block is 'invalid' for code embedding if too big modifications to the block data are needed in order to embed a bit into this block. The criteria of validation of the block depends on the specific label-embedding methods to be described in the next section.

Let C be the embedded code, and represented as a binary bit stream (c_0, c_1, \dots, c_n) . Let i be the index of current bit in this stream. Let \mathcal{B} be the block set in which each block has been randomly selected. Initialize i to 0 and \mathcal{B} to $\{\}$. The framework for writing and reading robust labels is described below in Algorithm 1(a)-(b).

Algorithm 1(a): Framework (write).

- (1) If $i \geq n$, return.
- (2) Randomly select a block b , using the position sequence generation function $T_1(U_K, y)$ in Figure 1.
- (3) If b exists already in \mathcal{B} , go to (2), otherwise add b to \mathcal{B} .
- (4) Call $check_write(b, c_i)$ to check whether b is a valid block: if this function returns False (i.e. the block b is an invalid block), go to (2).
- (5) Call $write(b, c_i)$ to embed a bit c_i to the block b .
- (6) Increment i , go to (1).

Algorithm 1(b): Framework (read).

- (1) If $i \geq n$, return.
- (2) Randomly select a distributed or a contiguous 8×8 block b , using the position sequence generation function $T_k(U, X, y)$ in Figure 2.
- (3) If b exists already in \mathcal{B} , then go to (2), otherwise add b to \mathcal{B} .
- (4) Call $check_read(b, c_i)$ to check whether b is a valid block: if this function returns False (i.e. the block b is an invalid block), go to (2).
- (5) Call $read(b)$ to retrieve a bit from the block b .
- (6) Increment i , and go to (1).

3 Robust Label Embedding Methods

3.1 JPEG-Based Label Embedding for Gray-Scaled and Color Images

In this subsection, we first introduce briefly the JPEG compression model, then describe the principle of the embedding methods based on the JPEG compression model. Finally, the algorithms for embedding labels into gray-scaled and color images are developed.

Suppose the source image composes three components: one luminance (Y) and two chrominance (I and Q). That is, each pixel in the image can be represented with a triple of 8-bit values (Y, I, Q). Each component is broken up into contiguous blocks. The JPEG compression consists of six steps: normalization, DCT transformation, quantization, zigzag scan, run-length encoding and Huffman coding steps. Since our method is applied after the quantization step, we only describe briefly the first three steps of the JPEG model. The detailed description of the JPEG model is available elsewhere [1].

The normalization step brings all image values into a range, e.g. between -128 and 127 for a 24-bit image. The DCT step applies the discrete cosine transform (DCT) to each 8×8 block, producing a new 8×8 block [10]. If we call the new block $Y(k, l)$, with $k, l \in 0..7$, the equation of the DCT is:

$$Y(k, l) = \frac{1}{4} \sum_i \sum_j C(l, k) C(j, l) y(i, j)$$

where

$$C(l, k) = A(k) \frac{\cos(2i + 1)kn}{16} \quad A(k) = \frac{1}{\sqrt{2}} \text{ for } k = 0, \quad A(k) = 1 \text{ for } k \neq 0 \quad (1)$$

Each element of the new block is further quantized:

$$Y_c[k, l] = \text{Round}\left(\frac{Y[k, l]}{q[k, l]}\right) \quad (2)$$

Equation (2) represents the entire lossy modelling process of the JPEG compression. The choice of the quantization table ($q[k, l]$) determines both the amount of compression and the quality of the decompressed image. The JPEG standard includes recommended luminance and chrominance quantization tables resulting from human factors studies. To obtain different compression quality, we typically use a *quality factor* to scale the values of these default quantization tables.

In the JPEG decompression process, each element of $Y_Q(k,l)$ is multiplied by $q(k,l)$ to recover an approximation of $Y(k,l)$. Finally, the image block $y(i,j)$ can be recovered by performing an inverse 2-D DCT (IDCT):

$$y(i,j) = \frac{1}{4} \sum_k \sum_l C(k,l) G_j(j) Y(k,l) \quad (3)$$

The basic principle of the JPEG-based embedding method is that quantized elements have a moderate variance level in the middle frequency coefficient ranges, where scattered changes in the image data should not be noticeably visible. The specific frequencies being used to embed the code will be 'hopped' in this range to increase the robustness of the signal and making it more difficult to find [5],[2]. A label bit is embedded through holding specific relationship among three quantized elements of a block. The relationships among them compose 8 patterns (combinations) which are divided into three groups: two of them are used to represent '1' or '0' for embedded codes (valid patterns), and the other represents *invalid patterns*. If too big modifications are needed to hold a desired valid pattern representing a bit, this block is invalid. In this case, the relationships among the three elements of the selected location set are modified to any of the invalid patterns to 'tell' the label-retrieval process that this block is invalid. The criterion for invalid blocks is specified by a parameter MD, i.e. the maximum difference between any two elements of a selected location set in order to reach the desired valid pattern.

| Ser No. | (k_1,l_1) | (k_2,l_2) | (k_3,l_3) |
|---------|-------------|-------------|-------------|
| 1 | 2(0,2) | 9(1,1) | 10(1,2) |
| 2 | 9(1,1) | 2(0,2) | 10(1,2) |
| 3 | 3(0,3) | 10(1,2) | 11(1,3) |
| 4 | 10(1,2) | 3(0,3) | 11(1,3) |
| 5 | 9(1,1) | 7(0,2) | 10(1,2) |
| 6 | 2(0,2) | 9(1,1) | 10(1,2) |
| 7 | 9(1,1) | 16(2,0) | 2(0,2) |
| 8 | 16(2,0) | 9(1,1) | 2(0,2) |
| 9 | 2(0,2) | 9(1,1) | 16(2,0) |
| 10 | 9(1,1) | 2(0,2) | 16(2,0) |
| 11 | 10(1,2) | 17(2,1) | 3(0,3) |
| 12 | 17(2,1) | 10(1,2) | 3(0,3) |
| 13 | 10(1,2) | 3(0,3) | 17(2,1) |
| 14 | 3(0,3) | 10(1,2) | 17(2,1) |
| 15 | 9(1,1) | 16(2,0) | 17(2,1) |
| 16 | 16(2,0) | 9(1,1) | 17(2,1) |
| 17 | 10(1,2) | 17(2,1) | 18(2,2) |
| 18 | 17(2,1) | 10(1,2) | 18(2,2) |

Table 1. Possible location sets



Figure 3. Possible locations for embedding code in a block

| (k_1,l_1) | (k_2,l_2) | (k_3,l_3) | |
|-------------|-------------|-------------|--------------------|
| H | M | L | } patterns for '1' |
| M | H | L | |
| H | M | L | |
| M | L | H | } patterns for '0' |
| L | M | H | |
| L | L | H | } invalid patterns |
| H | L | M | |
| L | H | M | |
| M | M | M | |

Table 2. '1', '0' and invalid patterns (H: High, M: Middle, L: Low)

Our statistic results of the possible locations holding the specific frequencies are illustrated in Figure 3 as shadowed areas within a 8x8 block. In Table 1, we give our statistic results of the best location sets

combined from these possible elements. The algorithms to write and read a label into and from an color or gray-scaled image are described in Algorithm 2(a)-(d).

Two parameters are provided for adjusting the robustness vs. modification visibility in an embedding process. The first one is the distance (D) between selected quantized frequency coefficients for representing an embedded bit. The default value of this distance is 1. The greater distance produces stronger robustness, but also may cause more serious modification visibilities. The second parameter is the quantization factor (Q) used to quantize the values selected for embedding code. The greater quantization factor results in less modifications to image data but weaker robustness against lossy JPEG compression. The default value of this quantization factor is 75%.

Algorithm 2(a): check_write(b, c_i)

- (1) A three-element location set of the block b is pseudo-randomly (from the user key and image data) selected from the possible location sets listed in Table 1. They are denoted as (k_1, l_1) , (k_2, l_2) and (k_3, l_3) .
- (2) The block b is locally DCT transformed and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q parameter. Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.
- (3) When $c_i=1$, if $\text{MIN}(|Y_Q(k_1, l_1)|, |Y_Q(k_2, l_2)|) + MD < |Y_Q(k_3, l_3)|$ where $|Y_Q(k_u, l_u)|$ is the absolute value of $Y_Q(k_u, l_u)$ with $u \in 1..3$, MIN is an operation that returns the minimum value of two elements, and MD is the maximum modification distance, then b is an invalid block:
 - (i) modify them to any of the invalid patterns shown in Table 2,
 - (ii) de-quantize and inversely transform (IDCT) them, and write them back to the block b ,
 - (iii) return False.
- (4) When $c_i=0$, if $\text{MAX}(|Y_Q(k_1, l_1)|, |Y_Q(k_2, l_2)|) > |Y_Q(k_3, l_3)| + MD$ where MAX is an operation that returns the maximum value of two elements, and MD is the maximum modification distance, then b is an invalid block:
 - (i) modify them to any of the invalid patterns shown in Table 2,
 - (ii) de-quantize, inversely transform (IDCT) them, and write them back to the block b ,
 - (iii) return False.
- (5) For other cases, return True.

Algorithm 2(b): check_read(b, c_i)

- (1) A three-element location set of the block b is pseudo-randomly (from the user key and image data) selected from the possible location sets listed in Table 1. They are denoted as (k_1, l_1) , (k_2, l_2) and (k_3, l_3) .
- (2) The block b is locally DCT transformed and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q parameter. Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (3) If $|Y_Q(k_1, l_1)|$, $|Y_Q(k_2, l_2)|$ and $|Y_Q(k_3, l_3)|$ form any of the invalid patterns as illustrated in Table 2, return False, otherwise return True.

Algorithm 2(c): write(b, c_i)

Assume that a valid three-element location set of the block b has been pseudo-randomly selected. They are denoted as (k_1, l_1) , (k_2, l_2) , and (k_3, l_3) . The block b is locally DCT transformed, and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q . Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$, and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (1) When $c_i=1$, modify the $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ such that they satisfy the following conditions: $Y_Q(k_1, l_1) > Y_Q(k_3, l_3) + D$, and $Y_Q(k_2, l_2) > Y_Q(k_3, l_3) + D$
- (2) When $c_i=0$, modify the $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ such that they satisfy the following conditions: $Y_Q(k_1, l_1) + D < Y_Q(k_3, l_3)$, and $Y_Q(k_2, l_2) + D < Y_Q(k_3, l_3)$
- (3) $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$ and $Y_Q(k_3, l_3)$ are de-quantized, inversely transformed (IDCT), and written back to the block b .

Algorithm 2(d): read(b)

Assume that a valid three-element location set of the block b has been pseudo-randomly selected. They are denoted as (k_1, l_1) , (k_2, l_2) , and (k_3, l_3) . The block b is locally DCT transformed, and quantized at the locations (k_1, l_1) , (k_2, l_2) and (k_3, l_3) with the quality factor Q . Let $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$, and $Y_Q(k_3, l_3)$ be the quantized coefficient values at the selected locations.

- (1) If $Y_Q(k_1, l_1) > Y_Q(k_2, l_2) + D$ and $Y_Q(k_2, l_2) > Y_Q(k_3, l_3) + D$, return 1.
- (2) If $Y_Q(k_1, l_1) + D < Y_Q(k_3, l_3)$, and $Y_Q(k_2, l_2) + D < Y_Q(k_3, l_3)$, returns 0.
- (3) In other cases, the embedded bit in this block b has been damaged.

3.2 Black/White Rate-Based Label Embedding for Binary Images

The value of each pixel in a binary image is either '1' or '0'. This determines that, in general, there is no 'noise' space which can be used for embedding additional information. To do it, we must find appropriate image areas where modifications for embedding labels do not affect seriously the quality of the original image. Obviously, these areas are varied with individual images or at least with types of images.

The proposed method for binary images is based on the ratio of '1' and '0' in a selected block. Suppose '1' represent black bit and '0' represent white bit in the source binary image. Let $P_1(b)$ be the rate (percentage) of blacks in the selected block b :

$$P_1(b) = \frac{N_1(b)}{64} \text{ where } N_1(b) \text{ is the number of '1' in the block } b.$$

Since the sum of percentages of blacks and whites in a block is 100%, the rate (percentage) of whites in the block b is $P_0(b) = 100 - P_1(b)$. A bit is embedded into a block b in the following way: a '1' is embedded into the block b if $P_1(b)$ is greater than a given threshold, and a '0' is embedded into the block b if $P_1(b)$ is less than another given threshold. A sequence of contiguous or distributed blocks is modified by switching whites to blacks or vice versa until such thresholds are reached.

We have classified two categories of binary images on which the generic method described above can be applied. These binary images are identified by distribution feature of blacks and whites. The first type of binary images is dithered image in which the black and white are well interlaced. The second type of binary images is black/white sharply contrasted images in which there exist clear boundaries between black and white areas.

Two modification strategies are adopted for these two types of binary images, respectively. For dithered binary images, modifications are well-distributed throughout the whole block: the bit that has most neighbors with the same value (either black or white) is reversed. For sharply contrasted binary images, modifications are carried out at the boundary of black and white pixels: the bit that has most neighbors with the opposite value is reversed. At the borders of the contiguous block, the neighbor bits in the neighbor blocks are also taken into account in both approaches. Two examples of both modification strategies are illustrated in Figure 4 and 5, respectively.

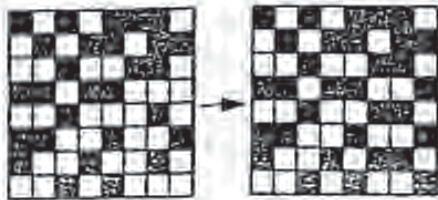


Figure 4. Well-distributed modifications.



Figure 5. Modifications at black and white boundary.

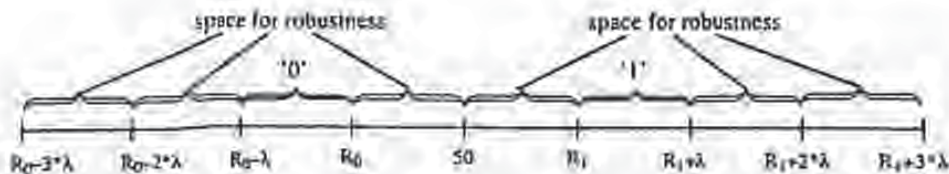


Figure 6. Achieve robustness in the black/white rate-based embedding method.

Let R_1 be the threshold rate for '1'. Thus, the threshold rate for '0' is $R_0 = (100\% - R_1)$. Let λ be the robustness degree against image processing of labeled images. It represents the number of bits that can be altered after image processing without damage of embedded bits. For example, when λ is 5%, alternation (i.e. reversion from '1' to '0' or vice versa) of less than 4 bits in a block does not damage the embedded code. Our experiments have shown that the following values of them are the reasonable choices both in robustness of embedding code and the modification visibility:

$$R_1 = 55, R_0 = 45, \text{ and } \lambda = 5.$$

The algorithms to write and read a label into and from a binary image are described in Algorithm 3(a)-(d).

Algorithm 3(a): check_write(b, c_i)

(1) If $P_1(b) > R_1 + 3\lambda$ or $P_1(b) < R_1 - 3\lambda$, return False.

- (2) When $c_i=1$, if $P_1(b) < R_0$, modify the block b such that $P_1(b) < R_0 - 3\lambda$, and then return False.
- (3) When $c_i=0$, if $P_1(b) > R_1$, modify the block b such that $P_1(b) > R_1 + 3\lambda$, and then return False.
- (4) For other cases, return True.

Algorithm 3(b): check_read(b, c_i)

- (1) If $P_1(b) > R_1 + 2\lambda$ or $P_1(b) < R_0 - 2\lambda$, return False.
- (2) For other cases, return True.

Algorithm 3(c): write(b, c_i)

Assume that a valid block b has been pseudo-randomly selected. A bit c_i is embedded into b by switching blacks to whites or vice versa using the different modification strategies described above in order to reach a specified threshold rate.

- (1) When $c_i=1$, modify the block b such that: $P_1(b) \geq R_1$ and $P_1(b) \leq R_1 + \lambda$.
- (2) When $c_i=0$, modify the block b such that: $P_1(b) \leq R_0$ and $P_1(b) \geq R_0 - \lambda$.
- (3) write the block b back to the image.

Algorithm 3(d): read(b)

Assume that a valid block b has been pseudo-randomly selected.

- (1) If $P_1(b) > 50$, return 1.
- (2) If $P_1(b) < 50$, return 0.
- (3) For other cases, the embedded bit in the block b has been damaged.

4 Conclusion

The 'SysCoP' has been implemented on UNIX platform, and provides a graphical interface, a set of UNIX commands and an API (Application Programming Interface). It currently supports JPEG, PPM, GIF, and TIFF image formats. Experiments have been carried out to demonstrate the robustness of our methods against image processing. For the gray-scaled and color images using the JPEG-based embedding method, three images were labeled, and then processed by JPEG compression, format conversions and color reduction. In general, the results are quite satisfactory and meet the basic requirements for embedding codes as copyright labels. Due to the space limitation of the paper, concrete results are omitted. For the binary images, a dithered TIFF binary image and a sharply contrasted TIFF binary image were used in our tests. They are labeled first with $R_1=55\%$ and the robustness degree (λ) 5%. The labeled TIFF images are then smoothed and converted to PBM. The embedded codes were not damaged in both labeled images after smoothing and conversions.

Our methods are still weak against physical damages (e.g. cut a pixel line, grab an area, etc.). Currently, we address this problem by allowing the user to specify 'valuable or sensitive' areas of an

image into which labels are (repeatedly) embedded. Thus, cutting a part which is not in these areas does not damage embedded labels.

The methods described in this paper for embedding robust copyright labels for images have been extended to support MPEG-1. Two additional attacks in embedding copyright labels into MPEG-1 videos have been identified: removal of frames and re-compression with different patterns. To be resistant against them, the copyright label is repeatedly embedded into each frame. Thus we ensure that the label can be retrieved from each I-frame regardless of re-compression with different patterns. Furthermore, we are developing new labeling methods for other digital media, i.e. structured electronic documents (e.g. PostScript, SGML documents) and audio data. In addition, a WWW (World Wide Web) image copyright labeling server incorporating the methods described in this paper is being developed.

Acknowledge We are grateful to Scott Burgett from GMI, USA, who initiated and completed the JPEG-based embedding method of 'SysCoP' during his visiting stay at the Fraunhofer-IGD in Darmstadt. We also want to thank Martin Claviez and Joachim Krumb for helping us in implementing the 'SysCoP' system.

References

- [1] J. BRASSIL, S. LOW, N. MAXEMCHUK, L. O'GORMAN. *Electronic Marking and Identification Techniques to Discourage Document Copying*. AT&T Bell Laboratories, Murray Hill, NJ, 1994.
- [2] S. BURGETT, E. KOCH, J. ZHAO. A Novel Method for Copyright Labeling Digitized Image Data. Technical Report of Fraunhofer Institute for Computer Graphics, Darmstadt, August, 1994. (Also submitted to IEEE Trans. on Communication, September, 1994).
- [3] A.K. CHOUDHURY, N.F. MAXEMCHUK, S. PAUL, H.G. SCHULZTRINNE. *Copyright Protection for Electronic Publishing over Computer Networks*. AT&T Bell Laboratories, June 1994.
- [4] W. DIFFIE and X. HELLMAN. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.
- [5] R. C. DIXON. *Spread Spectrum Systems*, 2nd ed., Wiley, New York, NY, 1984.
- [6] B. KAHIN. The strategic environment for protecting multimedia. *IMA Intellectual Property Project Proceedings*, vol. 1, no.1, 1994, pp.1-8.
- [7] B. KOCH, J. RINDFREY, J. ZHAO. Copyright Protection for Multimedia Data. *Proceedings of the International Conference on Digital Media and Electronic Publishing* (6-8 December 1994, Leeds, UK).
- [8] K. MANTUSI and K. TANAKA. Video-Sicgnography: How to secretly embed a signature in a picture. *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, 1994.
- [9] W. NIBLACK, R. BARBER, W. EQUITZ, M. FLICKNER, E. GLASMAN, D. PETKOVIC, P. YANKER, C. FALOUTOS, G. TAUBER. The QBIC Project: Querying Images By Content Using Color, Texture, and Shape. *SPIE* vol. 1908, 1993, pp.173-187.
- [10] K.R. RAO and P. YIP. *Discrete Cosine Transform: Algorithms Advantages, Applications*. Academic Press, 1990.
- [11] G.K. WALLACE. The JPEG still picture compression standard. *Communications of the ACM*, vol. 34, no. 4, April 1991, pp.30-40.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CROPPED AT TOP, BOTTOM OR SIDES
- IMAGE IS TOO DARK OR TOO LIGHT
- UNRECOGNIZABLE TEXT OR DRAWINGS
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

469 687

1 ic

1995 IEEE WORKSHOP ON NONLINEAR SIGNAL AND IMAGE PROCESSING

Neos Marmaras
Greece
20 - 22 June 1995

Sponsored by

- Aristotle University of Thessaloniki
 - CERES Flying Dolphins
 - Commission of the EU, Long Term Research
 - Domaine Carras
 - ESPRIT III Project NAT
 - EURASIP
 - Greek Ministry of Research and Technology
 - IEEE CAS and ASSP Societies
 - INTRACOM
-

ELECTRONIC WORKSHOP PROCEEDINGS

Papers listed by session

Invited papers

19.1. Towards Robust and Hidden Image Copyright Labeling

Session 19 : Image Signatures

Authors: E. Koch, J. Zhao

Fraunhofer Inst. for Computer Graphics

Page 1

Page 2

Page 3

Page 4

NSIP 95

 HTML
2.0

10

Towards Robust and Hidden Image Copyright Labeling

E. Koch & J. Zhao

Fraunhofer Institute for Computer Graphics
Wilhelmshavenstr. 7, 64283 Darmstadt, Germany
email: {ekoch,zhao}@igd.fhg.de

Abstract — This paper first presents the "hidden label" approach for identifying the ownership and distribution of multimedia information (image or video data) in digital networked environment. Then it discusses criteria and difficulties in implementing the approach. Finally a method using a JPEG model based, frequency hopped, randomly sequenced pulse position modulated code (RSPPMC) is described. This method supports robustness of embedded labels against several damaging possibilities such as lossy data compression, low pass filtering and/or color space conversion.

1 Introduction

The electronic representation and transfer of digitized multimedia information (text, video, and audio) have increased the potential for misuse and theft of such information, and significantly increases the problems associated with enforcing copyrights on multimedia information [1,2]. These problems are rooted from the intrinsic features of the digitally formatted information: (1) making copies is easy and inexpensive; (2) each copy is exactly identical to the original; and (3) distribution of the copies (e.g. via network or floppy) is easy and fast. For this reason, creators or publishers of multimedia materials fear providing their works for usage in new multimedia services, and are seeking technical solutions to the problems associated with copyright protection of multimedia data.

These problems have recently raised attention in national IT (information technology) programmes, for example, NII (National Information Infrastructure) launched in the United States in 1993 established a working group on Intellectual Property Rights which is mainly concerned with copyright law and its application and effectiveness in the context of NII [3]. Several projects are currently or have recently been concerned with copyright and related issues in the digital world, for example, the EC ESPRIT project CITED (Copyright in transmitted electronic data) [4] and COPICAT (Copyright Ownership Protection in Computer Assisted Training) [5], and the EC RACE

project ACCOPI (Access Control and Copyright Protection for Images) [6].

In [2], we have summarized that the technical mechanism of copyright protection for information in digital form can be divided into three levels: access control, use right control, and labeling-based mechanisms. This paper addresses the problems in developing the last level of mechanism, and presents a JPEG-based method of labeling image for copyright protection.

Although some attention has been given to steganographic labeling and similar problems [7], there exists no technology designed to secretly embed a robust and invisible (hidden) copyright label in images. In particular, no current method adequately addresses the possibilities of using data compression, low pass filtering and/or simply changing the file format to remove an embedded code. Therefore, one of the main goals of this paper is to define a reasonable set of functional requirements and design criteria for an image copyright labeling method, and to furthermore demonstrate that the main difficulties involved in designing such a system can be solved.

The discussion begins with a section which outlines the functionality of the proposed system and general design criteria for the novel embedding technique. A specific method based on the JPEG compression standard for embedding copyright labels in image data is then presented.

2 Requirements and possible attacks

In order to be effective and workable in a multimedia environment, the copyright label must be difficult to remove and survive processing which does not seriously reduce the value of the image. This encompasses a wide range of possibilities including format conversions, data compression, and low pass filtering. In addition to copyright labeling of broadcast images, application areas for steganographic labeling techniques include copyright and/or secure records labeling of electronic publishing, facsimiles, scientific imaging, and medical imaging.

BEST AVAILABLE COPY

Requiring the copyright label to be a reliable property identification tool imposes following basic functional requirements on the system:

- (1) The image must contain a label or code, which marks it as property of the copyright holder.
- (2) The image data must contain a user code, which verifies the user is in legal possession of the data.
- (3) The image data is labeled in a manner which allows its distribution to be tracked.

It is assumed, the main purpose of any attack would be to make the embedded label unverifiable. There are essentially two general ways to make the embedded label unverifiable: (1) alter the image data to render the copyright label unreadable, and (2) show that the label is not a reliable identification tool.

In addition several properties of digital data and design constraints, which are related to preventing attack on the copyright label, should be considered carefully: First, forgery of a digital copyright can only be prevented, if a forger cannot produce a valid copyright code. Second, the basic nature of digital images ensures that the copyright label can be easily altered if an attacker can identify the label data. Third, most digital images found in a multimedia environment can be low pass filtered, transformed to a different format or color space, or carefully re-quantized and compressed without significantly altering the images appearance or affecting its value. Finally, the image data is the only random sequence available to mark the data, and the statistics of the images, although generally unknown, are not under the control of the copyright system.

In sum, each of these points represents a potential means of attacking the copyright label and the following functional specifications are designed to prevent these attacks:

- (1) A secret key type encryption code must be created using the unique identification of a work and used as the copyright label to prevent forgery of labeling.
- (2) The image data must camouflage the copyright label code both visually and statistically to prevent an attacker from finding and deleting it. The functional requirement stating that the copyright label appears to be part of a normal image sequence and visually transparent is designed to prevent this attack.
- (3) The signals used to embed the copyright label must contain a noise margin in resist damage if the image is processed or compressed.
- (4) The system must be designed in such a way that the copyright labels locations and the same copyright

code are not used repeatedly for embedding codes in different images to prevent the label from being found by comparing different images signed by the same owner.

The noise margin created by modeling the lossy compression allows for some loss of energy in the pulse, before the pulse becomes unreadable. Therefore if the pulse energy is concentrated at low frequencies, the embedded code should be relatively robust. Unfortunately, the final consideration with regard to pulse design and visual camouflaging, is in direct conflict with using low frequency pulse shapes. Specifically, it is widely accepted that noise in the low frequency components of images is more noticeable than noise in the high frequency components. This is the basic concept behind the very efficient transform and sub-band coding techniques [8-10]. A reasonable trade-off between protection against processing attacks and visibility of the embedded code, is to make the pulses bandpass processes. Some additional design criteria must be developed to allow both requirements to be met simultaneously.

3 System Framework

The proposed approach, called Randomly Sequenced Pulse Position Modulated Code (RSPPMC) copyright labeling, is rooted in the well-known fact that typical digital images of people, buildings and natural settings can be considered as non-stationary statistical processes, which are highly redundant and tolerant of noise [8]. Hence, changes in the image data caused by moderate levels of wideband noise or controlled loss of information are hardly visibly noticeable, even when the altered images are compared directly with the original images.

Furthermore, the statistics of image sequences are only locally stationary and a priori unknown. More importantly, the process which produces such a sequence has random properties, which prevent the sequence from being reproduced exactly by a second experiment. This type of random signal is ideally suited for the purpose of statistically masking a sparse sequence of moderately large pulses.

The RSPPMC method consists of splitting the problem into two components. The first component produces the actual copyright code and a random sequence of locations for embedding the code in the image. This component is designed with the intention of implementing it, using existing encryption and pseudo random number generation techniques [11,12]. In fact,

BEST AVAILABLE COPY

(these methods are only discussed to establish a framework for developing a novel technique for embedding data in images. The second component actually embeds the code at the specified locations, using a simple pulsing method, designed to appear to be a natural part of the image, which yet resists being damaged through simple processing techniques. This component consists of four steps:

- (1) The position sequence is used to generate a sequence of pixel mapped locations where the code will be embedded.
- (2) The blocks of 2-D image data, $y(k,l)$ where k,l are the indices of discrete image points, are locally transformed and quantized at the locations selected in step 1, in a manner reflecting acceptable information loss in the image for the application to produce a 2-D image residual, $n(k,l)$, in which the RSPPMC will actually be embedded.
- (3) The code pulses, i.e. high or low, representing the binary code being embedded, are superimposed on the signal $n(k,l)$ selected locations.
- (4) The quantized data is decoded; and then, inversely transformed to produce the labeled image data.

In order to comply with functional requirements related to robustness, the transformation used in the second step includes the color space transformation and sub-banding and/or frequency transformations to allow direct access to the appropriate frequency bands in the gray scale component of an image. A quantization process is included in this step to guarantee that the label will survive a specific amount of information loss. A JPEG Compression Standard Based RSPPMC Copyright Label will be described in the next section.

4 Embedding = RSPPMC in Quantized JPEG Coefficients

Considering the functional requirement of robustness in a multimedia environment, the loss model in step 2 of the label process should be based on an industrial standard. From this perspective, image compression schemes used in GIF, TIFF, MPEG and JPEG are of interest. However, the wide spread use and growth of the JPEG [9] and MPEG formats and their efficiency in compressing images make transform coding the obvious choice for designing a copyright labeling system. Also, transform coding and/or sub-band coding techniques have the advantage of allowing direct access to specific frequency bands in the image, where the RSPPMC is to be embedded. This eliminates the

problem of designing and detecting bandpass wavelets.

The basic characteristics of images, which make transform quantization a useful image data compression tool are (1) images are generally low pass processes, and (2) high frequency image components have little visual impact.

The DCT representation of images has been widely researched [10]. The typical characteristics of image DCT's are also well known. Readers unfamiliar with the DCT and image transform quantization should refer to [8-10] for details.

The second point allows the higher frequency coefficients to be more coarsely quantized than the low frequency components by the transform quantizer. Presumably, the JPEG transform quantizer utilizes this fact by increasing $q(k,l)$ as a function of the increasing frequency vector normal.

Using these assumptions, several signals can be derived from the image data $Y(i,j)$, which naturally contain pulses meeting the requirements outlined in section 2. One of the simplest is the sub-block signal,

$$N(k_1,l_1,k_2,l_2) = |Y_Q(k_1,l_1)| - |Y_Q(k_2,l_2)| \quad (1)$$

where $Y_Q(k_1,l_1)$, $Y_Q(k_2,l_2)$ are the quantized coefficient values in the selected locations. This non-stationary random process should have an expected value of approximately zero if $|k_1,l_1|$ is approximately equal to $|k_2,l_2|$. Also, the signal should have a moderate variance level in the middle frequency ranges, i.e. $1.5 \leq |k,l| \leq 4.5$, where scattered changes in the image data should not be noticeably visible. The specific frequencies being used to embed the pulses will be "hopped" in this range to increase the robustness of the signal and making it more difficult to find. The principle being employed here is identical to the concept of frequency hopped spread spectrum communications [13].

A logical choice for the detection of "highs" and "lows", based on the signal defined in (1) is decided high if:

$$N(k_1,l_1,k_2,l_2) > 0, \quad (2a)$$

and decided low if,

$$N(k_1,l_1,k_2,l_2) = 0. \quad (2b)$$

However, embedding the code in this signal must also take into account the JPEG quantization process and any noise margin added to the pulses in the code. Therefore, the test for a written high is set as:

$$|Y_Q(k_1,l_1)| > |Y_Q(k_2,l_2)| + p. \quad (3a)$$

BEST AVAILABLE COPY

where p is a noise margin factor. The corresponding equation for n written low is

$$|Y_Q(k_2, l_2)| > |Y_Q(k_1, l_1)| + p. \quad (3b)$$

Standard JPEG compression uses a "quality factor" to scale the quantization, allowing for different image qualities and compression factors. In order to guarantee that the copyright label will survive compressions up to a specific level compression, the quantization table should be scaled to the desired quality factor. Also, due to numerical problems (in calculating quantization step size according to quality factor, and in the quantization process) which can occur if the image is quantized with a JPEG quality greater than the designed factor for embedding the copyright code, some conditions must be met. They are not discussed in this paper because of the limited space.

The method used to embed the copyright label in the sequence, $N(k_1, l_1, k_2, l_2)$, is not complicated. The high/low pulse pattern of the copyright label code is forced on the natural sequence at the selected group locations using a minimum mean square error approach, if it does not occur naturally. More complicated pulse patterns may be developed for representing the high/low bit, e.g. to use combinations (i.e. relationships) of three quantized elements $Y_Q(k_1, l_1)$, $Y_Q(k_2, l_2)$, $Y_Q(k_3, l_3)$ to replace equation (3).

In summary, the random pulse signal and conditions for detecting naturally occurring highs and lows described in equations (1) - (3) are designed to survive a JPEG compression down to a specified quality level. Clearly, decreasing the quality factor for the copyright code will make the signal more robust. However, this will also reduce the number of naturally occurring bits in the sequence. In addition, a lower quality factor will increase the likelihood that the changes necessary to superimpose the embedded code on the signal will be noticeably visible.

5 Conclusions

Using the prototypes we have developed, the experimental results indicate that the design requirements, developed in sections 2 for embedding a copyright label in image data, can be met, using the JPEG model based RSPPMC method developed in section 4. In particular, it was demonstrated that a copyright label code could be embedded in several images, using pulses with sufficient noise margins to survive common processing, such as lossy compression, color space conversion, and low pass filtering.

However, these results also indicate significant room for improvement in the method. One possibility for improvement could be in use different frequency band sets for encoding the high and low pulses. Also, methods could be developed to utilize image restoration techniques and pattern recognition techniques for verifying copyright labels. For example, pattern recognition techniques could be used to read copyright labels from images which have been cropped. In addition, methods suitable for applications with special requirements, such as cartography and medical imaging, are currently being investigated.

The authors would like to acknowledge Scott Burgett and Jochen Rindfrey, for their contributions to this work.

References

- [1] B. Kahl, "The strategic environment for protecting multimedia", (IMA Intellectual Property Project Proceedings, vol. 1, no. 1, 1994, pp. 1-8.
- [2] E. Kueh, J. Rindfrey, J. Zhao, "Copyright Protection for Multimedia Data", *Proceedings of the International Conference on Digital Media and Electronic Publishing* (5-6 December 1994, Leeds, UK).
- [3] B.A. Lehman, R.H. Brown, "Intellectual Property and the National Information Infrastructure": Preliminary draft of the working group on intellectual property rights, July 1994.
- [4] G. Van Slyke, Natural language version of the generic CITED model, ESPRIT II CITED Project 5469, June 28, 1994.
- [5] A.J. Kitson and D.T. Scotton (eds.), Copyright Ownership Protection in Computer Assisted Training (COPICAT), Esprit Project 8195, Workpackage 2 (Requirements Analysis), Deliverable 1, June 3, 1994.
- [6] RACE M 1005, Access control and copyright protection for images (ACCOPI), Workpackage 1 Deliverable, July 1994.
- [7] K. Manusi and K. Tanaka, "Video-Steganography: How to secretly embed a signature in a picture," *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, 1994.
- [8] A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall, Englewood Cliffs, NJ, 1989.
- [9] G.K. Wallace, "The JPEG still picture compression standard", *Communications of the ACM*, vol. 34, no. 4, April 1991, pp. 30-40.
- [10] K.R. Rao and P. Yip *Discrete Cosine Transform: Algorithms, Advantages, Applications*, Academic Press, 1990.
- [11] G. J. Simmons, *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, New York, 1994.
- [12] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., New York, et al., 1994.
- [13] R. C. Dixon, *Spread Spectrum Systems*, 2nd ed., Wiley, New York, NY, 1984.

BEST AVAILABLE COPY

TOWARDS A ROBUST DIGITAL WATERMARK

R.G.van Schyndel(*), A.Z.Tirkel(+), C.F.Osborne(*)

(*) Department of Physics, Monash University, Clayton, 3168, Australia.

(+) Scientific Technology, P.O.Box 3018, E. Brighton, 3187, Australia.

Abstract

This paper discusses the feasibility of coding a robust, undetectable, digital water mark on a standard 512*512 intensity image with an 8 bit gray scale. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation. This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access. The method chosen is based on linear addition of the water mark to the image data. Originally, the authors made use of one dimensional encoding using m-sequences [1],[2], a process which, whilst showing promise, had considerable shortcomings. This paper presents an analysis of the one dimensional scheme and some constructions to extend this work to two dimensions.

1 Background

There exist two basic classes of electronic water marks: fragile and robust. Interest in both types has increased in recent times because of the explosion in digital communications and the rapidity and ease of transmission of electronic material which is subject to copyright. The authors have been concerned with the construction of the robust type, i.e. one which is resilient to some image distortions such as pixel or bit tampering, cropping, translation, rotation and shear. At this stage, our watermark possesses limited immunity against the first three distortions, but the intention is to improve its performance in the future. This should be contrasted with a novel technique involving a fragile watermark as described in [3], where, by deliberate design, any distortions render the watermark non-recoverable and this becomes proof of tampering. Both methods use LSB manipulation. Walton [3], also introduces an ingenious and effective palette manipulation technique to increase the watermark effectiveness by involving the complete RGB image components. A totally different technique and its variations is reviewed in [4]. Its major

advantage is its compatibility with the JPEG format, whilst its principal disadvantage is that the watermark recovery requires the presence of the unencoded image. In this respect it differs from the other techniques. Our technique involves a linear addition of the watermark pattern, followed by a correlative recovery. Correlation can be defined as; cyclic or extended, global or character specific.

Correlation functions can be decomposed into: even and odd, or periodic and aperiodic. At this stage we are confined to binary characters only. Our watermarks are chosen from two-dimensional array patterns based on m-sequences or extended m-sequences. An m-sequence basis is chosen because of their balance (zero mean), random appearance, resilience to filtering, cropping and individual bit errors, optimal autocorrelation properties and constrained cross-correlation. The water mark can be encoded by the choice of m-sequences and their phases.

2 Method

Our encoding method uses LSB addition for embedding the water mark [1], [2]. In many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence its manipulation is invisible, or of limited significance. The linear addition process is difficult to crack and makes it possible to embed multiple watermarks on the same image [2]. The decoding process makes use of the unique and optimal auto-correlation of m-sequence arrays to recover the watermark and suppress the image content. Since the correlation process involves averaging over long strings of binary digits, it is relatively immune to individual pixel errors, such as may occur in image transmission. The correlation process requires the examination of the complete bit pattern and must therefore be performed off-line, unless some form of dedicated, real-time, parallel processing is involved. The decoding process is not completely error free, due to partial correlation of the image data with the encoding sequence. In our previous work, we overcame this by filtering and dynamic range

BEST AVAILABLE COPY

compression [2]. These artificial steps would be undesirable in a practical system. A typical 128*128 (unfiltered) image encoded with a one-dimensional watermark is shown in Fig.1(Top left). The message is encoded on a line by line basis, using the ASCII character to select a sequence phase shift. There are numerous message repeats. The decoder output Fig.1(centre left) shows distinct message correlation peaks (white). Note that there are significant sidelobes due to image crosscorrelation effects. The top half of Fig.1. shows encoded images that have been progressively high-pass filtered, removing 10, 60 and 100 of the spatial frequency components from the total of 128. The watermark peaks survive all these filtering processes, demonstrating the robustness of the technique. The image content in the original and the decoded version is rendered negligible after the second or third of the filters. It is also clear that the filtering introduces progressively more severe ringing in the decoded output. This can result in ambiguities. We are presently investigating the feasibility of rectifying this shortcoming by the introduction of a matched filter in the decoding process. Fig.2. shows similar effects on the watermark alone (encoded on a null image). Contrast enhancement was employed to render the watermark visible.

3. Watermark requirements

An ideal watermark would possess:

- (i) High in-phase autocorrelation peak for rows and columns [All]
- (ii) Low out-of-phase autocorrelation for rows and columns [Costas Arrays]
- (iii) Low cross-correlation between rows and between columns & between rows and columns [Perfect Maps, Hadamard Matrix, Legendre Arrays]
- (iv) Low cross-correlation with image content [Folded M-sequence]
- (v) Array diversity [Gold, Extended Gold Arrays]
- (vi) Balance [All except Costas and some Gold]

The first two criteria are required for unambiguous watermark registration, the third is necessary to avoid scrambling, the fourth minimises image related artefacts, whilst the fifth is concerned with the information capacity of the watermark. The sixth criterion maximises the significance of the correlation operation: in the binary case, the minority symbol determines the correlation score. Constructions can be optimised for each of these requirements. However, a global optimisation requires compromise. We have examined all the criteria in detail, with the exception of (iv).

Presently, we are examining methods of watermark design to minimise crosscorrelation with the image.

3.1 Image crosstalk suppression (ideal)

Clearly, it is possible to analyse the image content, by DCT or Walsh Transform and deduce a low crosscorrelation watermark by remapping any pattern, satisfying all criteria above except (iv). Similar effects could be assured by a random or adaptive search for a mapping to minimise the crosscorrelation with the image. However, such a procedure is impractical because there is no guarantee of uniqueness and hence the computation of the inverse mapping at the decoder.

3.2 Crosstalk suppression (practical)

There are at least three approaches which do not suffer from the above problem.

- (1) Use longer m-sequences
- (2) Use high pass filtering.
- (3) Use a "random" mapping.

The first is obvious. The other methods rely on the low overlap of the spatial frequency content of the image and watermark. In most cases (except

BEST AVAILABLE COPY

random or fractal images), the image exhibits a (peaked) spatial frequency content constrained to low frequencies. By contrast, the m-sequence content is almost perfectly white. Therefore, as demonstrated by Fig.1., high pass filtering can reduce image related artefacts, without significantly degrading the peak.

3.3 Analysis

(3) requires an appreciation of the significant moments of the cross-correlation. Since the mean is subtracted from the image in the decoding stage, the correlation is that between two zero-mean functions and hence is itself zero. The variance, however is not so easily constrained. It is the main source of high cross-correlation peaks. Intuitively, this variance can be calculated by resolving each function into an orthogonal basis and applying random-phase statistics to each component. (A one dimensional analogy of this analysis is presented in the Appendix). The cross-correlation can therefore be expressed as a restricted summation over the m overlapping components. In the case of a "white" image, the total 2^m-1 components would contribute. Hence, assuming laws of large numbers, the ratio of variances is:

$$\frac{\sigma_w}{\sigma_m} \approx \sqrt{\frac{m}{2^m-1}} \quad 1$$

A more complete analysis of these phenomena is presented in the Appendix.

For example, a linear image of 312 pixels can be expressed as a summation of 32 DCT components.

The improvement offered by "whitening" is approximately a factor of 4.

It is not necessary to modify the image in order to implement this "whitening" process. It can just as easily be performed by embedding the m-sequence on the image with "random" pixel offsets, or by performing an orderly interleaving operation. The random offsets can be obtained from the m-sequence vector ($n \times 1$) for one dimensional or ($n \times m$) for two dimensional patterns. We are presently investigating and comparing the performance of this technique against that of high-pass filtering.

4 Two-dimensional m-sequence based arrays

M-Sequences can be formed from starting vectors by a Fibonacci recursion relation. They are of

maximal length (2^m-1) for a vector of length m . The autocorrelation function of an m-sequence is two valued: 2^m-1 (in phase), -1 (out of phase).

4.1 Extension of one dimensional arrays

A two-dimensional construction can be performed using a row by row phase shift. The effect on columns is that of decimation. Unique phase shifts as determined from Galois Field theory lead to the formation of columns, which are themselves m-sequences. The resulting array is an unbalanced Hadamard Matrix. Alternatively, a long sequence can be folded diagonally into an array format [5]. In this manner, the desirable one-dimensional autocorrelation property can be extended to two dimensions. The encoding and decoding performance of the Hadamard technique suffers from the image related effects because the correlations are performed in the (short and thus interference prone) row or column basis. The folded m-sequence is more immune to these effects, owing to its increased length. However, its information storage capacity is inferior. Watermarks encoded by both methods are presented, compared and analysed in the paper.

4.2 Intrinsic 2D constructions

We have also studied other fundamentally two-dimensional constructions. Costas Arrays are optimal in that their out-of-phase autocorrelation is minimum for shifts in either or both dimensions [6] (Uniformly low sidelobe point-spread-function). They have been successfully deployed in radar and sonar, where time delays and frequency shifts (Doppler) can occur simultaneously. However, they are highly unbalanced and therefore prone to image related artefacts. Perfect Maps are constructions, where every $m \times n$ basis vector occurs once in a large pattern or map and hence can be used for automatic location. (An m-sequence is a one dimensional example of this category). The construction algorithm for Perfect Maps of large dimensions, commensurate with our image sizes is complicated [7]. However, some perfect maps are also Hadamard Matrices. We have examined examples of these, but still found them to be inadequate at rejecting image related artefacts. Legendre sequences and modified Legendre sequences, which are based on a quadratic residue (modulo n) and are similar to m-sequences of non-maximal length are also being studied. They are expected to improve on m-sequences for short lengths only. Extended m-sequences are attractive because they are commensurate with the image size (2^n). Whenever the extension by adding a zero to the m-sequence is performed to the longest

BEST AVAILABLE COPY

run lengths of zeros, the resulting sequence still exhibits a strong in-phase autocorrelation peak of 2^n . This peak is surrounded by n zero values on either side, making it easy to recognise by filtering techniques. However, this is at the expense of numerous sidelobes at other phase shifts. The effect of these is being investigated. Gold Codes are linear additions of a preferred pair of m -sequences in with a prescribed relative phase shift.

Alternatively, they can be viewed as sequences generated by a non-maximal feedback configuration shift register constructed to implement a product of the individual m -sequence generating polynomials. The family of codes generated by all the relative phase shifts and the original parent m -sequences in 2^{n-1} , of which approximately half are balanced. The auto and cross correlations are constrained to approximately $2^{n/2}$. These linear codes can be folded into array format, just as m -sequences. They offer greater information storage capacity because of their great diversity and constrained correlations. Gold codes can also be extended to length 2^n in a similar manner to m -sequences.

5 Conclusion

This paper presents a method of encoding and the recovery of a (two-dimensional digital) water mark on test images. The performance of the recovery process is analysed and improvements suggested.

6 References

- [1] A.Z.Tirkel, G.A.Bankin, R.M.van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. Electronic Water Mark. DICTA-93 Macquarie University, Sydney, December 1993, p.666-672.
- [2] R.G. van Schyndel, A.Z.Tirkel, N.R.A.Mee, C.F.Osborne. A Digital Watermark. First IEEE Image Processing Conference, Houston TX, November 15-17, 1994, vol II, p.86-90.
- [3] E.Walton. Image Authentication for a Slippery New Age. Dr.Dobb's Journal, April 1995, p.18-26, 42-47.
- [4] F.M.Boland, I.K.K. O'Ruanaidh and C.Dautzenberg. Watermarking Digital Images for Copyright Protection.
- [5] F.J. MacWilliams and N.J.A.Sloane. Pseudo-random Sequences and Arrays. Proc.IEEE, vol 64, 1715-1729, Dec. 1976.
- [6] S.W.Golomb and H.Taylor. Two-Dimensional Synchronization Patterns for Minimum Ambiguity. IEEE Trans. on Information Theory, vol 11-28, no.4, p.600-604, July 1982.
- [7] T.Fitzell. Construction for Perfect Maps and Pseudorandom Arrays. IEEE Trans. on

Information Theory, vol 34, no 5, p.1308-1317, September 1988.

APPENDIX

Consider, for the sake of simplicity, a 512 pixel, one dimensional image $I(x)$ and an encoding m -sequence $M(x)$. This analysis can be extended to two dimensions. Both functions can be expressed as Fourier sums:

$$I(x) = \sum_{n=1}^{2^{n-1}} I_n \cos(\omega_n x + \phi_n) \quad (A1)$$

and since the m -sequence distribution is white,

$$M(x) = \sum_{m=1}^{2^{n-1}} m \cos(\omega_m x + \phi_m) \quad (A2)$$

The encoding process can be described by:

$$W(x) = I(x) - cM(x) \quad (A3)$$

where, in our case, c corresponds to LSB scaling. The decoding process involves the following:

1. Remove mean.
2. Perform correlation with a reference m -sequence in particular phase.
3. Repeat for all m -sequence phases.
4. Compare global correlation maximum and record m -sequence phase.

The correlation can be expressed as:

$$Y(\phi_m) = Y_m c + \sum_{n=0}^{2^{n-1}} \sum_{m=1}^{2^{n-1}} I_n m \cos(\omega_n x_i + \phi_m) \quad (A4)$$

where Y_m is the two-valued autocorrelation function of the m -sequence (2^{n-1} for $m=1, -1$ otherwise). The first term contains information in n as the choice of sequence, whilst the summation term represents the interference (cross correlation with the image content). The value of m is determined by locating the maximum in $Y(\phi_m)$ in order to avoid false positive identification, missed detection and ambiguities, the image cross-correlation peaks must be smaller than that of the m -sequence. This cross-correlation has zero mean, but its variance can be estimated as:

$$\sigma_i = \langle Y(\phi_m) \rangle = \left[\sum_{n=0}^{2^{n-1}} \sum_{m=1}^{2^{n-1}} \frac{1}{2} I_n^2 \right]^{1/2} \quad (A5)$$

Where the random phase approximation and the laws of large numbers have been implied. A value of $\sigma_i < (2^n - 1)/6$ will guarantee correct detection unconditionally for images with Gaussian statistics.

BEST AVAILABLE COPY

Most physical images contain only a few significant spectral components (L), around 0 frequency. Assuming a rectangular distribution,

$$\sigma_y \approx \sigma_i \frac{2^{p-1}}{L^2} \quad (A6)$$

where σ_i is the image variance, whose maximum is approximately $256/6 \approx 43$ for a 256 gray scale gaussian image.

There are two obvious methods of minimising σ_y . High pass filtering the encoded image before performing the correlation will render the second term in (A4) negligible. However, the filter cut-in frequency is image-dependent. Also, this method introduces a degradation in the m-sequence autocorrelation peak (peak erosion) and an increase in sidelobe levels. There are also effects due to image content beyond the filter cut-in frequency (image leakage). Nevertheless, this method is capable of increasing the peak-to-sidelobe ratio by a factor of 2.

The second method of relative "whitening" described in the main text does not suffer from the above deficiencies, but does affect the spatial properties of the m-sequence. It is not clear if both techniques can be used in cascade, nor if they are commutative.

BEST AVAILABLE COPY

A TWO-DIMENSIONAL DIGITAL WATERMARK

A. Z. Tirkel(+), R. G. van Schyndel(*), C. F. Osborne(*)

(+)Scientific Technology,
P.O.Box 3018, Dandy Brighton, 3186, Australia.

(*) Department of Physics, Monash University,
Clayton, 3168, Australia.

ABSTRACT

This paper discusses the feasibility of coding a robust, undetectable, digital water mark on a standard 512*512 intensity image with an 8 bit gray scale. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation. This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access. The method chosen is based on linear addition of the water mark to the image data. Originally, the authors made use of one dimensional encoding using m-sequences [1],[2], a process which, whilst showing promise, had considerable shortcomings. This paper analyses constructions to extend this work to two dimensions and discusses compatibility of the technique with JPEG image transmission.

1 Review

There exist two basic classes of electronic water marks: fragile and robust. Interest in both types has increased in recent times because of the explosion in digital communications and the rapidity and ease of transmission of electronic material which is subject to copyright. The authors have been concerned with the construction of the robust type, i.e. one which is resilient to some image distortions such as pixel or bit tampering, cropping, translation, rotation and shear. Another form of robustness concerns lossy compression processing, such as coding via the Discrete Cosine Transform, such as JPEG. At this stage, our watermark possesses limited immunity against the first three pixel related distortions. In this paper, we discuss methods of addressing JPEG compatibility.

Our watermarking method differs significantly from the novel technique recently introduced by Walton [3]. This involves a fragile watermark, where, by deliberate design, any distortions render the watermark non-recoverable and this becomes proof of tampering. Both methods use LSB manipulation. Walton [3], also introduces an ingenious and effective palette manipulation technique to increase the watermark effectiveness by involving the complete RGB image components.

A totally different technique and its variations is reviewed in [4]. Its major advantage is its compatibility with the JPEG format, whilst its principal disadvantage is that the watermark recovery requires the presence of the unencoded image. In this respect it differs from the other techniques.

Our technique involves a linear addition of the watermark pattern, followed by a correlative recovery. Correlation can be defined as: cyclic or extended, global or character specific.

Correlation functions can be decomposed into: even and odd, or periodic and aperiodic. At this stage we are confined to binary characters only. Our watermarks are chosen from two-dimensional array patterns based on m-sequences or extended m-sequences. An m-sequence basis is chosen because of their balance (zero mean), random appearance, resilience to filtering, cropping and individual bit errors, optimal autocorrelation properties and constrained cross-correlation. The water mark can be encoded by the choice of m-sequences and their phases.

BEST AVAILABLE COPY

2. Method

Our encoding method uses LSB addition for embedding the water mark [1], [2]. In many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence its manipulation is invisible, or of limited significance. The linear addition process is difficult to crack and makes it possible to embed multiple watermarks on the same image [2]. The decoding process makes use of the unique and optimal auto-correlation of m-sequences arrays to recover the watermark and suppress the image content. Since the correlation process involves averaging over long strings of binary digits, it is relatively immune to individual pixel errors, such as may occur in image transmission. The correlation process requires the examination of the complete bit pattern and must therefore be performed off-line, unless some form of dedicated, real-time, parallel processing is involved. The decoding process is not completely error free, due to partial correlation of the image data with the encoding sequence. In our previous work, we overcame this by filtering and dynamic range compression [2]. These artificial steps would be undesirable in a practical system. A typical 128*128 (unfiltered) image encoded with a one dimensional watermark is shown in Fig.1(Top left). The message is encoded on a line by line basis, using the ASCII character to select a sequence phase shift. There are numerous message repeats. The decoder output Fig.1(centre left) shows distinct message correlation peaks (white). Note that there are significant sidelobes due to image crosscorrelation effects. The top half of Fig.1, shows encoded images that have been progressively high-pass filtered, removing 10, 60 and 100 of the spatial frequency components from the total of 128. The watermark peaks survive all these filtering processes, demonstrating the robustness of the technique. The image content in the original and the decoded version is rendered negligible after the second or third of the filters. It is also clear that the filtering introduces progressively more severe ringing in the decoded output. This can result in ambiguities. We are presently investigating the feasibility of rectifying this shortcoming by the introduction of a matched filter in the decoding process.

3. Watermark properties

An ideal watermark would possess:

- (i) High in-phase autocorrelation peak for rows and columns [All]
- (ii) Low out-of-phase autocorrelation for rows and columns [Costas Arrays]
- (iii) Low cross-correlation between rows and between columns & between rows and columns [Perfect Maps, Hadamard Matrix, Legendre Arrays]
- (iv) Low cross-correlation with image content [Folded M-sequences]
- (v) Array diversity [Gold, Extended Gold Arrays]
- (vi) Balance [All except Costas and some Gold]
- (vii) Compatibility with standard image transmission format such as JPEG [Folded M-sequences].
- (viii) Long span in order to prevent unauthorized cracking. [GMW codes]

The first two criteria are required for unambiguous watermark registration, the third is necessary to avoid scrambling, the fourth minimises image related artefacts, whilst the fifth is concerned with the information capacity of the watermark. The sixth criterion maximises the significance of the correlation operation: in the binary case, the minority symbol determines the correlation score.

The seventh criterion requires robustness against the low-pass filtering along a diagonal raster. It is described in more detail in 3.2. The eighth criterion relates to code inversion property. All codes can be generated by a recursion relation and this can be deduced from a sample of the code by solution of a set of simultaneous equations (matrix inversion). The minimum number of terms required for unambiguous inversion is called the span. M-sequences have a short span of $2n$, where n is the order of the polynomial describing the recursion relation. This is because of their linear nature. GMW codes

use non-linear recursion, which is optimised to yield much larger spans, with minimum impact on sequence properties. They are therefore ideal in situations where security is paramount. Constructions can be optimised for each of these requirements. However, a global optimisation requires compromise. We have examined all the criteria in detail with particular reference to (iv) [5] and (vii).

3.1 Image crosstalk suppression

Clearly, it is possible to analyse the image content, by DCT or Walsh Transform and deduce a low crosscorrelation watermark by remapping any pattern, satisfying all criteria above except (iv). Similar effects could be assured by a random or adaptive search for a mapping to minimise the crosscorrelation with the image. However, such a procedure is impractical because there is no guarantee of uniqueness and hence the computation of the inverse mapping at the decoder. There are at least three approaches which do not suffer from the above problem.

- (1) Use longer m -sequences.
- (2) Use high pass filtering.
- (3) Use a "random" mapping.

The first is obvious (longer averaging). The other methods rely on the low overlap of the spatial frequency content of the image and watermark. In most cases (except random or fractal images), the image exhibits a (peaked) spatial frequency content constrained to low frequencies. By contrast, the m -sequence content is almost perfectly white, as shown in Fig 2. Therefore, as demonstrated by Fig. 1., high pass filtering can reduce image related artefacts, without significantly degrading the peak.

3.2 JPEG compatibility

As already demonstrated in Fig. 1, the watermark is resilient against severe (0.25 quality factor) DCT high-pass filtering. Since the watermark mask is almost perfectly (spectrally) white, the same is true about low-pass filtering. In order to preserve this feature in raster format, the m -sequence should be embedded in a commensurate diagonal manner. The folded m -sequence of [5] is ideal for this purpose. The partitioning of the process into $8*8$ blocks should pose no significant problems. The m -sequence employed in Fig. 1. was 4 times longer than the linear dimension of the image, with no discernible effects on the result. We have actually experimented with $8*8$ blocks and found no surprises. The only disadvantage of JPEG processing is that the high-pass filtering method of image-related artefacts (section 3.1) is incompatible, with the low-pass filtering involved in image compression. The same is likely to apply to the random mapping technique. Hence, the suppression of image related effects can only be achieved by the use of longer sequences. This imposes a limit on the information content of the watermark. The effects of sequence length on information content have been discussed in [1]. Another feature of JPEG processing is the capability of performing image manipulations on-line. This poses no problems at the encoding stage of our watermark. However, the watermark recovery process requires the execution of a sliding correlation to determine the location of a global maximum. At present, this process is being performed sequentially and hence off-line. We are investigating hardware and software techniques to render these operation parallel. Alternatively, a DCT-based correlation computation could be devised. This is also being examined.

4 Two-dimensional m -sequence based arrays

M -Sequences can be formed from starting vectors by a Fibonacci recursion relation. They are of maximal length (2^n-1) for a vector of length n . The autocorrelation function of an m -sequence is two valued: 2^n-1 (in phase), -1 (out of phase).

4.1 Extension of one dimensional arrays

A two-dimensional construction can be performed using a row by row phase shift. The effect on columns is that of decimation. Unique phase shifts as determined from Galois Field theory lead to the formation of columns, which are themselves m -sequences. The resulting array is an unbalanced Hadamard Matrix. Alternatively, a long sequence can be folded diagonally into an array format [5]. In this manner, the desirable one-dimensional autocorrelation property can be extended to two dimensions. The encoding and decoding performance of the Hadamard technique suffers from the image related effects because the correlations are performed on the (short and thus interference prone) row or column basis. The folded m -sequence is more immune to these effects, owing to its increased length. However, its information storage capacity is inferior. Watermarks encoded by both methods are presented, compared and analysed in the paper.

4.2 Intrinsic 2D constructions

We have also studied other fundamentally two-dimensional constructions. Costas Arrays are optimal in that their out-of-phase autocorrelation is minimum for shifts in either or both dimensions [6]. (Uniformly low sidelobe point-spread-function). They have been successfully deployed in radar and sonar, where time delays and frequency shifts (Doppler) can occur simultaneously. However, they are highly unbalanced and therefore prone to image related artefacts. Perfect Maps are constructions, where every $m \times n$ basis vector occurs once in a large pattern or map and hence can be used for automatic location. (An m -sequence is a one dimensional example of this category). The construction algorithm for Perfect Maps of large dimensions, commensurate with our image sizes is complicated [7]. However, some perfect maps are also Hadamard Matrices. We have examined examples of these, but still found them to be inadequate at rejecting image related artefacts. Legendre sequences and modified Legendre sequences, which are based on a quadratic residue (modulo n) and are similar to m -sequences of non-maximal length are also being studied. They are expected to improve on m -sequences for short lengths only. Extended m -sequences are attractive because they are commensurate with the image size (2^n). Whenever the extension by adding a zero to the m -sequence is performed to the longest run length of zeros, the resulting sequence still exhibits a strong in-phase autocorrelation peak of 2^n . This peak is surrounded by n zero values on either side, making it easy to recognise by filtering techniques. However, this is at the expense of numerous sidelobes at other phase shifts. The effect of these is being investigated. Gold Codes are linear additions of a preferred pair of m -sequences with a prescribed relative phase shift. Alternatively, they can be viewed as sequences generated by a non-maximal feedback configuration shift register constructed to implement a product of the individual m -sequence generating polynomials. The family of codes can be generated by all the relative phase shifts and the original parent m -sequences in 2^n+1 , of which approximately half are balanced. The auto and cross correlations are constrained to approximately $2^{n/2}$. These linear codes can be folded into array format, just as m -sequences. They offer greater information storage capacity because of their great diversity and constrained correlations. Gold codes can also be extended to length 2^n in a similar manner to m -sequences.

4.3 Extensions to Multi-Dimensional Arrays

So far, our watermarking scheme has been confined to one and two-dimensional spatial constructions employing a gray scale image. Extensions to colour (RGB) encoding have the potential of enlarging the dimensionality to a total of 3. This could be employed for:

- (i) Increasing the information content of the watermark. For example, three independent, two-dimensional messages could be encoded instead of one.
- (ii) Increasing the length of the watermark code to reduce image related effects.
- (iii) Redundancy coding.

- (iv) Novel, multi-dimensional array coding.
- (v) Non-binary character sequences.

These aspects are presently being evaluated.

4.4 Non-imaging applications

The watermarking technique discussed here has potential applications to audio copyright protection and audio system and equalisation control. Two one-dimensional patterns can be embedded in each of the stereo channels on CD-ROM or DAT. These codes could be designed to have a deliberately long span (such as GMW codes), in order to prevent cracking. This technique offers potential resistance to resampling/subsampling, which are akin to scaling/rotation. These codes could also be employed in automatic spectral and delay calibration/equalisation of the sound system, because of their optimal impulse response. This feature could be particularly useful in dynamic situations, where the audio environment is constantly changing.

5 Conclusion

This paper presents a method of encoding and recovery of a two-dimensional digital water mark on test images. The compatibility of the watermarking process with JPEG coding is discussed.

6 Acknowledgements

The authors would like to extend their gratitude to Nicholas Mee and Gerard Rankin for their assistance in mathematical theory and computer based sequence generation and analysis respectively. Their contributions have been invaluable.

7 References

- [1] A.Z.Tirkel, G.A.Rankin, R.M.van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. Electronic Water Mark. DICTA-93 Macquarie University, Sydney, December 1993. p.666-672.
- [2] R.G. van Schyndel, A.Z.Tirkel, N.R.A.Mee, C.F.Osborne. A Digital Watermark. First IEEE Image Processing Conference, Houston TX, November 15-17, 1994, vol II, p.86-90.
- [3] S.Walton. Image Authentication for a Slippery New Age. Dr.Dobb's Journal, April 1995. p.18-26, 82-87.
- [4] F.M.Boland, J.K.K. Ó Rouanaidh and C.Dautzenberg. Watermarking Digital Images for Copyright Protection.
- [5] F.J. MacWilliams and N.J.A.Sloane. Pseudo-random Sequences and Arrays. Proc.IEEE, vol 64, 1715-1729, Dec.1976.
- [6] S.W.Golomb and H.Taylor. Two-Dimensional Synchronization Patterns for Minimum Ambiguity. IEEE Trans. on Information Theory, vol IT-28, no.4, p.600-604, July 1982.
- [7] T.Etzion. Construction for Perfect Maps and Pseudorandom Arrays. IEEE Trans. on Information Theory, vol 34, no 5, p.1308-1317. September 1988.

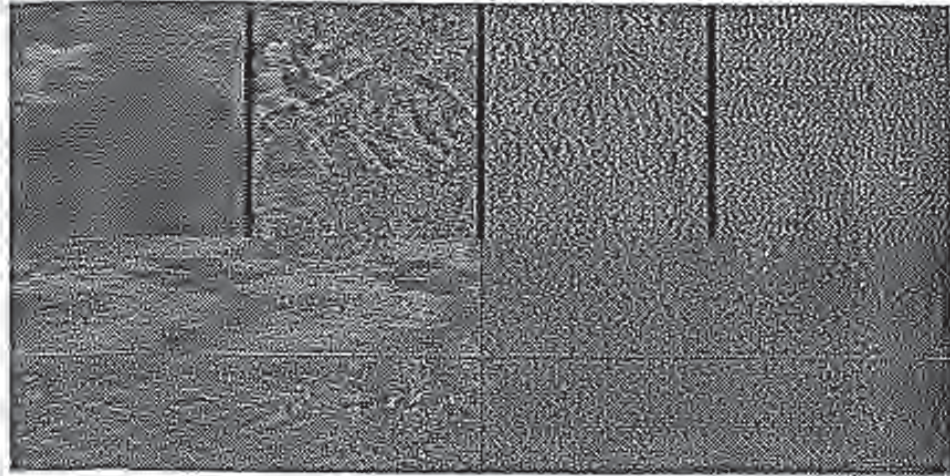


Figure 1
 Upper (left to right): Encoded image after high pass filtering, removing
 (a) 0, (b) 10, (c) 60, (d) 100 of 128 Spatial Frequency Components
 Lower (Centre Left, Bottom Left, Centre Right, Bottom Right) : Corresponding Decoded Patterns
 (Medium gray=0, darker=negative, lighter=positive - all image intensities have been suitably scaled)

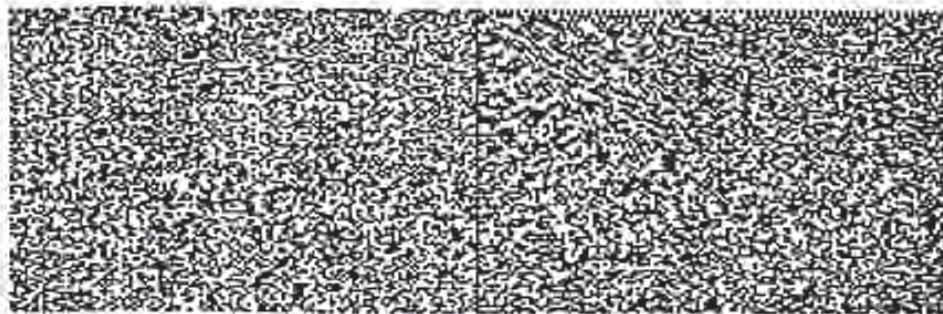


Fig 2.
 Left - DCT of watermark
 Right - DCT of image
 (Interpretation as in Fig 1)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGES CUT OFF AT TOP, BOTTOM OR SIDES

IMAGES NOT SQUARE

IMAGES NOT FULL FRAME FOR DRAWINGS

SKEWED/SIANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



IMAGE WATERMARKING - A SPREAD SPECTRUM APPLICATION

Anatol.Z.Tirkel* (Senior Member), Charles F Osborne, Ron G. van Schyndel

*Scientific Technology, 3/9 Barnato Gve., Armadale 3143 Australia
 Department of Physics, Monash University, Clayton 3168 Australia
 Andrew.Tirkel@scl.monash.edu.au

ABSTRACT

This paper discusses the feasibility of coding a robust, undetectable, digital water mark on a standard 512x512 intensity image with an 24 bit RGB format. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation.

This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access. The method chosen is based on linear addition of the water mark to the image data. The patterns adopted to carry the watermark are adaptations of m-sequences in one and two dimensions. The recovery process is based on correlation, just as in standard spread spectrum receivers. The technique is quite successful for one dimensional encoding with binary patterns, as shown for a variety of gray scale test images. A discussion of extensions of the method to two dimensions, RGB format and non-binary alphabets is presented. A critical review of other watermarking techniques is included.

1 BACKGROUND

The art of hiding messages in written text was known to the ancient Greeks as steganography. Many ingenious schemes to achieve that objective have been devised over the centuries. However, the more recent development of computer technology and the proliferation of image and graphics type data have generated the capability and the motivation for electronic watermarking as a means of copyright protection. There exist two basic classes of electronic water marks: fragile and robust. This paper is concerned with the construction of the robust type, i.e. one which is resilient to some image distortions such as pixel or bit tampering, cropping, translation, rotation and shear. At this stage, such a watermark possesses limited immunity against the first three distortions, but the intention is to improve its performance in the future. This should be contrasted with a novel technique involving a fragile watermark as described in [3], where, by deliberate design, any distortions render the watermark non-recoverable and this becomes proof of tampering. Both methods use LSB manipulation. Waiton [3], also introduces an ingenious and effective palette manipulation technique to increase the watermark effectiveness by involving the complete RGB image components. A totally different technique and its

compatibility with the JPEG format, whilst its principal disadvantage is that the watermark recovery requires the presence of the unencoded image. In this respect it differs from the other techniques. Other techniques being investigated are concerned with encryption of JPEG bit stream and involve the use of checksums [14]. The technique described here involves a linear addition of the watermark pattern, followed by a correlative recovery. Correlation can be performed as cyclic or extended, global or character specific operations. Novel methods of defining correlation can be devised. The traditional decomposition of correlation functions into even and odd, or periodic and aperiodic components does not apply, because the embedding pattern has periodicity commensurate with that of the image. So far, the watermarks have been chosen from one and two-dimensional array patterns based on m-sequences or extended m-sequences [5]. An m-sequence basis is chosen because of their balance (zero mean), random appearance, optimal autocorrelation properties and constrained cross-correlation. The water mark has been encoded by the choice of m-sequences and their phases.

2 METHOD

The encoding method uses LSB addition for embedding the water mark [1], [2], [8], [13]. A similar method has since been developed commercially by Digimarc [10], who add random multiples of the LSB on a pixel by pixel basis. Their decoding process is subtractive in the presence of the unencoded image and seems to be correlative in its absence. The extension of the scheme described here to multiple LSB's has been considered to be an integral part of the transition to a non-binary alphabet, such as that offered by the RGB format. The restriction to LSB manipulation has certain advantages, since in many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence this form of implementation renders the watermark invisible. Our present technique involves the addition of unfiltered m-sequences, although it is possible to devise a matched filter, such that the spectral components of the watermark match those of the image. This reduces the visibility of the watermark and permits the use of higher order bits in the encoding process. Another benefit of such filtering is that it ensures that any distortions due to lossy image compression or transmission errors affect the watermark and the image equally. Therefore, as long as the image is acceptable, so is the watermark.

The only significant case where watermarks are readily detectable is that of computer generated images, which are free of noise. In that instance, other means of

BEST AVAILABLE COPY

watermarks on the same image [2]. The decoding process makes use of the unique and optimal auto-correlation of m-sequence arrays to recover the watermark and suppress the image content. Since the correlation process involves averaging over long strings of binary digits, it is relatively immune to individual pixel errors, such as may occur in image transmission. The correlation process requires the examination of the complete bit pattern and must therefore be performed off-line, unless some form of dedicated, real-time, parallel processing is involved. Presently, two image processing hardware platforms (SGS Thomson IMSA100 and a Philips OPTIC-Optimized Pixel Template Image Correlator) are being evaluated as candidates for on-line performance of the decoding algorithm. The decoding process is not completely error free, due to partial correlation of the image data with the encoding sequence. The presence of significant correlation between the image and the watermark typically results in false peaks and true peak erosion. This in turn can result in ambiguous or false decoding. In previous work, this was overcome by filtering and dynamic range compression [2]. These artificial steps would be undesirable in a practical system. Other means such as redundancy coding restrict the data content of the watermark. Morphological methods of peak detection, based on the unique neighbourhood characteristics of the pixel corresponding to the peak correlation have been evaluated, but so far the improvement attributable to them appears similar to that of filtering. Neural nets trained for local peak detection are another option for future evaluation.

A typical 128*128 (unfiltered) image encoded with a one dimensional watermark is shown in Fig.1(Top left). The message is encoded on a line by line basis, using the ASCII character to select a sequence phase shift. There are numerous message repeats. The decoder output Fig.1(centre left) shows distinct message correlation peaks (white). Note that there are significant sidelobes due to image crosscorrelation effects. The top half of Fig.1 shows encoded images that have been progressively high-pass filtered, removing 10, 60 and 100 of the spatial frequency components from the total of 128. The watermark peaks survive all these filtering processes, demonstrating the robustness of the technique. The image content in the original and the decoded version is rendered negligible after the second or third of the filters. A different presentation of this process is shown in Fig.2.

3. WATERMARK PROPERTIES

An ideal watermark would possess:

- (i) High in-phase autocorrelation peak for rows and columns
- (ii) Low out-of-phase autocorrelation for rows and columns
- (iii) Low cross-correlation between rows and between columns & between rows and columns
- (iv) Low cross-correlation with image content
- (v) Array diversity
- (vi) Balance
- (vii) Compatibility with standard image transmission format such as JPEG
- (viii) Long span, in order to prevent unauthorised cracking.

The first two criteria are required for unambiguous

whilst the fifth is concerned with the information capacity of the watermark. The sixth criterion maximises the significance of the correlation operation: in the binary case, the minority symbol determines the correlation score.

The seventh criterion requires robustness against the low-pass filtering along a diagonal raster. The eighth criterion relates to code inversion property. All codes can be generated by a recursion relation and this can be deduced from a sample of the code by solution of a set of simultaneous equations (matrix inversion). The minimum number of terms required for unambiguous inversion is called the span. M-sequences have a short span of $2n$, where n is the order of the polynomial describing the recursion relation. This is because of their linear nature. GMW codes use non-linear recursion, which is optimised to yield much larger spans, with minimum impact on sequence properties. They are therefore ideal in situations where security is paramount. The sidelobe performance of these has not yet been evaluated. A search for a mapping to convert two dimensional arrays into GMW format is continuing.

Constructions can be optimised for each of these requirements. However, a global optimisation requires compromise. All criteria have been examined in detail with particular reference to (iv) [8] and (vii).

4. TWO-DIMENSIONAL M-SEQUENCE ARRAYS

M-Sequences can be formed from starting vectors by a Fibonacci recursion relation. They are of maximal length i.e. (2^n-1) for a vector of length n . Typically, the alphabet of symbols used to generate the sequence forms a finite base field, a Galois Field (GF). In most applications, binary or binary derived base fields such as GF(2) are involved. A good review of non-binary base field applications can be found in [12]. The recursion relation can be described by a generating polynomial over the GF. These polynomials, whose roots are not elements of the base field, themselves form an extension field. Their solutions (in the extension field) are powers of each other, which is equivalent to sequences being decimations of each other.

Two dimensional patterns are generated by polynomials in two variables. This is equivalent to a two-dimensional shift register. One dimensional polynomials have been studied extensively, whilst higher dimensional constructions have been devised ad-hoc, with specific applications in mind. [5] is one of the few references which attempts to treat this problem and its extensions to base fields other than GF(2).

4.1 SOME TWO-DIMENSIONAL CONSTRUCTIONS

The autocorrelation function of binary m-sequence is two valued: 2^n-1 (in phase), -1 (out of phase). A two-dimensional construction can be performed using a row by row phase shift. The effect on columns is that of decimation. Unique phase shifts as determined from Galois Field theory lead to the formation of columns, which are themselves m-sequences. The resulting array is an unbalanced Hadamard Matrix. Alternatively, a long sequence can be folded diagonally into an array format [5].

In this manner, the desirable one-dimensional autocorrelation property can be extended to two

BEST AVAILABLE COPY

the Hadamard technique suffers from the image related effects because the correlations are performed on the (short and thus interference prone) row or column basis. The folded m -sequence is more immune to these effects, owing to its increased length. However, its information storage capacity is inferior. We have encoded watermarks by both methods and have found them lacking.

There exist other fundamentally two-dimensional constructions. Costas Arrays are optimal in that their out-of-phase autocorrelation is minimum for shifts in either or both dimensions [6]. (Uniformly low sidelobe point-spread-function). They have been successfully deployed in radar and sonar, where time delays and frequency shifts (Doppler) can occur simultaneously. However, they are highly unbalanced and therefore prone to image related artefacts. Perfect Maps are constructions, where every m^n basis vector occurs once in a large pattern or map and hence can be used for automatic location. (An m -sequence is a one dimensional example of this category). The construction algorithm for Perfect Maps of large dimensions, commensurate with our image sizes is complicated. However, some perfect maps are also Hadamard Matrices. We have examined examples of these, but still found them to be inferior at rejecting image related artefacts.

4.3 EXTENSIONS TO NON-BINARY ALPHABETS

The watermarking scheme demonstrated in the diagrams has been confined to one and two-dimensional spatial constructions employing a gray scale image. Extensions to colour (RGB) encoding have the potential of expanding the capabilities. This could be employed for:

- (i) Increasing the information content of the watermark. For example, three independent, two-dimensional messages could be encoded instead of one.
- (ii) Increasing the length of the watermark code to reduce image related effects.
- (iii) Redundancy coding.
- (iv) Non-binary character sequences.

The last feature is of particular interest because of the difference between the encoding process of the watermark and the standard embedding of the spreading code on the carrier as practiced in spread spectrum communications. There, the use of QPSK calls for $GF(4)$ as a natural base field. It also permits the use of an isomorphism of the characters with complex roots of unity to derive convenient constructions of the complex correlation. The existence of two quadrature carriers is beneficial, but is quite irrelevant to the watermarking scheme. The RGB format permits the use of $GF(8)$ as a base field. An example of a two dimensional RGB pattern based on $GF(8)$ is shown in the presentation. This example uses the multiplication table based on each character being associated with a power of a primitive root of unity. This is not an essential requisite. A counter example is demonstrated by [12], who considers all possible algebras over $GF(4)$ for communications applications. Many of these algebras are not based on roots of unity. In our future work, we propose to examine $GF(8)$ in a similar manner. It may even be practical to combine two LSB's of RGB channels to construct a character set based on Galois Fields of dimension 64. These character sets can be generated from $GF(2)$ by numerous field

degeneracies to construct arrays which suppress the undesirable two-dimensional symmetries present in the McWilliams and Sloane folded m -sequence construction. These unattractive symmetries and a leading blank row/column are shown to be present in $GF(8)$ and survive transformation mappings based on m -sequences, as is shown in the presentation. Green [15] devises constructions of large size over $GF(2)$, which avoid these problems, but the minimum array size (91×45) and its aspect ratio is not conducive to imaging applications. It may be possible to construct square arrays over $GF(8)$ or $GF(64)$ based on algebraic degeneracy or adapt perfect maps to those non-binary character sets. In fact, it may be possible to devise a distance based correlation measure, as opposed to the use of complex multiplication. The merits of such a technique are still being investigated. It may also be feasible to reduce the spectral occupancy of the watermark by modulating RGB components alternately and using differential coding, as in a more generalised form of QPSK or Frank coding. Such a scheme could be incorporated into the JPEG conversion table. There may be applications of such techniques to spread spectrum communications, where QPSK is combined with polarization modulation.

5 NON-IMAGING APPLICATIONS

The watermarking technique discussed here has potential applications to audio copyright protection and audio system and equalisation control. Two one-dimensional patterns can be embedded in each of the stereo channels on CD-ROM or DAT. These codes could be designed to have a deliberately long span (such as GMW codes), in order to prevent cracking. These codes could also be employed in automatic spectral and delay calibration/equalisation of the sound system, because of their optimal impulse response. This feature could be particularly useful in dynamic situations where the audio environment is constantly changing. A technique called Argent has been located on the internet as a commercial version of CD copyrighting, but so far, meaningful details on this method have been unavailable.

6 CONCLUSIONS

This paper demonstrates a method of encoding and recovery of a digital watermark on test images, using spread spectrum techniques. A critical analysis of the extension of the method to genuine two-dimensional patterns using non-binary characters is presented. The ultimate objective is the construction of an optimal set of colour patterns. A brief outline of the current state of the art is included.

7 ACKNOWLEDGEMENTS

The authors would like to extend their gratitude to Dr. Alistair McAndrew, Nicholas Mee and Dr. Derek Rogers for the numerous helpful discussions on finite fields and coding theory.

BEST AVAILABLE COPY

- [1] A.Z.Turkel, G.A.Rankin, R.M.van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne, Electronic Water Mark. DICTA-93 Macquarie University, Sydney, December 1993. p.666-672.
- [2] R.G. van Schyndel, A.Z.Turkel, N.R.A.Mee, C.F.Osborne. A Digital Watermark. First IEEE Image Processing Conference, Houston TX, November 15-17, 1994, vol II, p.86-90.
- [3] S.Walton. Image Authentication for a Slippery New Age. Dr.Dobb's Journal, April 1995. p.18-26, 82-87.
- [4] F.M.Boland, J.K.K. Ó Rouanaídh and C.Dautzenberg. Watermarking Digital Images for Copyright Protection. In publication.
- [5] F.J. MacWilliams and N.J.A.Sloane. Pseudo-random Sequences and Arrays. Proc.IEEE, vol 64, 1715-1729, Dec.1976.
- [6] S.W.Golomb and H.Taylor. Two-Dimensional Synchronization Patterns for Minimum Ambiguity. IEEE Trans. on Information Theory, vol IT-28, no.4, p.600-604, July 1982.
- [8] R.G. van Schyndel, A.Z.Turkel, C.F.Osborne. Towards a Robust Digital Watermark, ACCV95 Conference, Nanyang Technological University, Singapore, December 5-8, 1995, vol 2, p.504-508
- [9] I.S.Reed and R.M.Stewart. Note on the Existence of Perfect Maps. IRE Trans. on Information Theory. vol IT-8, p.10-12, Jan. 1962
- [10] G.B. Rhoads. "Identification/Authentication Coding Method and Apparatus" Patent Application WO 95/14289.
- [11] M.Cooperman. Digital Information Commodities Exchange (DICE). Argent Algorithm used by CANE Records (Independent Music Label run by University of Miami) Ref. www.buyinfo/archive/95Q3/0084.html
- [12] D.P.Rogers. "Non-Binary Spread Spectrum Multiple-Access Communications". Ph.D.Thesis, Department of Electrical and Electronic Engineering, University of Adelaide, March 1995.
- [13] A.Z.Turkel, R.G.van Schyndel, C.F.Osborne. "A Two Dimensional Digital Watermark", DICTA'95, University of Queensland, Brisbane, December 6-8, 1995. p.378-383.
- [14] J.A.Lim, A.J.Maeder. "Image Authentication Extension for Lossy JPEG". DICTA'95, University of Queensland, Brisbane, December 6-8, 1995. p.210-216.
- [15] D.H.Green "Structural properties of pseudorandom arrays and volumes and their related sequences" IEE Proceedings, Vol 132, Pt.E, No.3, May 1985, p.133-145.

BEST AVAILABLE COPY

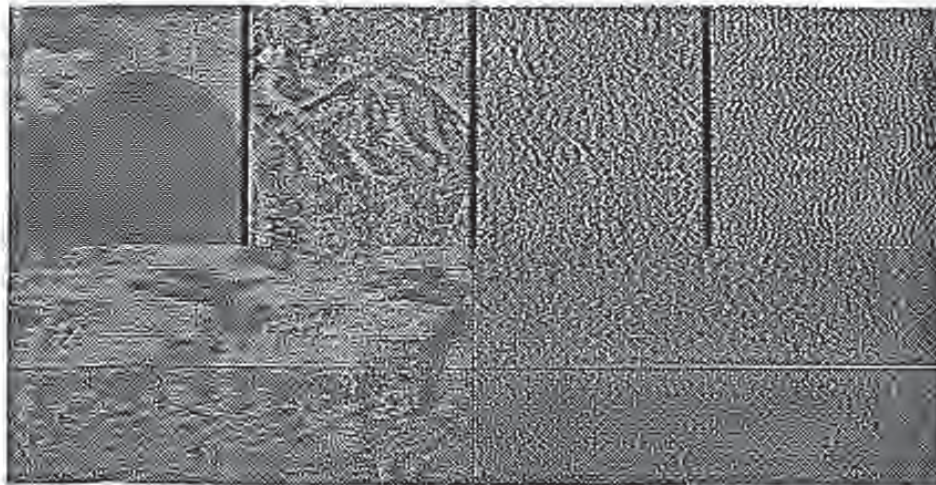


Figure 1

Upper (left to right): Encoded image after high pass filtering, removing
 (a) 0, (b) 10, (c) 60, (d) 100 of 128 Spatial Frequency Components

Lower (Centre Left, Bottom Left, Centre Right, Bottom Right) : Corresponding Decoded Patterns:

(medium gray=0, darker=negative, lighter=positive - all image intensities have been suitably scaled)

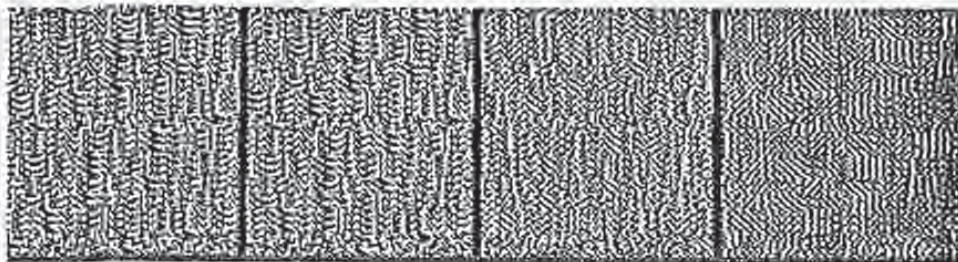
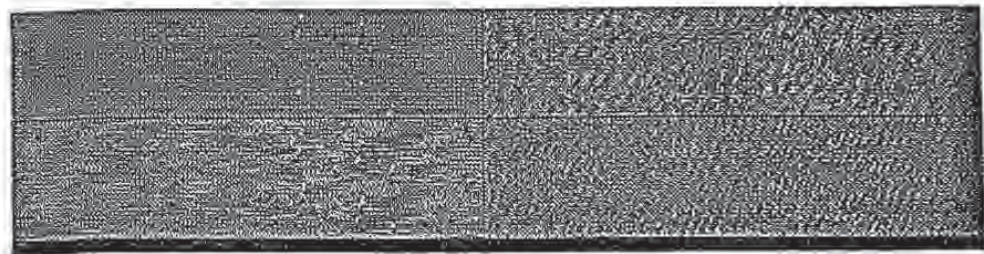


FIG 1.

BEST AVAILABLE COPY

Correlation presented in line format (Watermark peaks are clearly visible)



BEST AVAILABLE COPY

THE PROCEEDINGS

VISION, IMAGE AND SIGNAL PROCESSING

Volume 143, Number 4, August 1996

UNIVERSITY OF MINNESOTA
special section
from **IPA95**
LIBRARIES



BEST AVAILABLE COPY

Watermarking digital images for copyright protection

J.J.K. Ó Ruanaldh
W.J. Dowling
F.M. Boland

Indexing terms: Copyright protection, Image processing, Steganography, Spread spectrum communications

Abstract: A watermark is an invisible mark placed on an image that is designed to identify both the source of an image as well as its intended recipient. The authors present an overview of watermarking techniques and demonstrate a solution to one of the key problems in image watermarking, namely how to hide robust invisible labels inside grey scale or colour digital images.

1 Introduction

Computers, printers and high rate transmission facilities are becoming less expensive and more generally available. It is now feasible and very economical to transmit images and video sequences using computer networks rather than to send hard copies by post. In addition, images may be stored in databases in digital form. A major impediment to the use of electronic distribution and storage is the ease of intercepting, copying and redistributing electronic images and documents in their exact original form. As a result, publishers are extremely reluctant to use this means of disseminating material. The commercial possibilities for the World Wide Web are steadily becoming more appreciated. However, if these possibilities are to be realised, an integrated approach to the secure handling, issue and duplication of issued documents is required. Public key encryption systems such as the RSA algorithm [1-3] do not completely solve the problem of unauthorised copying because of the ease with which images may be reproduced from previously published documents. All encrypted documents and images need to be decrypted before they can be inspected or used. Once encryption is removed the document can be passed on in an electronic form. If there is more than one recipient of an image, there is no direct proof that any particular authorised recipient is responsible for passing it on to unauthorised users. The idea of using an indelible

watermark to identify uniquely both the source of an image and an intended recipient has therefore stimulated much interest in the electronic publishing and printing industries.

To be effective, an embedded watermark should be visually imperceptible, secure, reliable and resistant to attack.

Imperceptible. The image must not be visibly degraded by the presence of the mark. The mark should serve as a unique identifier with a high information content.

Secure and reliable. The mark must be strongly resistant to unauthorised detection and decoding. The watermark must also be capable of identifying the source and intended recipient with a low probability of error. It is also desirable that it would be difficult for an unauthorised agent to forge watermarks. Innovative error-control coding and digital signature techniques are required to ensure reliable and secure communication of the mark as well as authentication of the encoded message.

Robust. The mark must be robust to attack and must be tolerant to reasonable quality lossy compression of the image using transform coding, vector quantisation or any other technique. Standard image processing operations such as low pass filtering, cropping, translation and rescaling should not remove the mark.

Later we shall describe a method which fulfils most of the above requirements. In this paper, we argue that watermarking needs to be *adaptive* in order to be robust. In direct contrast to many other techniques, with the notable exception of Cox *et al.* [4], the method here places the watermark on the *most perceptually significant* components of an image. The logic behind the premise is quite simple. A watermark that is nonintrusive is one which resembles the image it is designed to protect. By virtue of its similarity to the image, any operation that is intentionally performed to damage the watermark will also damage the image.

The factors affecting the transmission of information embedded in images are quite complex. First, there is the need for robustness. The second factor is visibility. Intuitively, one can see that less information can be hidden on flat featureless regions of the image. It should be possible to incorporate more information into those parts of the image that contain more texture or around edges, provided edge integrity is maintained. Psychovisual phenomena are obviously factors in the transmission of hidden information.

There are two main principles involved in designing a watermark. The first principle, mentioned earlier, is

© IEE, 1995

IEE Proceedings online no. 19960711

Paper first received 22nd December 1995 and in revised form 14th June 1996

J.J.K. Ó Ruanaldh was with Trinity College Dublin and is now with the Computer Vision Group, Centre Universitaire d'Informatique, 24 Rue Général Dufour, Université de Genève, CH 1211-Geneve 4, Switzerland

W.J. Dowling and F.M. Boland are with the Department of Electronic and Electrical Engineering, Trinity College Dublin, Dublin 2, Ireland

that a successful watermarking algorithm should explicitly identify and place the mark in the most important features of the image. There are some similarities to the key ideas behind image compression and there will be many ideas and techniques borrowed from this field. The second principle, which we shall outline briefly, is that of *spread spectrum communications* [3].

2. Previous work

Brazil *et al.* [6] have investigated different methods for marking text within documents with a unique binary codeword which serves to identify legitimate users of the document. The codeword is embedded in a document by making subtle modifications to the structure of the document such as modulation of line width and interword spacing as well as modification of character font. The presence of the codeword does not visibly degrade the document but can be readily detected by making a comparison with the original. Standard document handling operations such as photocopying and scanning do not remove the mark. The same idea may be extended to include the protection of images.

Kurak and McHugh [7] have considered the possible application of redundant features in digital images to the transmission of information. Their concern was the transmission of dangerous viruses (or 'Trojan horse programs') in the least significant bits of a data stream. They note that merely viewing an image is not sufficient for detecting the presence of some form of corruption. Depending on the texture of the image and the quality of a computer monitor, it is possible to exploit the limited dynamic range of the human eye to hide low-quality images within other images. Walton [8] has developed a technique for misdirecting viewers to the least significant bits of an image to implement a fragile watermark and thus prevent unauthorised tampering. Daarenberg and Boland [9] examined the use of the least significant bits as a possible scheme for introducing watermarks into images. This approach gave very poor results because standard lossy compression schemes, such as JREG [10], tend to have the effect of randomising the least significant bits during the quantisation stage of image compression.

Zhao and Koch [11] have investigated an approach to watermarking images based on the JPEG [10] image compression algorithm. Their approach is to segment the image into individual 8×8 blocks. Only eight coefficients occupying particular positions in the 8×8 block of DCT coefficients can be marked. These comprise the low frequency components of the image block, but exclude the mean value coefficient in coordinate (0,0), as well as the low frequencies at coordinates (0,4) and (4,0). Three of the remaining DCT coefficients are selected using a pseudorandom number generator to convey information. The resemblance of this technique to frequency hop spread spectrum communications is mentioned by the authors [11]. Zhao and Koch also take the precaution of placing the blocks at random positions in the image in order to make a successful attack by an enemy less likely.

Tricot *et al.* [12, 13] and van Schuydel *et al.* [14, 15] have applied the properties of m-sequences to produce watermarks that are resistant to filtering, image cropping and are reasonably robust to cryptographic attack. The original image is not required to decode the mark. Recent work [15] indicates progress towards producing more robust watermarks.

Majum and Tanaka [16] have applied linear predictive coding for watermarking video facsimile, filtered binary pictures and colour and grey scale images. Their approach to hiding a watermark is to make the watermark resemble quantisation noise. To a certain extent, their approach can be considered to be perceptually adaptive because quantisation noise is concentrated around edges and textured features. Cox *et al.* [4] believe that this method may not be robust to cropping. O'Ruanaidh *et al.* [17] and Cox *et al.* [4] have developed perceptually adaptive transform domain methods for watermarking. In direct contrast to the previous approaches listed above the emphasis was on embedding the watermark in the *most significant* components of an image. The general approach, used in these papers is to divide the image into blocks. Each block is mapped into the transform domain using either the discrete cosine transform [10, 18-20], the Hadamard transform [1, 16] or the Daubechies wavelet transform [19]. Only the components that are most significant to image intelligibility are marked. A transform-based watermarking algorithm is described in more detail in Section 4.

Transform domain modulation schemes possess a number of desirable features. First one can mark according to the perceptual significance of different transform domain components which means that one can adaptively place watermarks where they are least noticeable, such as within the texture of an image. As a result a transform domain watermark tends to resemble the original image. The watermark is also irregularly distributed over the entire image sub-block which makes it more difficult for enemies in possession of independent copies of the image to decode and to read the mark.

The scheme described by Cox *et al.* [4] differs from that used by O'Ruanaidh *et al.* [17] in several ways. The main differences lie in the detection and decoding of the mark. Cox *et al.* embed a unique Gaussian distributed sequence into the coefficients. The Gaussian distribution is chosen to prevent attacks by colluding parties comparing independent copies of the image. O'Ruanaidh *et al.* employ an alternative approach whereby a binary one is directly embedded in the image. One advantage of the latter approach is that it avoids the need to maintain large databases of watermarks. A disadvantage is that the sequences thus produced are discrete valued and therefore the watermark is less resistant to colluding parties. However, there is nothing to prevent one from using continuous watermarks to convey digital information. This would combine the best features of both approaches.

The discrete Fourier transform (DFT) may also be used in watermarking. The discrete Fourier transform of a real image is generally complex valued. This leads to a magnitude and phase representation for the image. Transform domain methods described above mark the components of real valued transforms. O'Ruanaidh *et al.* [21] and O'Ruanaidh *et al.* [17] have also investigated the use of DFT phase for the transmission of information. There are a number of reasons for doing this. First and most importantly, the human visual system is far more sensitive to phase distortions than to magnitude distortions [22]. Oppenheim and Lim [23] investigated the relative importance of the phase and magnitude components of the DFT to the intelligibility of an image and found that phase is more significant.

own
aise

s the
form
and
very
ages,
each
r dec-
rmed
ay be
ed to

ve dis-
n of a
n com-
all, of
tal the
ponen-
nts this
e of the
side the
ethod of
to lossy
scanning

using the
acks, and
e and the
s around
ize 256 *
expect to
ms. This
plication
dundancy
as well as
ill sec. this
marking in

watermark
dulation for
ably, a tech-
to be placed
d. Note that
exclusively
nsforms con-
in the paper
e watermark-

adapted from
n is a hybrid
ency shift key-

each pixel in

block so that

block.

5. Modulate selected coefficients of the transformation (e.g. using bidirectional coding). The coefficients that are selected are those that are most relevant to the intelligibility of the image.

6. Compute the inverse transform, denormalise, add the mean to each pixel in the block and replace the image block in the image.

Steps 2 and 3 above produce a normalised image sub-block with zero mean. Although one of the DCT coefficients computed in Step 4 already contains the mean, Step 2 is not redundant because the normalisation in Step 3 may only be carried out if the mean of the block is zero.

Watermark detection is easily performed by carrying out Steps 1 to 4 above on the original image and the watermarked image in parallel and comparing the values of the coefficients.

4.1 The number of bits

The most important factor in embedding a bit stream in an image is to determine the number of bits that can be placed into a given image block.

In a highly textured image block, energy tends to be more evenly distributed among the different DCT coefficients. In a flat featureless portion of the image the energy is concentrated in the low frequency components of the spectrum.

As stated earlier, the aim is to place more information bits where they are most robust to attack and are least noticeable. This may be accomplished by using a simple thresholding technique. The first stage is to use visual masking and to weight the transform coefficients $F(k_1, k_2)$, $0 \leq k_1 < N_1$ and $0 \leq k_2 < N_2$, according to a subjective measure of their visual perceptibility

$$G(k_1, k_2) = w(k_1, k_2) F(k_1, k_2) \quad (1)$$

The most significant components are then selected by comparing the component magnitude squared to the total energy in the block. The coefficient $F(k_1, k_2)$ is selected if

$$|G(k_1, k_2)|^2 \geq \epsilon \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} |G(k_1, k_2)|^2 \quad (2)$$

The quantisation tables [10] used in JPEG image compression can be exploited to choose the weighting in eqn. 1 for DCT watermarking with 8×8 blocks.

Lossy image compression algorithms are designed to disregard redundant information. Information bits placed within textured areas of the image are therefore more vulnerable to attack. There is a compromise to be reached between hiding a large number of information bits where they can least be seen, but where they can be attacked by image compression algorithms, or placing fewer bits on less textured but safer portions of the image. This may be achieved by opting for a moderately low value of threshold (e.g. $\epsilon = 0.2$).

It is worth noting that the number of bits that can be encoded using image transforms far exceeds that of the block-mean approach. The number of modulated DCT coefficients is generally around 10000 for a typical image. In the case of Zhao and Koch's method, 3 bits of information are encoded into each 8×8 block. If the blocks are tiled over the image then one could obtain a maximum code rate of 3/64 bits/pixel.

It is important to note the differences between the aims in image compression and in watermarking

images. In transform-based image compression, the goal is to obtain a small number of transform coefficients which can be used to obtain a good approximation to the original image. Small changes in the coefficient values should make little difference to the reconstructed image. However, the reverse does not necessarily hold since a small change to the image can result in a large change in the coefficient values (particularly when the basis images also change). This behaviour is obviously extremely undesirable since the embedded information depends on the value of these coefficients. The severity of this effect depends on the image transforms being used. Ill-conditioning tends to be much more severe for image transformations whose basis images are data-dependent (e.g. the singular value decomposition (SVD)). Image transformations with fixed basis functions (e.g. DCT and wavelet transforms) tend to exhibit more stable behaviour.

5. Reliable communications

The material in this paper thus far has described methods for watermarking images. However, we have not yet addressed the other main component in the watermarking problem, namely the reliable transmission of the watermark.

Reliable communication was proven by Shannon [25] to be theoretically possible providing the information rate does not exceed a threshold known as the channel capacity. In this Section we make some rather idealised assumptions regarding the form of the noise n corrupting a watermark and use information theory to derive rules for setting the optimal strength and location of the watermark x .

Let us write

$$x_i + n_i = y_i \quad 1 \leq i \leq N \quad (3)$$

where x_i is one element of a watermark vector of length N , n_i is an element of a noise vector and y_i is a element of a watermark distorted by image processing noise. All forms of image processing including vector quantisation, filtering and scanning introduce noise which degrades the watermark. We assume that the noise is additive, white, stationary and Gaussian:

$$p(y_i | x_i) = p(n_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(y_i - x_i)^2}{2\sigma^2}\right] \quad (4)$$

We also assume that the n_i are uncorrelated and that

$$p(y_1, y_2, \dots, y_N | x_1, x_2, \dots, x_N) = \prod_{i=1}^N p(y_i | x_i) \quad (5)$$

Channel capacity [26] may be defined as

$$C = \max_{p(x)} I(X; Y) \quad (6)$$

where the watermark probability density function $p(x)$ is chosen to maximise the average mutual information $I(X; Y)$.

According to Proakis [27] the capacity is maximised with respect to the distribution $p(x)$ if

$$p(x_i) = \frac{1}{\sqrt{2\pi\gamma^2}} \exp\left[-\frac{x_i^2}{2\gamma^2}\right] \quad (7)$$

which is a zero mean Gaussian density with variance γ^2 . In this case,

$$I_{max} = \frac{1}{2} N \log_2 \left[1 + \frac{\gamma^2}{\sigma^2} \right] \quad (8)$$

Note that eqn. 7 would seem to support the use of a Gaussian distributed watermark such as that used by Cox *et al.* [4].

In image watermarking we might expect that the transmission of information is functioning under quite extreme conditions in which case $\sigma^2 \gg \gamma^2$, which implies

$$\ln \left(1 + \frac{\gamma^2}{\sigma^2} \right) \approx \frac{\gamma^2}{\sigma^2} \quad (9)$$

Substituting the above into eqn. 8 we obtain the following condition for reliable communication:

$$\frac{\gamma^2}{\sigma^2} > (2 \ln 2) \frac{J}{N} \quad (10)$$

where the N is the number of sites used to hide watermark information bits and J is the information rate. Eqns. 8 and 10 reduce to the more familiar form [1] if the 'bandwidth' B of the channel is set to half the number of sites, $N/2$. Note that the noise power can be considerably greater than the signal power and, in theory at least, the message may still be transmitted reliably!

The strategy for communicating the watermark is now clear. Because a watermark should be imperceptible the signal to noise ratio (SNR) is severely limited. Reliable communication can only be assured by increasing bandwidth B to compensate for poor SNR. Hence, in the case of watermarking the maximum number N of suitable transform domain coefficients should be exploited for hiding information in the image. An analogous situation occurs in satellite and mobile communications where SNR is limited by power restrictions at the transmitter. There are also many similarities to secret military communications where an opponent may also attempt to detect, intercept or block a transmission. Watermarking may be considered as being an application of *spread spectrum communications* [5].

The Shannon limit may be approached by applying error control codes. Robust error correction techniques can be employed if necessary. Methods for error control coding are described by Sweeney [28], Chambers [1] and Blahut [29].

Information theory also gives some insights into where the watermark should be placed. Let us assume that the image may be considered as a collection of parallel uncorrelated Gaussian channels which satisfy eqn. 3 above with the constraint that the total watermark energy is limited:

$$\sum_{i=1}^N \gamma_i^2 \leq E \quad (11)$$

Using eqn. 4 and assuming that the noise variances are not necessarily the same in each channel, Gallager [26] shows that the capacity is

$$C = \frac{1}{2} \sum_{i=1}^N \log_2 \left(1 + \frac{\gamma_i^2}{\sigma_i^2} \right) \quad (12)$$

where σ_i^2 is the variance of the noise corrupting the watermark and γ_i^2 is the average power of the watermark signal in the i th channel. This is a more general form of eqn. 8. Capacity is achieved when

$$\gamma_i^2 + \sigma_i^2 = T_h \quad \text{if } \sigma_i^2 < T_h \quad (13)$$

$$\gamma_i^2 = 0 \quad \text{if } \sigma_i^2 \geq T_h \quad (14)$$

where the threshold T_h is chosen to maximise the sum on the left-hand side of eqn. 11 and thus maximise the

energy of the watermark. This result shows clearly that the watermark should be placed in those areas where the local noise variance σ_n^2 is smaller than threshold T_A and not at all in those areas where the local noise variance exceeds the threshold. Note that the simple analysis presented here assumes that the noise corruption suffered by the watermark, as a result of common forms of image processing, is Gaussian. This is not an accurate assumption to make in many cases. However, the Gaussian assumption is not a bad choice given that the aim is to derive rules and heuristics that apply in general to a number of fundamentally different (image processing scenarios). The Gaussian noise model leads to a tractable analysis in many cases. Theoretically, it can also be considered to be a general noise model because of its conservative nature. Three justifications for its adoption in the absence of any information regarding the noise statistics include the central limit theorem [50], Herschel's theorem [31] as well as the principle of maximum entropy [32, 33]. In

addition, additive white Gaussian noise (AWGN), gives the most difficult conditions in which to attempt communication [36]. Hence, the Gaussian noise assumption is actually quite conservative. A full analysis of the channel based on accurate knowledge of the noise statistics would lead to more accurate values for the channel capacity but would also be complicated by the need to evaluate difficult multidimensional integrals.

6 Examples

Fig. 1 shows 'Lena' watermarked using bidirectional coding and blocks with borders [9]. The image is of size 512×512 pixels, the inner block size is 12×12 pixels and the pixels are incremented by 3 to transmit a binary '1' and decremented by 3 to convey a binary '0'. The mark is for all intents and purposes invisible in Fig. 1 but may be detected quite readily [24, 9] even after lossy compression and scanning have been carried



Fig. 1 Lena image watermarked using bidirectional coding



Fig. 3 Lena watermarked using four-level Daubechies wavelets



Fig. 2 Lena image watermarked using bidirectional coding

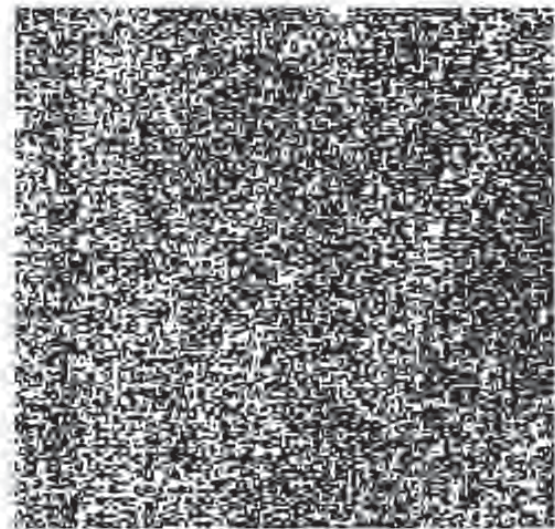


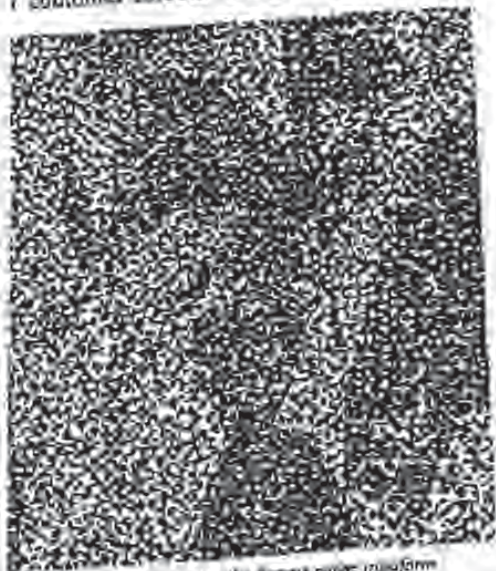
Fig. 4 Watermark produced using Daubechies wavelets

image convey the bits of information of and the standard message reads '0123456789'. Fig. 2 shows the same image out with a perturbation of ± 12 to make it visible.

The 'Lena' watermark using the Daubechies transform. The block size is 8×8 and a transform coefficient perturbation is ± 5 . The watermark is conveyed by modulating 1551 coefficients. The standard message is large number of times to occupy all of the capacity. Note that the presence of the mark is visible degradation.

shows the difference between the wavelet size of the standard image and the original. A factor of 30 and offset by 127 grey scale. 5 shows a similar difference image for a watermark produced using the DCT. As in the case of watermark, the DCT block size is 8×8 and a transform coefficient perturbation is ± 5 . The watermark is conveyed by modulating 11933 coefficients and the standard test message is encoded as before.

shows a watermarked image of a wolf on a black background. The image is of size 768×512 . It is very interesting from our point of view as it combines smooth background regions (the



Watermark produced using the discrete wavelet transform



6 Watermarked image of a wolf on a noisy background

watermark was produced using the redundant wavelet transform with an energy threshold $\alpha = 0.2$. The block size is 8×8 and the transform coefficient perturbation is ± 10 . The watermark is conveyed by modulating 3840 transform coefficients. The absolute difference between the original image and the marked image, contrast enhanced using histogram equalisation, is shown in Fig. 7. In this case, areas with high information density (expressed in terms of the number of embedded watermark bits per block) are white, while areas which attract fewer watermark bits are darker. The outline of the wolf's head is quite clear. Note that, as before, information density is higher in secured regions.

Fig. 8 shows a segment of a watermarked image of Lena after JPEG [10] image compression followed by cropping. The size of the segment is 512×200 pixels. The watermark embedded in the uncropped image is 4096 bits long and the block size is 8×8 (i.e. just one bit per block). The encoded message consists of 32 bits ('0123' in ASCII). The watermark was placed using a DCT and the perturbation in the coefficient values was ± 10 . JPEG was applied with a standard setting of 50 and no smoothing was used. By judicious use of concatenated error control codes [29, 1, 28] the watermark was recovered with ease from this cropped section.

It is apparent upon examining the watermarks in Figs. 4, 5 and 7 that the transform-based marking schemes possess a number of desirable features. One can mark according to the distribution of energy within the coefficients. In this way, one can place watermarks where they are least noticeable, such as within image texture and around edges. As a result, the watermark exhibits a ghost-like resemblance to the original image.

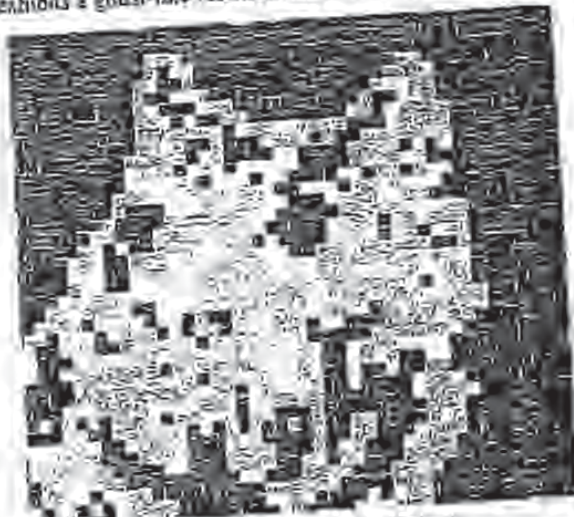


Fig. 7 Watermark overlaid the region of the wolf's head. The watermark was generated using the Redundant Wavelet Transform. Areas with a high density of information are indicated by the brighter blocks.



Fig. 8 Cropped grey scale image of Lena. The size of image is 512×200 pixels.

paper has outlined a scheme for embedding robust marks in digital images. The watermarks are not to be invisible, even to a careful observer, but in sufficient information to identify both the original intended recipient of an image with a very low ability of error.

The key feature of the transform-based methods is information bits can be placed adaptively, thereby making the watermark more robust to attack. A watermark is made imperceptible because it is designed to match the characteristics of the image to be protected. Transform-based methods have proven to be reasonably robust to image compression and standard image processing operations. In addition, transform-based methods yield a relatively large number of transform coefficients in which to embed the watermark. Future work will include the use of human visual models in ongoing watermarking schemes. The application of variable error correction codes and digital signature techniques will also be investigated. In particular, the statistical characteristics of the watermarking channel need careful study. It is known that the distribution of DCT coefficients of a typical image is well approximated by a Laplacian distribution [18]. It has been observed that the noise distortion imposed on the watermark by common image processing operations is non-Gaussian and impulsive in nature. Soft error correction codes designed for additive wideband Gaussian noise (AWGN) channels (e.g. Reed-Muller codes) are particularly effective in this application. The design of an optimal detector for the watermark depends on our knowledge of the noise statistics because such a detector can only be as good as the model assumptions on which it is based. Finally, work will continue on devising watermarking schemes that do not require the original image to decode the watermark [21].

Acknowledgment

This work was supported by a Forbairt strategic research grant. The authors would like to thank Dr Peter J. Cullen for helpful advice and stimulating discussions.

References

CHAMBERS, W.G.: 'Basics of communications and coding' (Oxford Science Publications, Clarendon Press, Oxford, 1985)
 HAYKIN, S.: 'Communications systems' (Wiley, 1994, 2nd edn.)
 SCHNEIER, B.: 'Applied cryptography' (Wiley, 1995, 2nd edn.)
 COX, I., KILLIAN, J., LEIGHTON, T., and SHAMMOON, T.: 'Secure spread spectrum communication for multimedia', Technical report, NEC Research Institute, 1995 (<http://ftp.nj.nec.com/pub/ingemar/papers/watermark.ps.Z>)
 PICKHOLTZ, R.L., SCHILLING, D.L., and MILSTEIN, L.B.: 'Theory of spread spectrum communications-a tutorial', *IEEE Trans.*, 1982, COM-30, (5), pp. 855-884

age document copying', *Proceedings of INFOCOM 94*, 1994
 7 KUBAK, C., and MCHUGH, J.: 'A cautionary note on image downgrading', *Proceedings 8th Annual Computer Security Applications Conference*, San Antonio, 1992
 8 WALTON, S.: 'Image authentication for a slippery new age', *Dr Dobbs J.*, 1995, 20, (4), pp. 18-36, 82-87
 9 DAUTZENBERG, C.: 'Embedding Robust F.M.: 'Watermarking images', Technical report, Department of Electronic and Electrical Engineering, Trinity College Dublin, 1994
 10 PENNEBAKER, W.B., and MITCHELL, J.L.: 'JPEG still image compression standard' (Van Nostrand Reinhold, New York, 1993)
 11 ZHAO, J., and KOCH, E.: 'Embedding robust labels into images for copyright protection', Technical report, Fraunhofer Institute for Computer Graphics, Darmstadt, Germany, 1994
 12 TIRKEL, A.Z., RANKIN, G.A., VAN SCHYNDEL R.G., HO, W.J., MEE, N.R.A., and OSBORNE, C.F.: 'Electronic watermark', *Proceedings of Dista-93*, 1993, pp. 666-672
 13 TIRKEL, A.Z., VAN SCHYNDEL R.G., and OSBORNE, C.F.: 'A two-dimensional digital watermark', *Proceedings of ACCV*, Singapore, 1995
 14 VAN SCHYNDEL R.G., TIRKEL, A.Z., and OSBORNE, C.F.: 'A digital watermark', *Proceedings of IEEE International Conference on Image Processing*, Austin, Texas, 1994, pp. 86-90
 15 VAN SCHYNDEL, R.G., TIRKEL, A.Z., and OSBORNE, C.F.: 'Towards a robust digital watermark', *Proceedings of Dista-95*, 1995
 16 MATSUI, K., and TANAKA, K.: 'Video-steganography: how to secretly embed a signature in a picture', *IMA Intellectual Property Project Proceedings*, January 1994, pp. 187-206
 17 O RUANAIDH, J.J.K., DOWLING, W.J., and BOLAND, F.M.: 'Phase watermarking of images', *IEEE International Conference on Image Processing*, Lausanne, Switzerland, September 1996
 18 CLARKE, R.J.: 'Transform coding of images' (Academic Press, London, 1985)
 19 PRESS, W.H., TEUKOLSKY, S.A., VETTERLING, W.T., and FLANNERY, B.P.: 'Numerical recipes in C' (Cambridge University Press, 1992, 2nd edn.)
 20 RAO, K.R., and YIP, P.: 'The discrete cosine transform: algorithms, advantages, applications' (Academic Press, 1990)
 21 O RUANAIDH, J.J.K., BOLAND, F.M., and SINNEN, O.: 'Watermarking digital images for copyright protection', *Proceedings of the Electronic Imaging and Visual Arts Conference*, Florence, February 1996. <http://kaimao.isee.tcd.ie/people/jjr/eva-pp.html>
 22 LIM, J.S.: 'Two-dimensional signal and image processing' (Prentice-Hall International, 1990)
 23 OPPENHEIM, A.V., and LIM J.S.: 'The importance of phase in signals', *Proc. IEEE*, 1981, 69, (5), pp. 529-541
 24 CAEONNI, G.: 'Assuring ownership rights for digital images', in BRUEGGEMANN, H.H., and GERHARDT-HAECKL, W. (Eds): 'Reliable IT systems VIS 95' (Vieweg Publishing Company, Germany, 1995)
 25 SHANNON, C.E.: 'A mathematical theory of communication', *Bell Syst. Tech. J.*, 1948, 27, pp. 379-423, 623-656
 26 GALLAGER, R.G.: 'Information theory and reliable communication' (Wiley, 1968)
 27 PROAKIS, J.G.: 'Digital communication' Series in electrical and computer engineering communications and signal processing (McGraw-Hill, 1995, 3rd edn.)
 28 SWEENEY, P.: 'Error control coding: an introduction' (Prentice-Hall, 1991)
 29 BLAHUT, R.E.: 'The theory and practice of error control codes' (Addison-Wesley, 1983)
 30 FAPOULIS, A.: 'Probability, random variables and stochastic processes' (McGraw-Hill, 1984, 2nd edn.)
 31 BRETTHORST, G.L.: 'Bayesian spectrum analysis and parameter estimation' (Springer-Verlag, 1989)
 32 JAYNES, E.T.: 'in ROSENKRANTZ, R.D. (Ed.): 'Papers on probability, statistics and statistical physics, a reprint collection' (Kluwer, 1989)
 33 BURTON, D., and FITZGERALD, W.J.: 'Bayesian parameter estimation: further results' Technical report, Marconi Maritime Research Laboratory, Cambridge, England, 1989

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

BLACK COLORED DEFECT AT TOP, BOTTOM OR SIDES

BLACK COLORED DRAWING

BLACK COLORED LABEL TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

29

Secure Spread Spectrum Watermarking for Multimedia

Ingemar J. Cox†, Joe Kilian†, Tom Leighton† and Talal Shamoont*[‡]

Abstract

We describe a digital watermarking method for use in audio, image, video and multimedia data. We argue that a watermark must be placed in perceptually significant components of a signal if it is to be robust to common signal distortions and malicious attack. However, it is well known that modification of these components can lead to perceptual degradation of the signal. To avoid this, we propose to insert a watermark into the spectral components of the data using techniques analogous to spread spectrum communications, hiding a narrow band signal in a wideband channel that is the data. The watermark is difficult for an attacker to remove, even when several individuals conspire together with independently watermarked copies of the data. It is also robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, resampling, and requantization, including dithering and recompression and rotation, translation, cropping and scaling. The same digital watermarking algorithm can be applied to all three media under consideration with only minor modifications, making it especially appropriate for multimedia products. Retrieval of the watermark unambiguously identifies the owner, and the watermark can be constructed to make counterfeiting almost impossible. Experimental results are presented to support these claims.

1 Introduction

The proliferation of digitized media (audio, image and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Conventional cryptography therefore provides little protection against data piracy, in which a publisher is confronted with unauthorized reproduction of information. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data, that is, it remains present within the data after any decryption process. In the context of this work, data refers to audio (speech and music), images (photographs and graphics), and video (movies). It does not include ASCII representations of text, but does include text

[†]Post: NEC Research Institute, 4 Independence Way, Princeton, NJ 08540.
Email: ingemar|joe|talal@research.nj.nec.com
[‡]Post: Mathematics Department and Laboratory for Computer Science, MIT, Cambridge, MA 02139.
Email: tl@math.mit.edu
* Authors appear in alphabetical order.

BEST AVAILABLE COPY

represented as an image. A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright owner. However, the watermark might contain additional information, including the identity of the purchaser of a particular copy of the material.

In order to be effective, a watermark should be:

Unobtrusive The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Robust The watermark must be difficult (hopefully impossible) to remove. Of course, in theory, any watermark may be removed with sufficient knowledge of the process of insertion. However, if only partial knowledge is available, for example, the exact location of the watermark within an image is unknown, then attempts to remove or destroy a watermark by say, adding noise, should result in severe degradation in data fidelity before the watermark is lost. In particular, the watermark should be robust to

Common signal processing The watermark should still be retrievable even if common signal processing operations are applied to the data. These include, digital-to-analog and analog-to-digital conversion, resampling, requantization (including dithering and recompression), and common signal enhancements to image contrast and color, or audio bass and treble, for example.

Common geometric distortions (image and video data) Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling.

Subterfuge Attacks: Collusion and Forgery In addition, the watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data. That is, the watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used as evidence in a court of law, it must not be possible for colluders to combine their images to generate a different valid watermark with the intention of framing a third-party.

Universal The same digital watermark algorithm should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conducive to implementation of audio and image/video watermarking algorithms on common hardware.

Unambiguous Retrieval of the watermark should unambiguously identify the owner. Further, the accuracy of owner identification should degrade gracefully in the face of attack.

Previous digital watermarking techniques, described in Section 2, are not robust, and the watermark is easy to remove. In addition, it is unlikely that any of the earlier watermarking methods would survive common signal and geometric distortions. The principal reason for these weaknesses is that previous methods have not explicitly identified the perceptually most significant components of a signal as the destination for the watermark. In fact, it is often the case that the perceptually significant regions are explicitly avoided. The reason for this is obvious - modification of perceptually significant components of a signal results in perceptual distortions much earlier than if the modifications are applied to perceptually insignificant regions. Hence, for example, the common strategy of placing a watermark in the high frequency components of a signal's spectrum.

The key insight of this paper is that in order for it to be robust, the watermark must be placed in perceptually significant regions of the data despite the risk of potential fidelity distortions. Conversely, if the watermark is placed in perceptually insignificant regions, it is easily removed, either intentionally or unintentionally by, for example, signal compression techniques that implicitly recognize that perceptually weak components of a signal need not be represented.

The perceptually significant regions of a signal may vary depending on the particular media (audio, image or video) at hand, and even within a given media. For example, it is well known that the human visual system is tuned to certain spatial frequencies and to particular spatial characteristics such as line and corner features. Consequently, many watermarking schemes that focus on different phenomena that are perceptually significant are potentially possible. In this paper, we focus on perceptually significant spectral components of a signal.

Section 3 begins with a discussion of how common signal transformations, such as compression, quantization and manipulation, affect the frequency spectrum of a signal. This motivates why we believe that a watermark should be embedded in the data's perceptually significant frequency components. Of course, the major problem then becomes how to insert a watermark into perceptually significant components of the frequency spectrum without introducing visible or audible distortions. Section 3.2 proposes a solution based on ideas from spread spectrum communications.

The structure of a watermark may be arbitrary. However, Section 4 provides an analysis based on possible collusion attacks that indicates that a binary watermark is not as robust as a continuous one. Furthermore,

we show that a watermark structure based on sampling drawn from multiple i.i.d Gaussian random variables offers good protection against collusion.

Of course, no watermarking system can be made perfect. For example, a watermark placed in a textual image may be eliminated by using optical character recognition technology. However, for common signal and geometric distortions, the experimental results of Section 5 strongly suggest that our system satisfies *all* of the properties discussed in the introduction, and displays strong immunity to a wide variety of attacks, though more extensive experiments are needed to confirm this. Finally, Section 6 discusses possible weaknesses and enhancements to the system.

2 Previous Work

Several previous digital watermarking methods have been proposed. L. F. Turner [Tur89] proposed a method for inserting an identification string into a digital audio signal by substituting the "insignificant" bits of randomly selected audio samples with the bits of an identification code. Bits are deemed "insignificant" if their alteration is inaudible. Such a system is also appropriate for two dimensional data such as images, as discussed in [vSTO94]. Unfortunately, Turner's method may easily be circumvented. For example, if it is known that the algorithm only affects the least significant two bits of a word, then it is possible to randomly flip *all* such bits, thereby destroying any existing identification code.

Caronni [Car95] suggests adding *tags* — small geometric patterns — to digitized images at brightness levels that are imperceptible. While the idea of hiding a spatial watermark in an image is fundamentally sound, this scheme is susceptible to attack by filtering and redigitization. The fainter such watermarks are the more susceptible they are such attacks and geometric shapes provide only a limited alphabet with which to encode information. Moreover, the scheme is not applicable to audio data and may not be robust to common geometric distortions, especially cropping.

Brassil *et al* [BLMO94] propose three methods appropriate for document images in which text is common. Digital watermarks are coded by: (1) vertically shifting text lines, (2) horizontally shifting words, or (3) altering text features such as the vertical endlines of individual characters. Unfortunately, all three proposals are easily defeated, as discussed by the authors. Moreover, these techniques are restricted exclusively to images containing text.

Tanaka *et al* [TNM90, MT94] describe several watermarking schemes that rely on embedding watermarks that resemble quantization noise. Their ideas hinge on the notion that quantization noise is typically im-