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***

UNITED STATES PATENT AND TRADEMARK OFFICE
DEPARTMENT OF COMMERCE

Certified by

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

10/049101

JC13 Rec'd PCT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
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.

TOTAL AMOUNT OF PAYMENT ($)

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

METHOD OF PAYMENT

1. [x] 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 Floyd Chapman

[x] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

[ ] Applicant claims small entity status. See 37 CFR 1.27

2. [ ] Payment Enclosed:

[ ] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	370.00
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($) 370.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below	Fee Paid
Total Claims	31	-20** =	11	X		= 99.00
Independent Claims	7	- 3** =	4	X		= 168.00
Multiple Dependent						= 0.00

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
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 claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 637.00

**or number previously paid, if greater. For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	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 *ex parte* reexamination	
112	920*	112	920*	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	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	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 - unavoidable	
141	1,280	241	640	Petition to revive - unintentional	
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 637.00

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Floyd B. Chapman	Registration No. (Attorney/Agent)	40,555	Telephone	202/719-7000
Signature	Floyd B Chapman			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.

Burden 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.

10/049101
JC13 Rec'd PCT/PTO 08 FEB 2002

PTO/SB/17 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
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.

TOTAL AMOUNT OF PAYMENT ($)

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

METHOD OF PAYMENT

1. ☐ 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 / Floyd Chapman

☑ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR 1.27

2. ☑ Payment Enclosed:

☐ Check ☑ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

		Extra Claims	Fee from below	Fee Paid
Total Claims	-20** =		X	=
Independent Claims	- 3** =		X	=
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
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 claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater. For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	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 *ex parte* reexamination	
112	920*	112	920*	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	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	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 - unavoidable	
141	1,280	241	640	Petition to revive - unintentional	640.00
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ____________

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 640.00

SUBMITTED BY				Complete *(if applicable)*	
Name (Print/Type)	Floyd B. Chapman	*Registration No. (Attorney/Agent)*	40,555	*Telephone*	202/719-7000
Signature	Floyd B Chapman			*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.

Burden 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.

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;

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 th3e 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:___

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;

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 th3e 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) EVA VON STREHLE Notary Public - State of Florida My Commission Expires Mar 8, 2005 Commission # DD007707

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 MNGUYEN 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

Application or Docket Number

10/049101

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

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		☐

* 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		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

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY OR OTHER THAN SMALL ENTITY

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

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

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

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		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

FORM PTO-875 (Rev. 8/01) ☆U.S.GPO:2001 482-124 / 59197 Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Charles A. Bell
Paralegal Specialist

MULTIPLE DEPEN[redacted]NT CLAIM FEE CALCULAT[redacted]SHEET
(FOR USE WITH FO[redacted]TO-875)

SERIAL NO. 10/04[redacted]101 | FILING DATE
APPLICANT(S) [redacted]

CLAIMS

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

PTO-1360 (3-78)

*MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

U.S. DEPARTMENT of COMMERCE

Best Available Copy

#2

PTO/SB/64/PCT (10-00)
Approved for use through 10/31/2002. OMB 0651-0031
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.

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

First named inventor: Scott A. MOSKOWITZ et al.

International (PCT) Application No.: PCT/US00/21189

U.S. Application No.: (if known)

Filed: August 4, 2000

Title: A SECURE PERSONAL CONTENT SERVER

RECEIVED
15 APR 2002
Legal Staff
International Division

Attention: PCT Legal Staff Attn: Boris Milef
Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

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).

APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION

NOTE: A grantable petition requires the following items:
(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.

1. Petition fee

☑ Small entity - fee $640.00 (37 CFR 1.17(m)). Applicant claims small entity status. See 37 CFR 1.27.

☐ Other that small entity - fee $_______(37 CFR 1.17(m))

2. Proper reply

A. The proper reply (the missing 35 U.S.C. 371(c) requirement(s) in the form of Request to enter National Stage under 371; filing fee and copy of appln. (identify type of reply):

☐ has been filed previously on ______________________.
☑ is enclosed herewith.

02/15/2002 MNGUYEN [illegible] 10049101
[illegible] 227.00 CH [illegible] OP

02/12/2002 MNGUYEN 00000131 501129 10049101

01 FC:241 640.00 OP

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

PATENT COOPERATION TREATY 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)

Applicant's or agent's file reference
066112.0139 031838.0013

IMPORTANT NOTICE

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/US00/21189	04 August 2000 (04.08.00)	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.

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

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

OIPE JC109 MAR 0 2 2001 PATENT & TRADEMARK OFFICE

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

CHAPTER II

DEMAND

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. PCT/US00/21189	International filing date *(day/month/year)* 4 August 2000	(Earliest) Priority date *(day/month/year)* 4 August 1999

Title of invention

A SECURE PERSONAL CONTENT SERVER

Box No. II APPLICANT(S)

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.)*	
Blue Spike, Inc. 16711 Collins Avenue, #2505 Miami, Florida 33160 USA	Telephone No.: Facsimile No.: Teleprinter No.:
State *(that is, country)* of nationality: US	State *(that is, country)* of residence: US

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.)*	
Scott A. Moskowitz 16711 Collins Avenue, #2505 Miami, Florida 33160 USA	
State *(that is, country)* of nationality: US	State *(that is, country)* of residence: US

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.)*	
Michael Berry 12401 Princess Jeanne Albuquerque, New Mexico 87112 USA	
State *(that is, country)* of nationality: US	State *(that is, country)* of residence: US

☐ Further applicants are indicated on a continuation sheet.

Sheet No. ...2

International application No. PCT/US00/21189

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:**

Sheet No. ...3

International application No.
PCT/US00/21189

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:

			For International Preliminary Examining Authority use only: received	not received
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	☐	☐

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

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ nucleotide and or amino acid sequence listing in computer readable form
6. ☐ 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

1. Date of actual receipt of DEMAND:
2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
3. ☐ 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.
4. ☐ 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.
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:

CHAPTER II

PCT

FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

International application No.	**PCT/US00/21189**
Applicant's or agent's file reference	**031838.0013**

For International Preliminary Examining Authority use only

Date Stamp of the IPEA

Applicant

BLUE SPIKE, INC.

Calculation of prescribed fees

1. Preliminary examination fee	490.00	P
2. Handling fee *(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.)*	137.00	H
3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box	627.00 TOTAL	

Mode of Payment

- ☒ authorization to charge deposit account with the IPEA (see below)
- ☐ cash
- ☐ cheque
- ☐ revenue stamps
- ☐ postal money order
- ☐ coupons
- ☐ bank draft
- ☐ other *(specify)*:

Deposit Account Authorization *(this mode of payment may not be available at all IPEAs)*

The IPEA/ US ☒ is hereby authorized to charge the total fees indicated above to my deposit account.

☒ *(this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit)* is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.

50-1640	2 March 2001	Floyd B Chapman
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

(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[7]: G06F

(21) International Application Number: PCT/US00/21189

(22) International Filing Date: 4 August 2000 (04.08.2000)

(25) Filing Language: English

(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).

(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, Alburquerque, NM 87112 (US).

(74) Agents: **CHAPMAN, Floyd, B.** et al.; Baker Botts, LLP, The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).

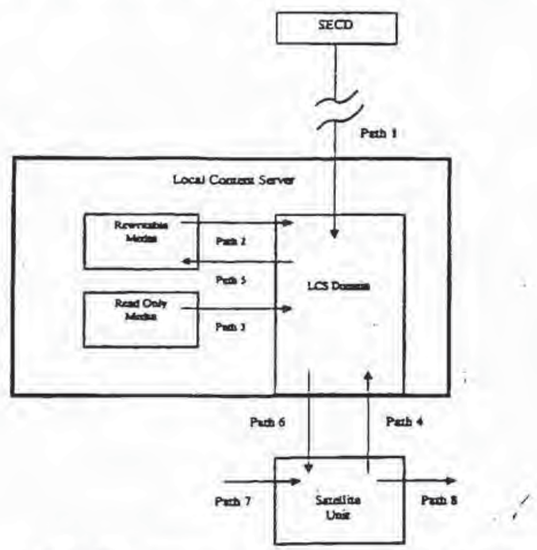
(81) Designated States (*national*): JP, US.

(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:
— *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.

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 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 06/23/2000, entitled "A Secure Personal Content Server."

This application also incorporates by reference the following applications: 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 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 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. 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 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.

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 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.

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".

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 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 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 or goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

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 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 are 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.

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). 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 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 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 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. 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-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. 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.

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.

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

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 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 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

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:

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.

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.

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.

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 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. 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

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 an 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.

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).

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.

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.

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;

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.

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

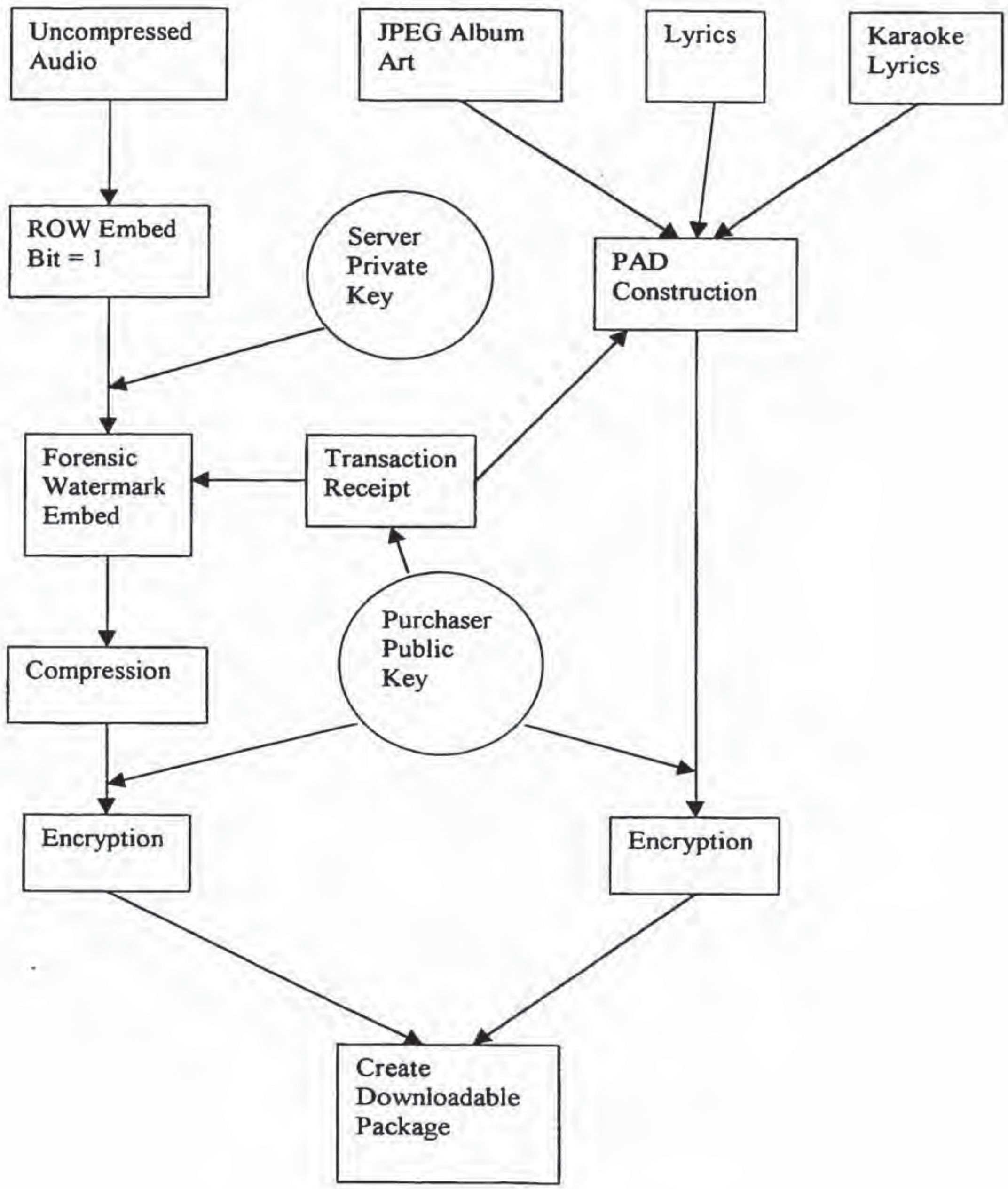


Table 2

SPCS Audio Player Input Stage

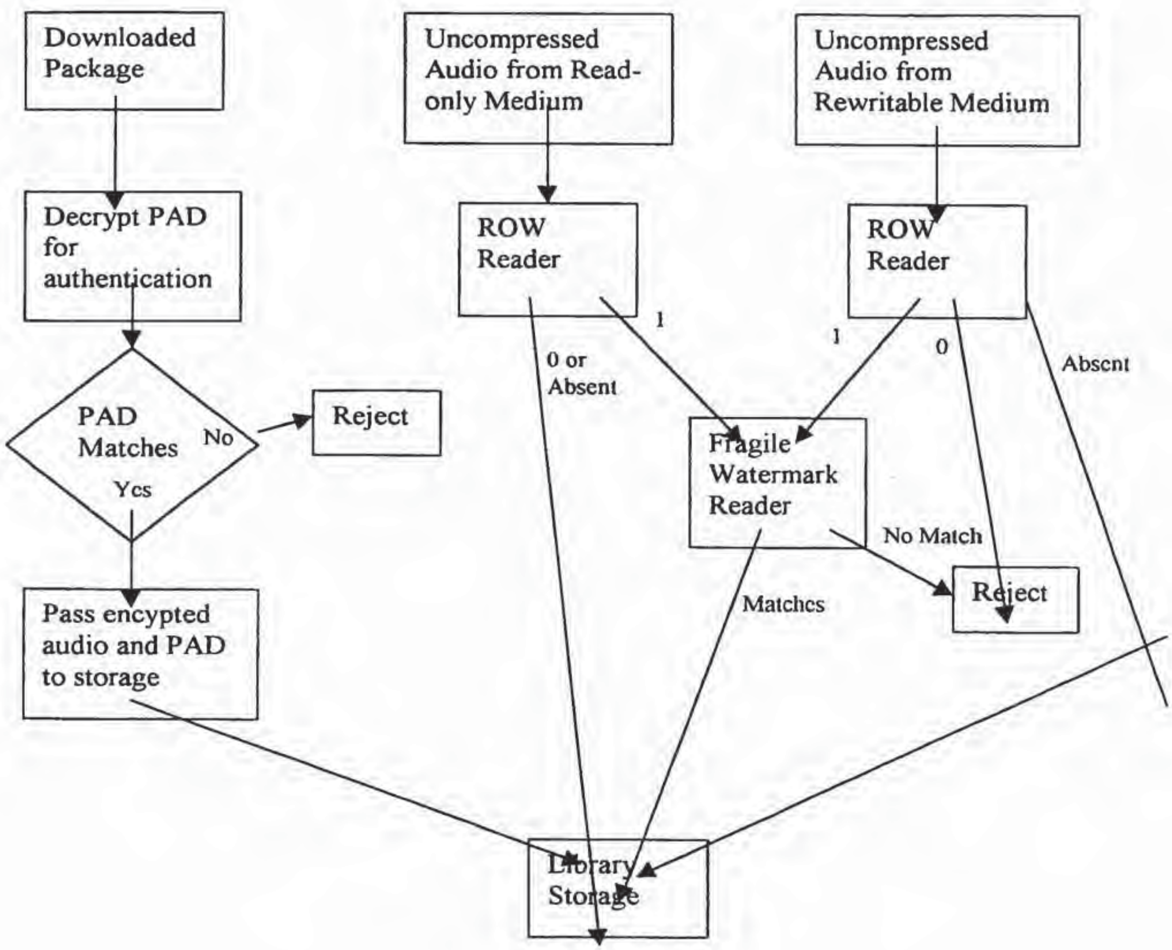
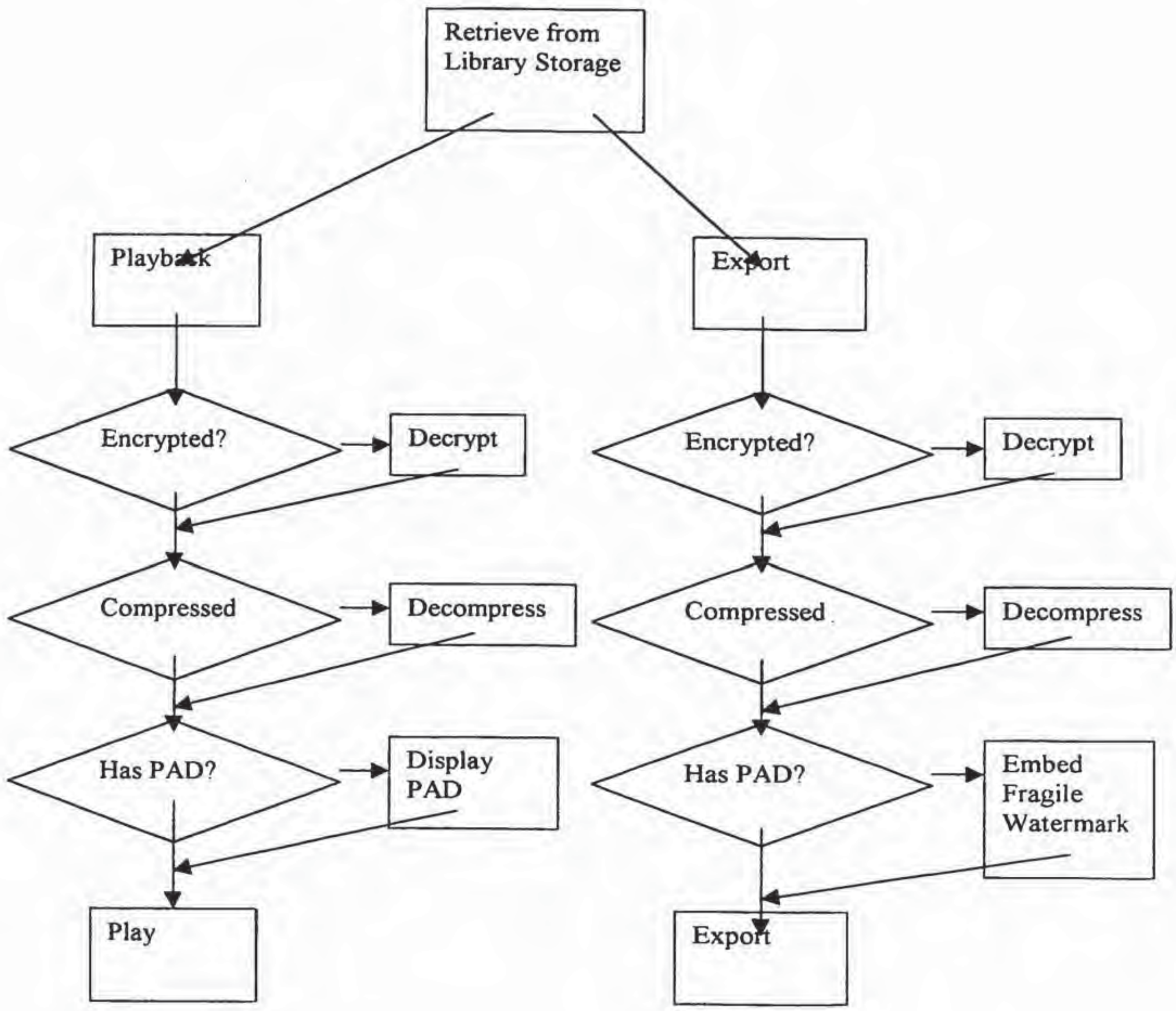


Table 3

SPCS Audio Player Output Stage



Claims:

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

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.

2. 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. 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;

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. 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;

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. 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,

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. 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. 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;

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:

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);

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;

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; 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:

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;

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.

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.

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 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:

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

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

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.

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.

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:

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:

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),

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.

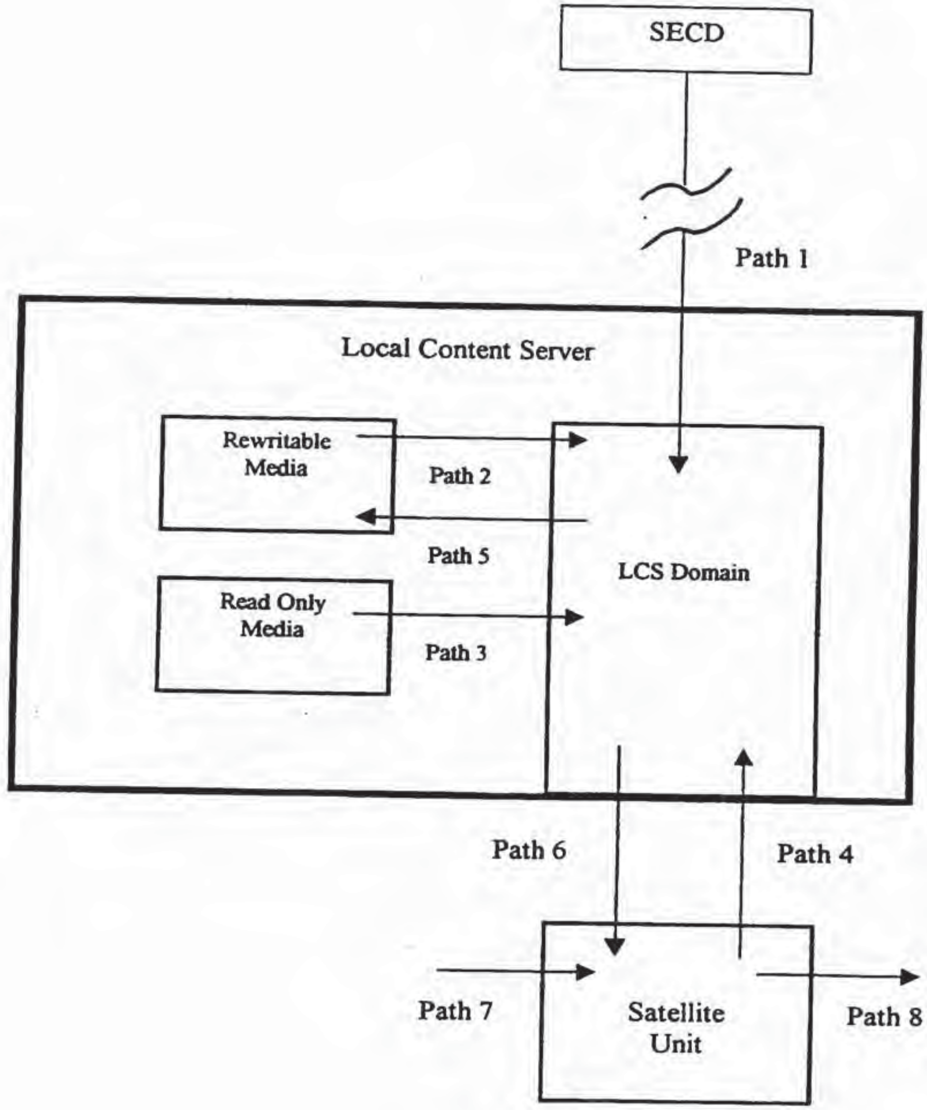

SECD
Path 1
Local Content Server
Rewritable Media
Path 2
Path 5
LCS Domain
Read Only Media
Path 3
Path 6
Path 4
Path 7
Satellite Unit
Path 8

FIG. 1

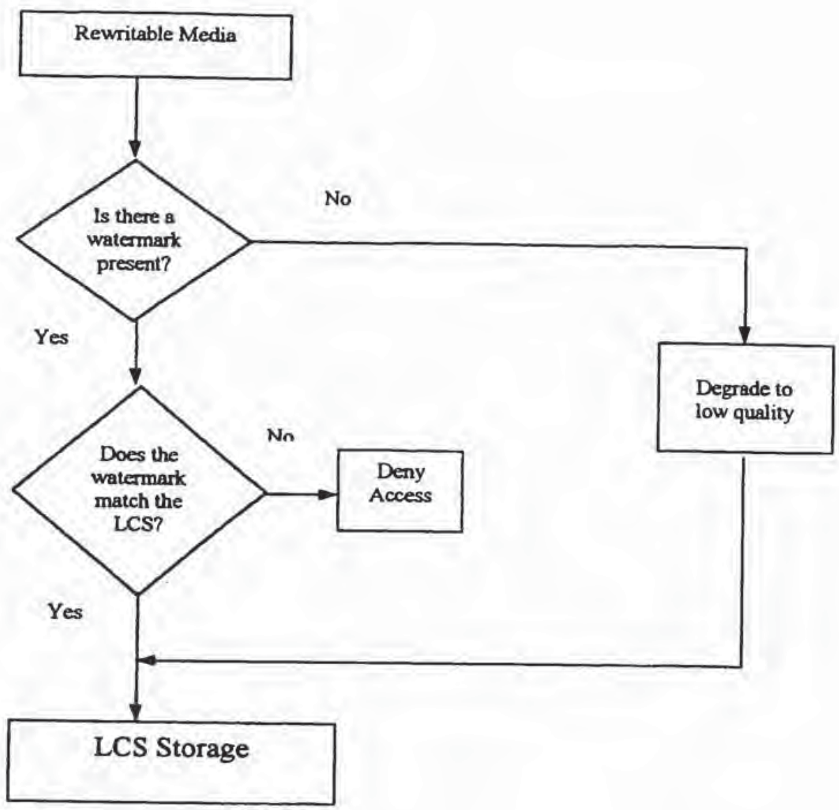

Rewritable Media
Is there a watermark present?
No
Yes
Degrade to low quality
Does the watermark match the LCS?
No
Deny Access
Yes
LCS Storage

FIG. 2

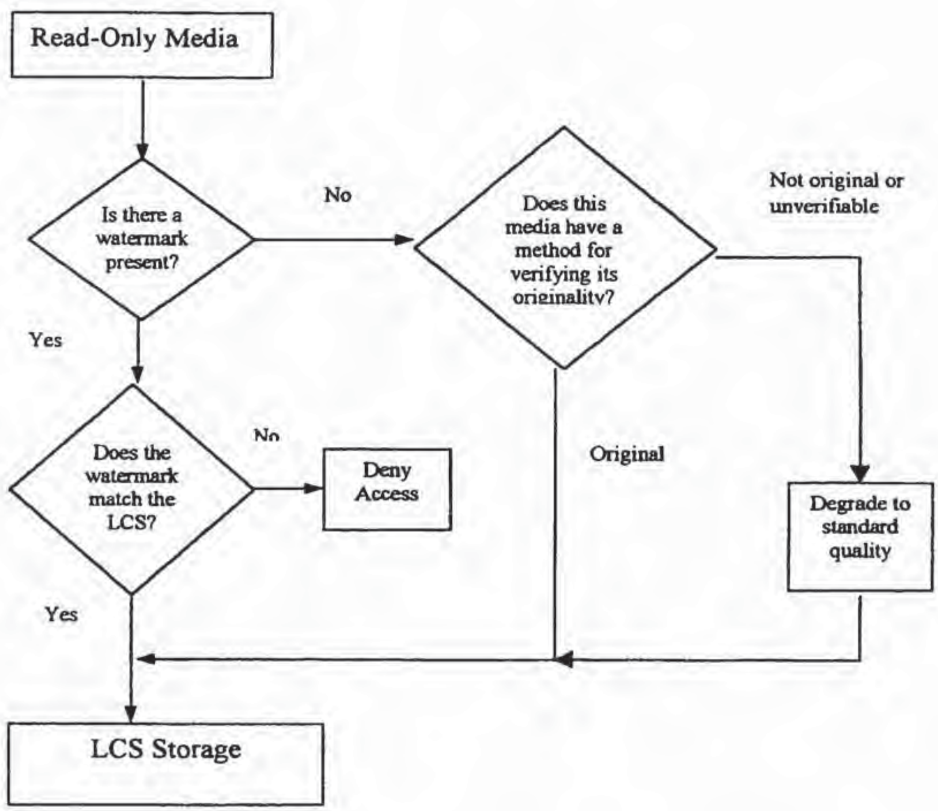

Read-Only Media
Is there a watermark present?
No
Does this media have a method for verifying its originality?
Not original or unverifiable
Yes
No
Does the watermark match the LCS?
Deny Access
Original
Degrade to standard quality
Yes
LCS Storage

FIG. 3

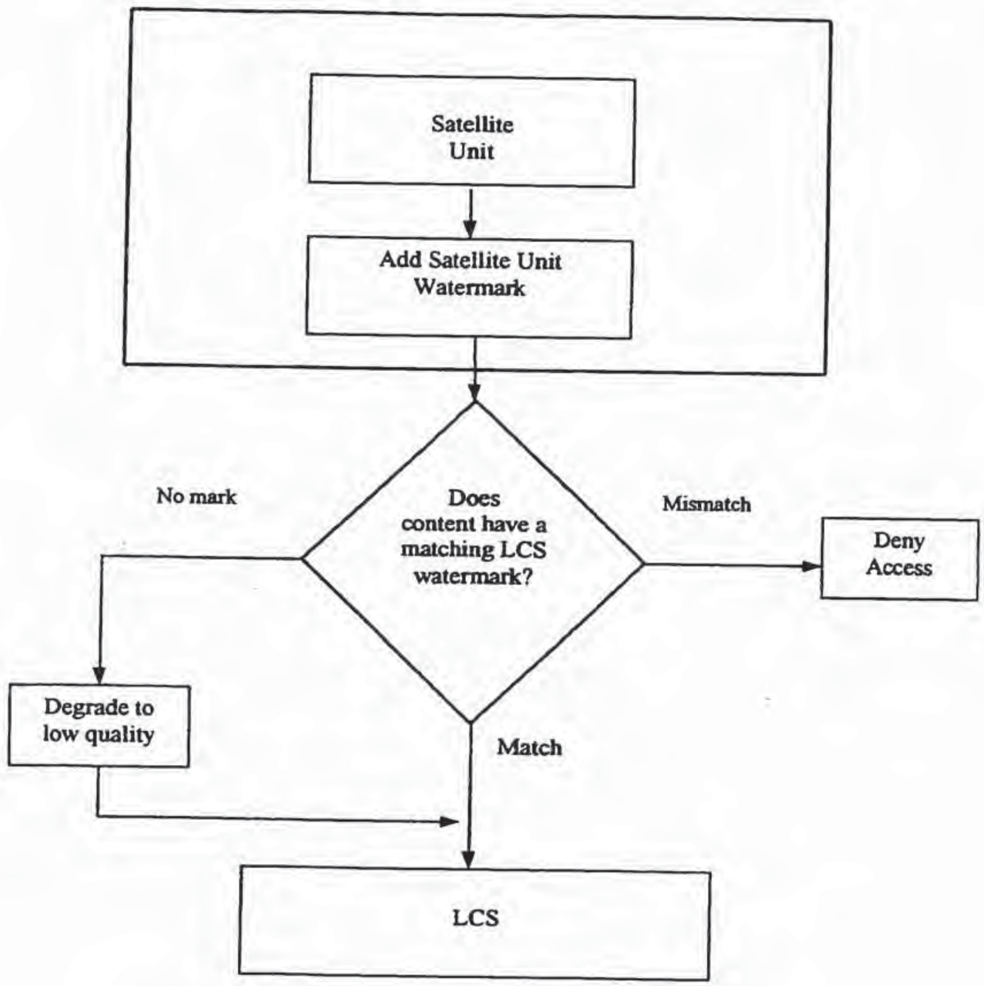

Satellite Unit
Add Satellite Unit Watermark
No mark
Does content have a matching LCS watermark?
Mismatch
Deny Access
Degrade to low quality
Match
LCS

FIG. 4

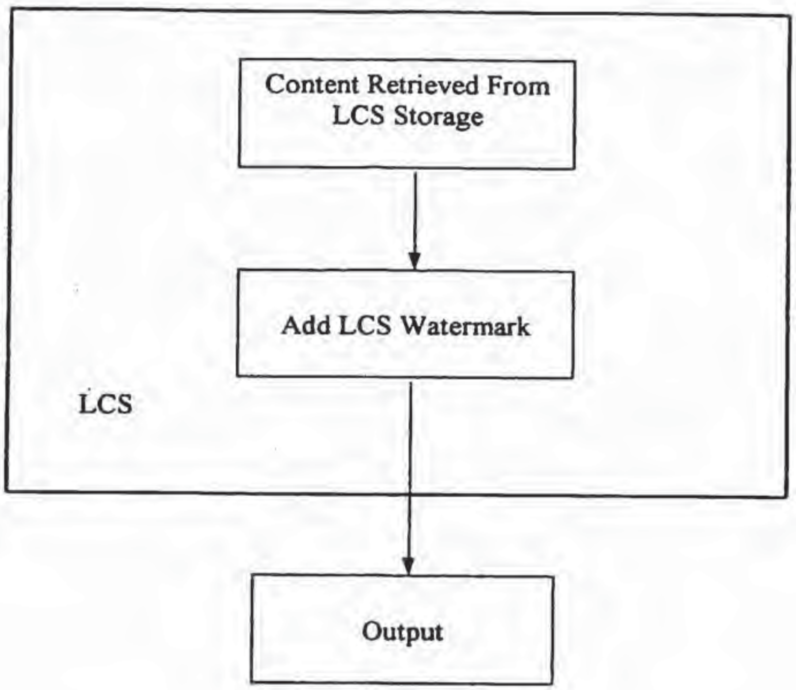

Content Retrieved From LCS Storage
Add LCS Watermark
LCS
Output

FIG. 5

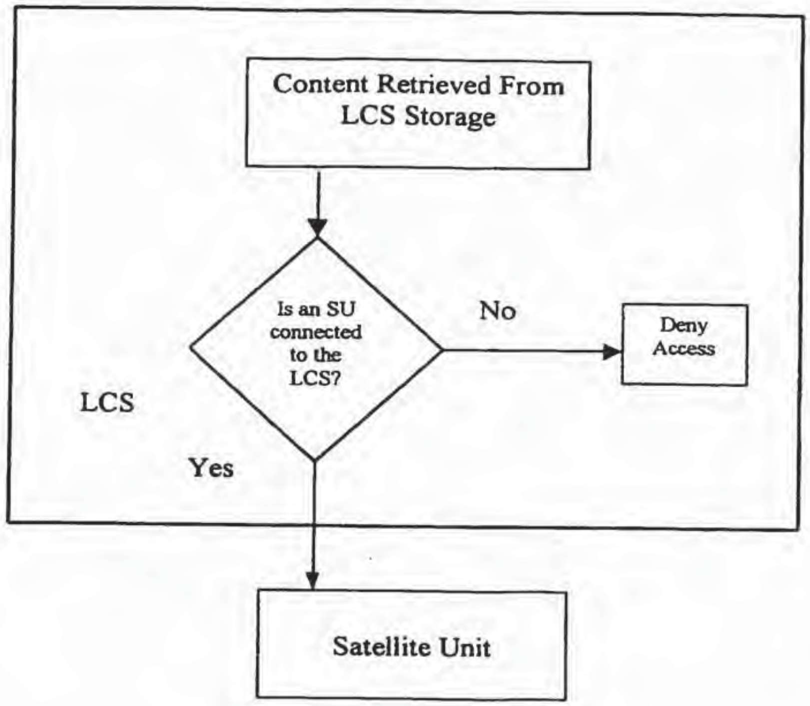

Content Retrieved From LCS Storage
Is an SU connected to the LCS?
No
Deny Access
LCS
Yes
Satellite Unit

FIG. 6

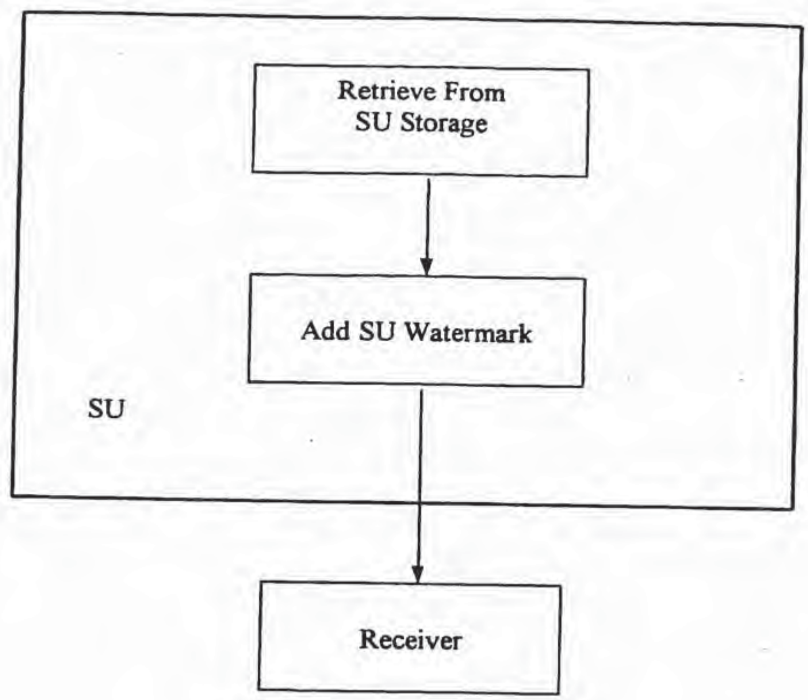


FIG. 7

(12) INTERNATIONAL AP ATION PUBLISHED UNDER THE PATEN OPERATION 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 Classification[7]: H04L 9/32, H04N 7/167

(21) International Application Number: PCT/US00/21189

(22) International Filing Date: 4 August 2000 (04.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: tf Teb 6 2/30

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).

(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, Alburquerque, 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.

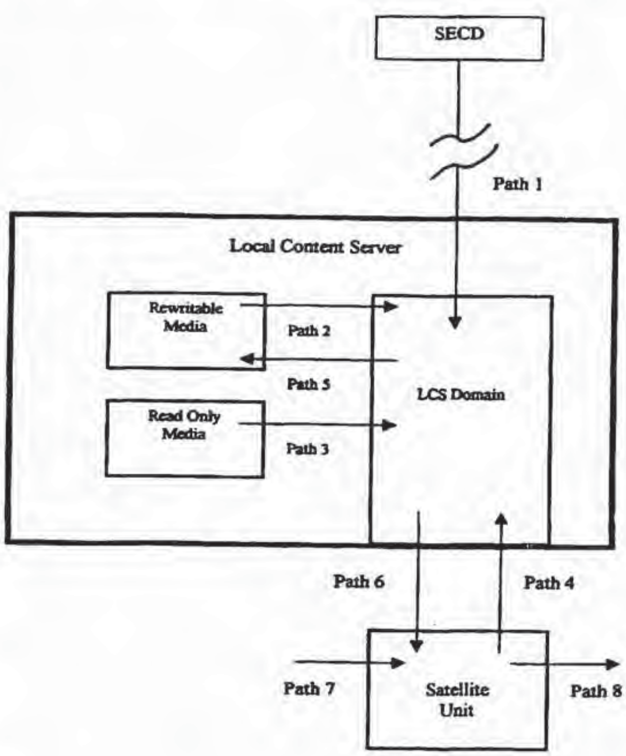
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

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.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 066112.0139	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 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.

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

1. **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 23.1(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 II).
4. With regard to the **title**,
   [X] 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.
   [X] 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
   [X] as suggested by the applicant.
   [ ] because the applicant failed to suggest a figure
   [ ] because this figure better characterizes the invention
   [ ] None of the figures.

Form PCT/ISA/210 (first sheet) (July 1998)★

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

☐ Further documents are listed in the continuation of Box C. ☐ 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

"E" earlier document published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 JANUARY 2001	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 Peggy Harrod Telephone No. (703) 305-3900

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

10/049101

JC13 Rec'd PCT/PTO 0 8 FEB 2002

PTO/SB/17 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
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.

TOTAL AMOUNT OF PAYMENT ($)

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

METHOD OF PAYMENT

1. ☑ 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 Floyd Chapman

☑ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR 1.27

2. ☐ **Payment Enclosed:**

☐ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	370.00
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($) 370.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below	Fee Paid
Total Claims	31	-20** =	11	X		= 99.00
Independent Claims	7	- 3** =	4	X		= 168.00
Multiple Dependent						= 0.00

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
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 claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 637.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	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 *ex parte* reexamination	
112	920*	112	920*	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	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	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 - unavoidable	
141	1,280	241	640	Petition to revive - unintentional	
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify)________

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($) 637.00

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Floyd B. Chapman	Registration No. (Attorney/Agent)	40,555	Telephone	202/719-7000
Signature	Floyd B Chapman			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.

Burden 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.

10/049101
JC13 Rec'd PCT/PTC 08 FEB 2002

PTO/SB/17 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
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.

TOTAL AMOUNT OF PAYMENT ($)

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

METHOD OF PAYMENT

1. ☐ 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 Floyd Chapman

☑ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR 1.27

2. ☑ Payment Enclosed:

☐ Check ☑ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

		Extra Claims	Fee from below	Fee Paid
Total Claims	-20** =		X	=
Independent Claims	- 3** =		X	=
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
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 claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	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 *ex parte* reexamination	
112	920*	112	920*	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	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	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 - unavoidable	
141	1,280	241	640	Petition to revive - unintentional	640.00
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ____________

*Reduced by Basic Filing Fee Paid — SUBTOTAL (3) ($) 640.00

SUBMITTED BY				Complete *(if applicable)*	
Name (Print/Type)	Floyd B. Chapman	Registration No. (Attorney/Agent)	40,555	Telephone	202/719-7000
Signature	Floyd B Chapman			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.

Burden 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.

MAY 1 6 200

#3

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	:	DECISION ON
PCT No.: PCT/US00/21189	:	
Int. Filing Date: 04 August 2000	:	PETITION UNDER
Priority Date: 04 August 1999	:	
Attorney's Docket No.: 80408.0011	:	37 CFR 1.137(b)
For: A SECURE PERSONAL CONTENT	:	
SERVER	:	

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

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. 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
1776 K Street NW
Washington, DC 20006

CONFIRMATION NO. 8028

371 FORMALITIES LETTER

OC000000008153082

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)

DT15 Rec'd PCT/PTO JU 4 2002

Patent
80408.0011US

#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Scott Moskowitz et al.

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

RECEIVED
01 JUL 2002
Legal Staff
International Division

International Application No.: PCT/US00/21189

Filing Date: February 4, 2002

International Filing Date: 04 August 2000

For: A SECURE PERSONAL CONTENT SERVER

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 <u>will be</u> 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

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

JC10 Rec'd PCT/PTO 0 8 FEB 2002

FORM PTO-1390
(REV. 9-2001)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
80408.0011

U.S. APPLICATION NO. (If known, see 37 CFR 1.5
10/049101

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/21189	August 4, 2000	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. [x] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [x] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [ ] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [x] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [x] is attached hereto (required only if not communicated by the International Bureau).
   b. [x] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [x] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [x] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [x] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [x] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [ ] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] 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. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [x] Other items or information:

PCT/IB/308
Copy of Published Application (WO 01/18628)
International Search Report

[redacted]

JC13 Rec'd PCT/PTO 08 FEB 2002

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
10/049101	PCT/US00/21189	80408.0011

21. ☑ The following fees are submitted:

				CALCULATIONS	PTO USE ONLY
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 =				$ 740.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	31 - 20 =	11	x **$18.00**	$ 198.00	
Independent claims	7 - 3 =	4	x **$84.00**	$ 336.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$280.00**	$ 0	
TOTAL OF ABOVE CALCULATIONS =				$ 1,274.00	
☑ 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 ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 0	
TOTAL NATIONAL FEE =				$ 637.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 0	
TOTAL FEES ENCLOSED =				$ 637.00	
				Amount to be refunded:	$
				charged:	$

a. ☐ A check in the amount of $ ______________ to cover the above fees is enclosed.

b. ☑ Please charge my Deposit Account No. 50-1129 in the amount of $ 637.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☑ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1129 . A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **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.

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

Floyd B Chapman
SIGNATURE

Floyd B. Chapman
NAME

40,555
REGISTRATION NUMBER

[redacted]

10/049101
PCT/US00/21189
JC13 Rec'd PCT/PTO 08 FEB 2002

7/prts

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 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 06/23/2000, entitled "A Secure Personal Content Server."

This application also incorporates by reference the following applications: 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 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 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. 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 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.

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 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.

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".

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 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 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 or goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

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 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 are 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.

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). 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 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 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 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. 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-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. 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.

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 examp.e, 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.

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

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 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 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

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:

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.

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.

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.

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 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. 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

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 an 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.

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).

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.

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.

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;

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.

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

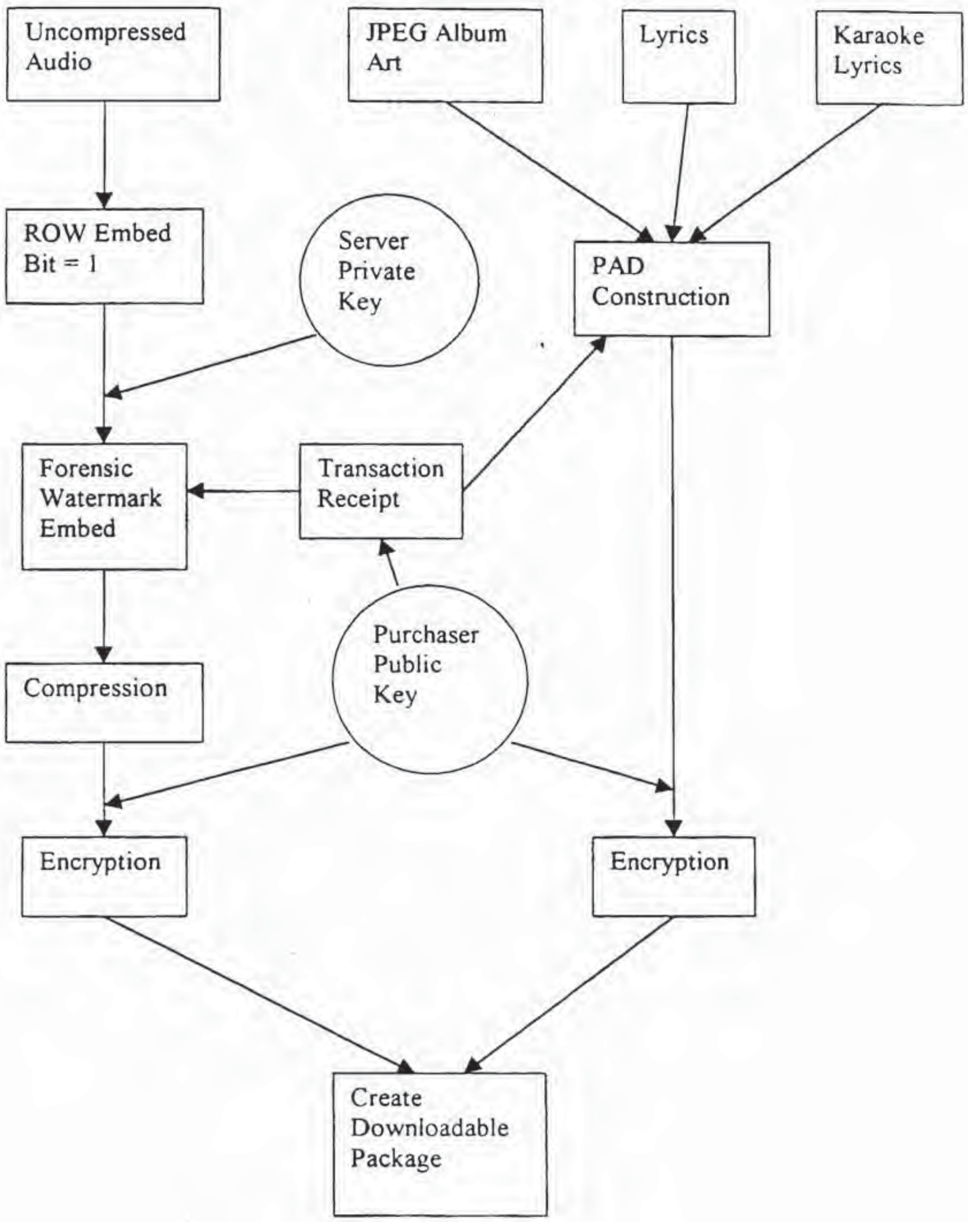


Table 2

SPCS Audio Player Input Stage

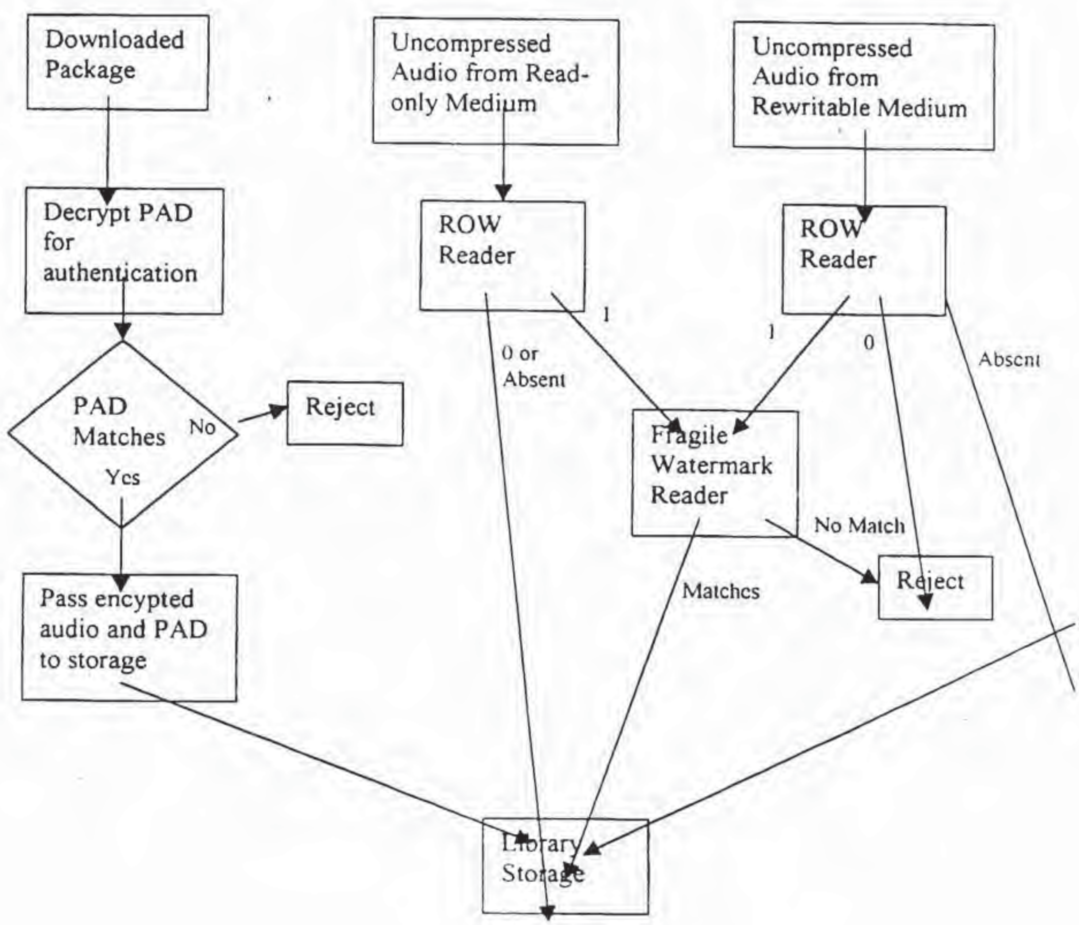
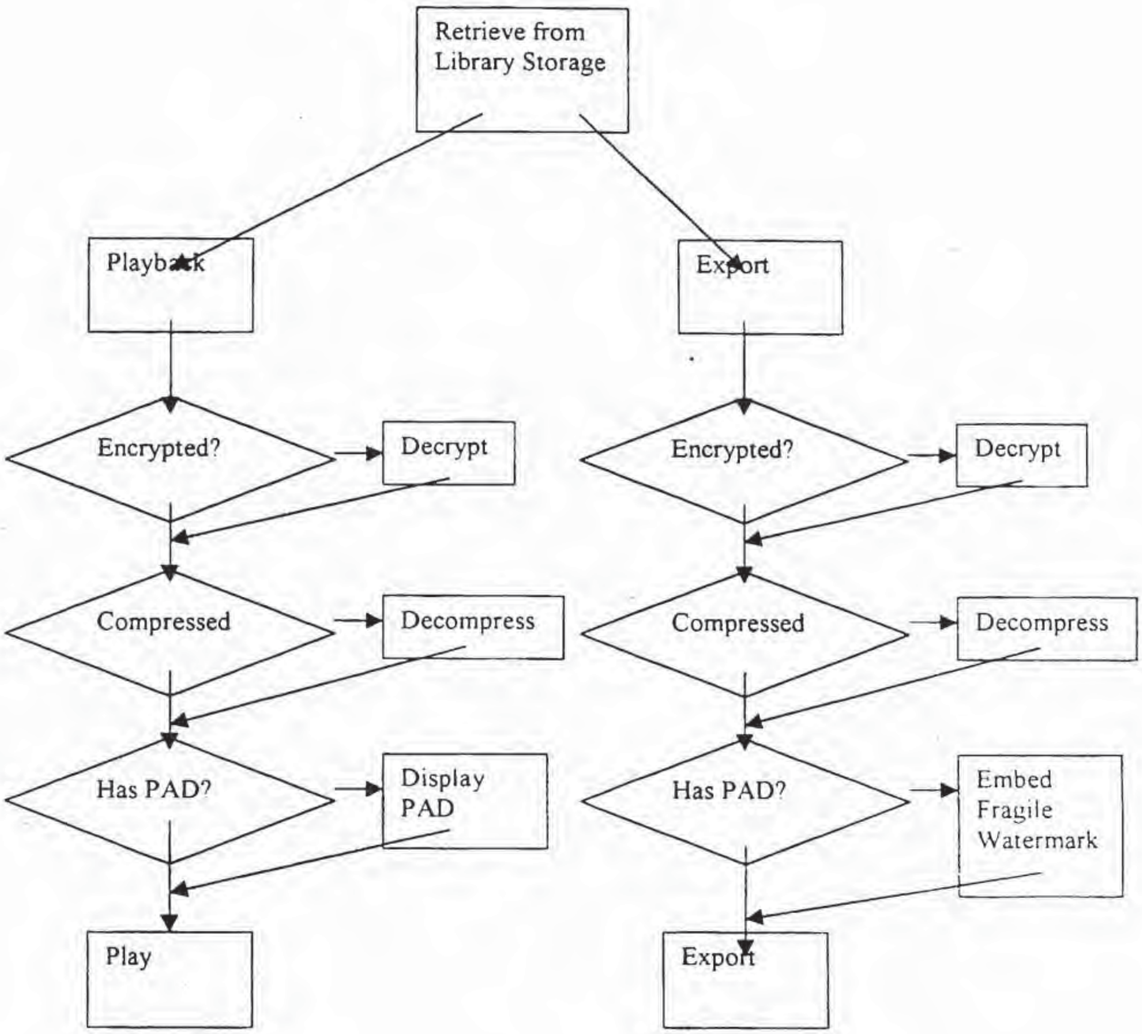


Table 3

SPCS Audio Player Output Stage



Claims:

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

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.

2. 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. 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;

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. 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;

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. 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,

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. 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. 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;

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:

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);

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;

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; 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:

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;

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.

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.

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 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:

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

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

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.

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.

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:

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:

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),

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.

10049101 .072302

(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[7]: G06F

(21) International Application Number: PCT/US00/21189

(22) International Filing Date: 4 August 2000 (04.08.2000)

(25) Filing Language: English

(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

04 Apr 01

(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).

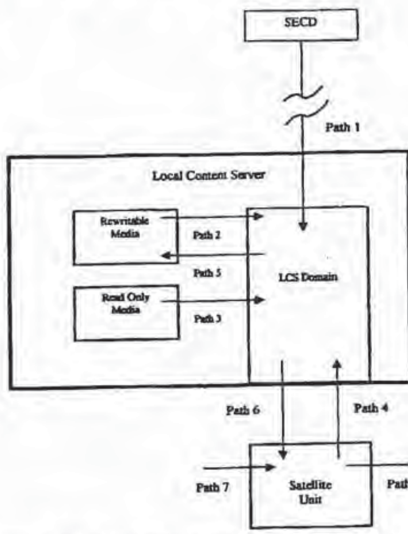
(81) Designated States (national): JP, US.

(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:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



WO 01/18628 A2

(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.

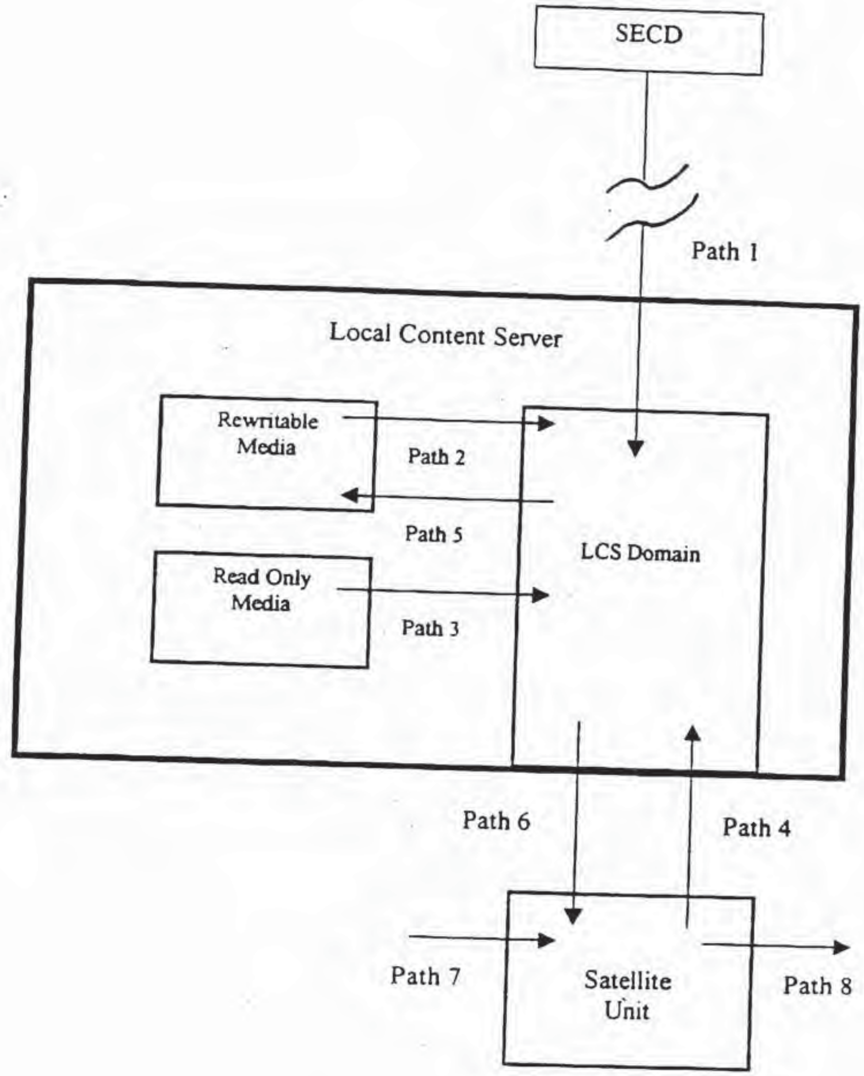

SECD
Path 1
Local Content Server
Rewritable Media
Path 2
Path 5
Read Only Media
Path 3
LCS Domain
Path 6
Path 4
Path 7
Satellite Unit
Path 8

FIG. 1

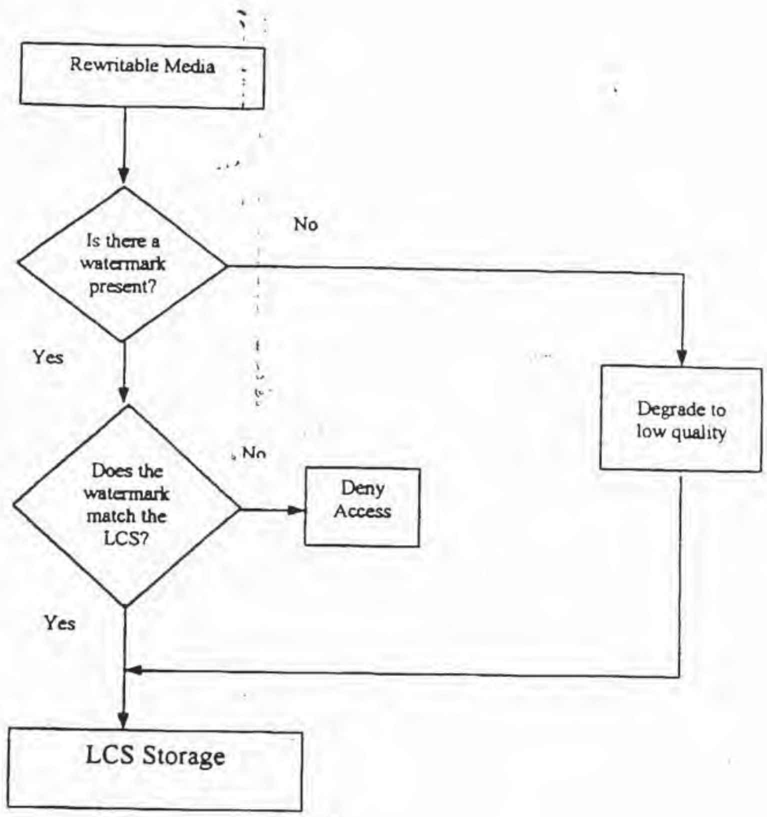

Rewritable Media
Is there a watermark present?
No
Yes
Degrade to low quality
Does the watermark match the LCS?
No
Deny Access
Yes
LCS Storage

FIG. 2

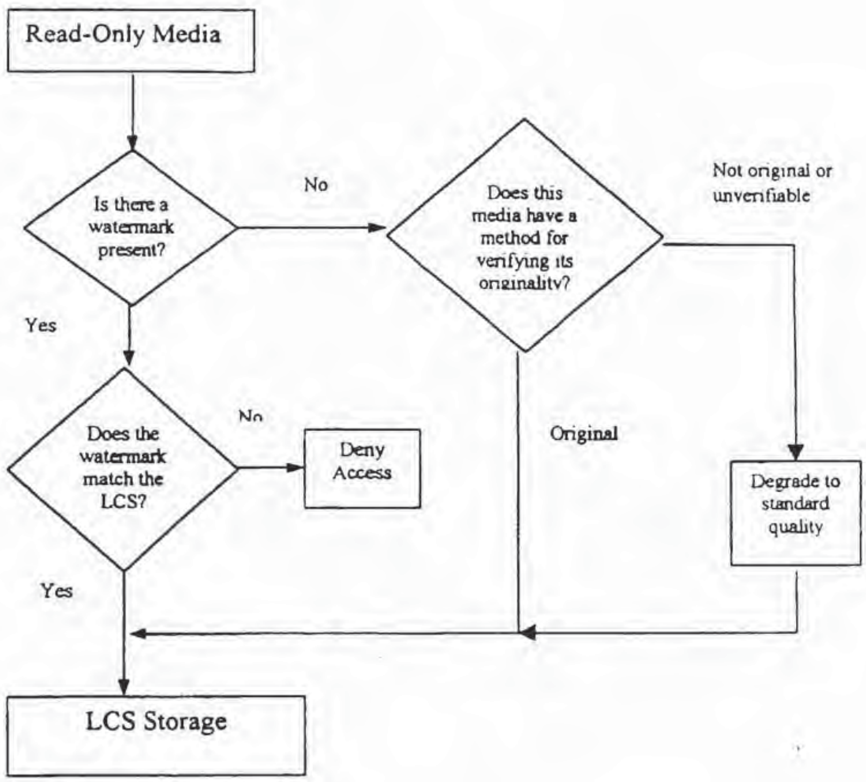

Read-Only Media
Is there a watermark present?
No
Does this media have a method for verifying its originality?
Not original or unverifiable
Yes
Does the watermark match the LCS?
No
Deny Access
Original
Degrade to standard quality
Yes
LCS Storage

FIG. 3

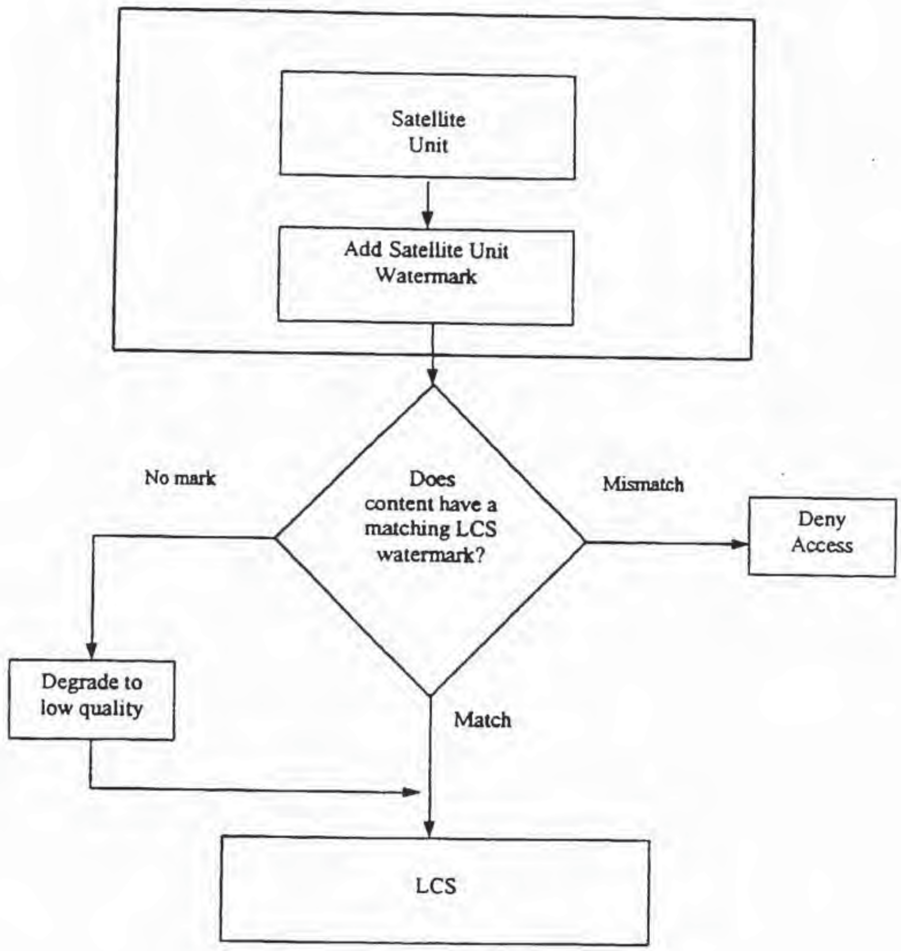

Satellite Unit
Add Satellite Unit Watermark
No mark
Does content have a matching LCS watermark?
Mismatch
Deny Access
Degrade to low quality
Match
LCS

FIG. 4

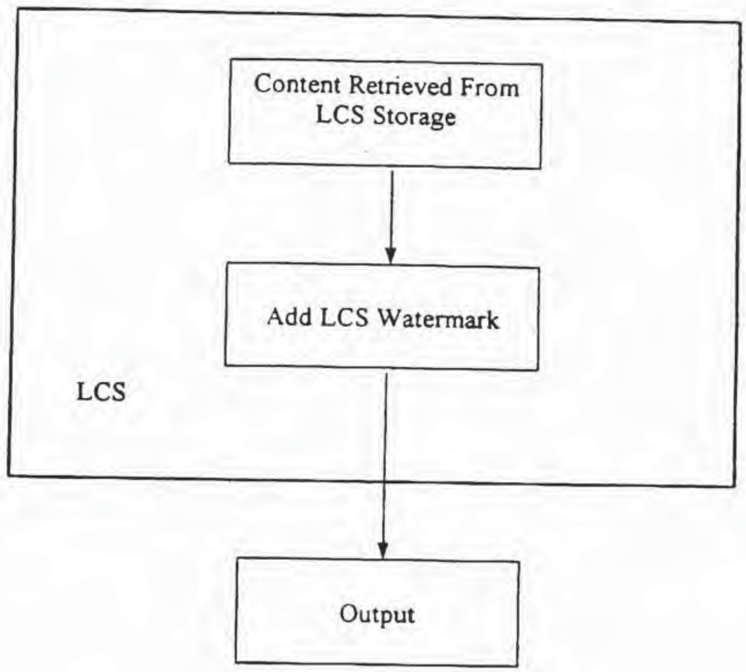

Content Retrieved From LCS Storage
Add LCS Watermark
LCS
Output

FIG. 5

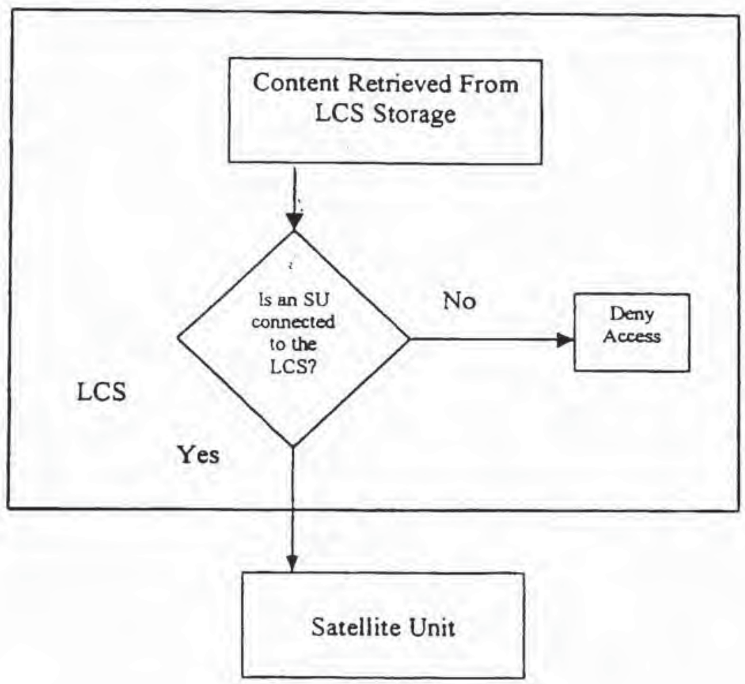

Content Retrieved From LCS Storage
Is an SU connected to the LCS?
No
Deny Access
LCS
Yes
Satellite Unit

FIG. 6

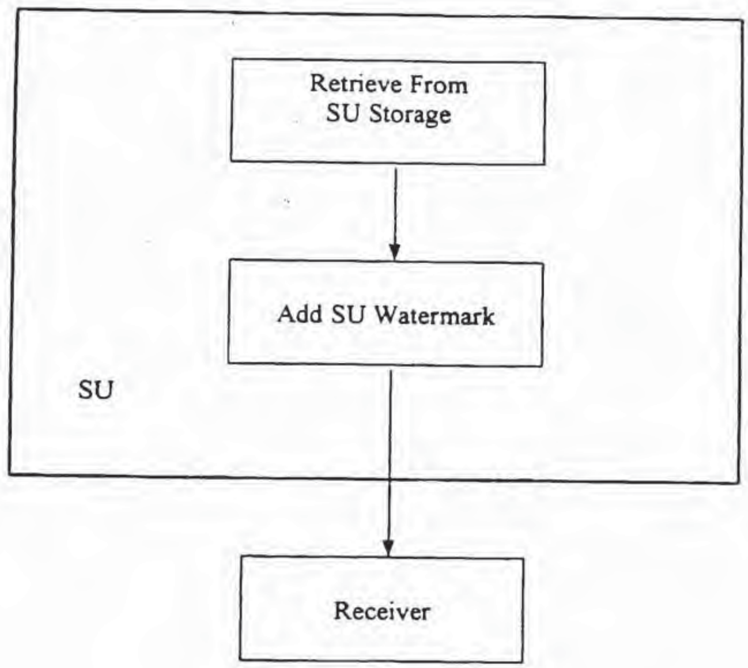


FIG. 7

Signature ______________________ Date ______________

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

2-0

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.

Attorney Docket: 80408.0011

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 ☒	No ☐
				Yes ☐	No ☐

10049101 .012302

PATENT
Attorney Docket No.: 80408.0011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Scott A. Moskowitz et al.	Art Unit: Unassigned
Appl. No.: 10/049,101	Examiner: Unassigned
Filed: February 4, 2002	
For: A SECURE PERSONAL CONTENT SERVER	

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 LLP1776 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.

[redacted]

10049101.072302

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

WRFMAIN 1142767.1

[redacted]

Attorney Docket: 80408.0011

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 ☒	No ☐
				Yes ☐	No ☐

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

10049101.072302

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.

1.00

Signature	Scott A. Moskowitz	Date 7/19/02	
Full Name of First Inventor:	MOSKOWITZ (Family Name)	Scott (First Given Name)	A. (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 (Family Name)	MICHAEL (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

10/049101

PTO/SB/17 (10-01)

Rec'd PCT/PTO

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

#7 Mar-03

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	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

1. [x] 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

[ ] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

[x] Applicant claims small entity status. See 37 CFR 1.27

2. [ ] Payment Enclosed:

[ ] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20** =		X		=	
Independent Claims		- 3** =		X		=	
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
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 claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	65.00
127	50	227	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 *ex parte* reexamination	
112	920*	112	920*	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	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	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 - unavoidable	
141	1,280	241	640	Petition to revive - unintentional	
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 65.00

SUBMITTED BY

Complete (*if applicable*)

Name (Print/Type)	Floyd B. Chapman	Registration No. (Attorney/Agent)	40,555	Telephone	202-719-7000
Signature	Floyd B. Chapman			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.

Burden 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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Bib Data Sheet

CONFIRMATION NO. 8028

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/049,101	07/23/2002 RULE	713	2182	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 **

	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ yes ☐ no 35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance Verified and Acknowledged _____ Examiner's Signature Initials	FL	7	30	7

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:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ________ ☐ Credit

Rec'd PCT/PTO 23 JUL 2002 #9

10/049101

PATENT

Atty Docket No.: 80408.0011

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE

In re 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.

00000120 501129 10049101

65.00 CH

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
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 : COMMUNICATION
Priority Date: 04 August 1999 :
Attorney's Docket No.: 80408.0011 :
For: A SECURE PERSONAL CONTENT :
SERVER :

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.

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

Leonard Smith
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. 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:

07/23/2002	07/23/2002
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	l2 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

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

EXAMINER	
HAST, NATHAN D	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/03/2006

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

PTO-90C (Rev. 10/03)

e

Office Action Summary	Application No.	Applicant(s)
	10/049,101	MOSKOWITZ, SCOTT A.
	Examiner	**Art Unit**
	Nathan D. Hast	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 3 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-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) 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 is 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 associate4 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 7-65, "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	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/049,101	07/23/2002 RULE	713	2136	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 ☐ yes ☒ no 35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance Verified and Acknowledged — Examiner's Signature — Initials	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
	FL	7	30	7

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

TITLE
Secure personal content server

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
702	No. _________ to charge/credit DEPOSIT ACCOUNT No. _________ for following:	☒ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ______________

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
10/049,101	MOSKOWITZ, SCOTT A.
Examiner	**Art Unit**
Nathan D. Hast	2136

X	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim Final	Claim Original	Date 3/15/06
	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 Final	Claim Original	Date
	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 Final	Claim Original	Date
	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	

Search Notes	Application/Control No. 10/049,101	Applicant(s)/Patent under Reexamination MOSKOWITZ, SCOTT A.
	Examiner Nathan D. Hast	Art Unit 2136

SEARCHED

Class	Subclass	Date	Examiner
N/A	N/A	3/15/2006	NDH

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)

	DATE	EXMR
EAST Search - Text Search	3/15/2006	NDH
CiteSeer and Google NPL - Search secure watermark "content distribution "	3/15/2006	NDH

U.S. Patent and Trademark Office

Part of Paper No. 20060315

O-I-P-E IAP45
JUN 0 6 2006
PATENT & TRADEMARK OFFICE

TfM

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

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
Attorney Docket Number	80408.0011

Total Number of Pages in This Submission: 3

ENCLOSURES (Check all that apply)

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ____________
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Revocation of Power of Attorney (Michael Berry); Revocation of Power of Attorney (Scott A. Moskowitz); Revocation of Power of Attorney (Blue Spike)

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Wiley Rein & Fielding LLP
Signature	Floyd B. Chapman
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	7		
Typed or printed name		Date	

O-I-P-E IAP45
JUN 0 6 2006
PATENT & TRADEMARK OFFICE

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

JUN 0 6 2006

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

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 Moskowitz

Scott A. Moskowitz, as President of Blue Spike, Inc.

Th

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 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.

PTO-90C (Rev. 10/03)

Interview Summary	Application No.	Applicant(s)	
	10/049,101	MOSKOWITZ, SCOTT A.	
	Examiner	**Art Unit**	
	Jeremiah Avery	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.

Jeremiah Avery
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 812.01 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.

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, <u>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,</u>

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[.] <u>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.</u>

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. (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 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[itiz]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]<u>m</u>ethod 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<u>, 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</u>.

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

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:

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 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.

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 (thereafter "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 1475, 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 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 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 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 Vaeck, 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

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 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).

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 (01-06)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 180.00

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Examiner Name	Nathan D. HAST
Art Unit	2136
Attorney Docket No.	80408.0011

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) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

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

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
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)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims ____ - 20 or HP = Extra Claims ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ____ - 3 or HP = Extra Claims ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ____ Fee Paid ($) ____

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(s).

Total Sheets ____ - 100 = Extra Sheets ____ / 50 = Number of each additional 50 or fraction thereof ____ (round up to a whole number) x Fee ($) ____ = Fee Paid ($) ____

4. OTHER FEE(S) Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) ____

Other (e.g., late filing surcharge): IDS after first Office Action $180.00

SUBMITTED BY

Signature	Scott A. Moskowitz	Registration No. (Attorney/Agent)	Telephone (305) 956 9041
Name (Print/Type)	Scott A. MOSKOWITZ		Date July 3, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/049,101	Confirmation No. 8028
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 HDESTA1 00000040 10049101
01 FC:1806 180.00 OP

☐ 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";

____ 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 Moskowitz

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.

Scott Moskowitz

Scott A. Moskowitz
President

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
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 contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2136
Examiner Name	HAST, Nathan D.
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 5,636,292	06-03-1997	Rhoads	
		US- 5,629,980	05-13-1997	Stefik et al.	
		US- 5,943,422	08-24-1999	Van Wie et al.	
		US- 5,636,276	06-03-1997	Brugger	
		US- 5,341,429	08-23-1994	Stringer	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

07 - 05 - 06

IFW 2136

OIPE IAP74 JUL 0 3 2006 PATENT & TRADEMARK OFFICE

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2136
Examiner Name	Nathan D. HAST
Attorney Docket Number	80408.0011

Total Number of Pages in This Submission

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ______
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott A. Moskowitz		
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	Scott Moskowitz		
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 and1.14. 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.

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~~ 11
INDEPENDENT CLAIMS	7 minus 3 =	* 4
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* 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		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

7-3-06

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 31	Minus	** 30	= 0
Independent	* 7	Minus	*** 7	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE		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	

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

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

AMENDMENT C	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		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.

FORM PTO-875 (Rev. 8/01)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

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 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

CONFIRMATION NO. 8028

OC000000019864599

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

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

CONFIRMATION NO. 8028

OC000000019864569

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

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 TSIGE
PTOSS (703) 305-3006

OFFICE COPY

A

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 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.

PTO-90C (Rev. 10/03)

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No. 10/049,101	Applicant(s) MOSKOWITZ, SCOTT A.	
	Examiner Jeremiah Avery	Art Unit 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 is 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

OCT 20 2006 OIPE PATENT & TRADEMARK OFFICE

PTO/SB/21 (08-06)
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 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2131
Examiner Name	Jeremiah L. AVERY
Attorney Docket Number	80408.0011

Total Number of Pages in This Submission

ENCLOSURES (Check all that apply)

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ______
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

✓ Reply to Notice of Non Compliant Amendment (37 CFR 1.121)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	
Signature	Scott Moskowitz
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	Scott Moskowitz		
Typed or printed name	Scott A. MOSKOWITZ	Date	October 20, 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; 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 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 [[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. (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);

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[itiz]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.

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.

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:

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.

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

Application or Docket Number

10/049101

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	30 minus 20=	* ~~+0~~ 11
INDEPENDENT CLAIMS	7 minus 3 =	* 4
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* 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		RATE	FEE
BASIC FEE	370	OR	BASIC FEE	
X$ 9=	99	OR	X$18=	
X42=	168	OR	X84=	
+140=		OR	+280=	
TOTAL	628	OR	TOTAL	

CLAIMS AS AMENDED - PART II

7-3-06

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 31	Minus	** 30	= 0
Independent	* 7	Minus	*** 7	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL FEE
X$ 9=	0	OR	X$18=	
X42=	0	OR	X84=	
+140=	0	OR	+280=	
TOTAL ADDIT. FEE	0	OR	TOTAL ADDIT. FEE	

10/20/06

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* Same	Minus	as	= above
Independent	*	Minus		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL 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.

FORM PTO-875 (Rev. 8/01) Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

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	**PAPER NUMBER**
2131	

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. 10/049,101	Applicant(s) MOSKOWITZ, SCOTT A.	
	Examiner Jeremiah Avery	Art Unit 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:

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. ____

CHRISTOPHER REVAK
PRIMARY EXAMINER

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..

OIPE IAP10 FEB 07 2007 PATENT & TRADEMARK OFFICE

2-8-07

TFW 2131

PTO/SB/21 (09-06)
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 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

Total Number of Pages in This Submission

ENCLOSURES (Check all that apply)

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ______
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks
37 CFR 1.121

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
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	Scott Moskowitz		
Typed or printed name	Scott A. MOSKOWITZ	Date	February 7, 2007

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

OIPE IAP19
FEB 0 7 2007
PATENT & TRADEMARK OFFICE

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[[.]] <u>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.</u>

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, <u>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,</u>

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[[.]] <u>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.</u>

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 <u>that</u> 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[[itiz]]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<u>, 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</u>; 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]]<u>m</u>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;

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.

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:

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.

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	30 minus 20=	* +10 11
INDEPENDENT CLAIMS	7 minus 3 =	* 4
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* 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		RATE	FEE
BASIC FEE	370	OR	BASIC FEE	
X$ 9=	99	OR	X$18=	
X42=	168	OR	X84=	
+140=	/	OR	+280=	
TOTAL	628	OR	TOTAL	

CLAIMS AS AMENDED - PART II

7-3-06

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 31	Minus	** 30	= 0
Independent	* 7	Minus	*** 7	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE		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	

2-7-07

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 31	Minus	** 31	=
Independent	* 7	Minus	*** 7	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

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

AMENDMENT C	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		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.

FORM PTO-875 (Rev. 8/01) Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Best Available Copy

04-18-07 TFW 2131

PTO/SB/21 (09-06)
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 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott MOSKOWITZ
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

Total Number of Pages in This Submission

ENCLOSURES (Check all that apply)

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ___________
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
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	Scott Moskowitz		
Typed or printed name	Scott MOSKOWITZ	Date	April 17, 2007

PTO/SB/17 (02-07)
Approved for use through 02/28/2007. OMB 0651-0032
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

Effective on 12/08/2004.
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

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott MOSKOWITZ
Examiner Name	Jeremiah AVERY
Art Unit	2131
Attorney Docket No.	80408.0011

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) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

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

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fees Paid ($)**
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)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims ______ - 20 or HP = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______

HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims — **Fee ($)** ______ **Fee Paid ($)** ______

Indep. Claims ______ - 3 or HP = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______

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(s).

Total Sheets ______ - 100 = **Extra Sheets** ______ / 50 = **Number of each additional 50 or fraction thereof** ______ (round up to a whole number) x **Fee ($)** ______ = **Fee Paid ($)** ______

4. OTHER FEE(S) **Fees Paid ($)**

Non-English Specification, $130 fee (no small entity discount) ______

Other (e.g., late filing surcharge): Information Disclosure Statement $180.00

SUBMITTED BY

Signature	Scott Moskowitz	Registration No. (Attorney/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 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 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-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 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 § 1.56(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:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.

Scott A. Moskowitz
President

APR 17 2007

PTO/SB/08B (09-06)
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 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)

Sheet 1 of 6

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

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 Crypography, 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 Practioner'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.vmich.edu/iep/works/SarkAsses.html on	
		Crawford, D.W. "Pricing Network Usage:A Market for Bandwith of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March	
		LOW, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.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.) Viewing Publishing Company Germany 1995	
		Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the european conf. on Mulitmedia Applications, Services & Techinques Louvain-La-Nevve, Belgium, May 1996	

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.
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 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 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, Alaxandria, 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 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.[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]
		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.Sc., 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 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] 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 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 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 6

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

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]
		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	
		Puate, 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 Neos Marmaras pp. 4	
		Van Schyandel, et al., Towards a Robust Digital Watermark, Second Asain 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.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
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 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)

Sheet 4 of 6

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

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]
		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 Institude, Techinal Report 95-10, pp. 33	
		Kahn, D., The Code Breakers, The MacMillan Company, 1969, pp. xIII, 81-83,513,515,522-526,863.	
		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 Mulitmedia 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 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.

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 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 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 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 5 of 6

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]
		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.	
		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 Hiróshima, Japan, 0-8186-7436-9196, 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, Bandwith 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., "PayWord 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 609. 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 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 6

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

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]
		Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB	
		Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security, Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 April 10, 2002, pp. 80-84	
		Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006, (to appear) 13	
		Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Crytography Research, Inc. 2002-2003, 14 pages	
		Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring), 5 March 1995, pp. 20-25, vol. CONF40	
		Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, 30 Sept 1998, pp. 1501-1510, Vol. 30, No. 16-18, NL, North Holland	
		Konrad, K. et al., "Trust and Elecronic Commerce-more than a techinal problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, 19-22 October 1999, pp. 360-365, Lausanne	
		Kini, a. et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216), 6-9 January 1998, pp. 51-61, Los	
		Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sept 1997, pp 118-124, vol. 5 No. 3, ACM, USA	
		Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp 1079-1107, July 1999, Vol. 87 No. 7, IEEE	

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.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

APR 1 7 2007

PTO/SB/08A (09-06)
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 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)

Sheet 1 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 Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,939,515	07/03/1990	Adelson	
		US-5,161,210	11/03/1992	Druyvesteyn,et.al.	
		US-5,450,490	09/12/1995	Jensen et.al.	
		US-5,530,751	06/25/1996	Morris	
		US-5,579,124	11/26/1996	Aijala 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	05/05/1998	Rhoads	
		US-6,330,672	12/11/2001	Shur	
		US-5,243,423	09/07/1993	DeJean et.al.	
		US-5,319,735	06/07/1994	Preuss et.al	
		US-5,113,437	05/12/1992	Best et.al.	
		US-4,876,617	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	Hustig et.al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		European Patent No. EP0565947A1	10/20/1993	Kuusama, 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 609. 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 Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

Sheet 2 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 Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,748,668	05/31/1998	Shamir, et.al.	
		US-4,789,928	12/06/1988	Fujisaki	
		US-4,908,873	03/13/1990	Philibert, et.al.	
		US-4,980,782	12/25/1990	Ginkel	
		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	Narasimhalv, et.al	
		US-5,487,168	01/23/1996	Geiner, et.al.	
		US-5,493,677	02/20/1996	Balogh, et.al	
		US-5,530,759	06/25/1996	Braudaway, et.al	
		US-5,606,609	02/25/1997	Houser, 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.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 99/62044	12/02/1999	Handel, 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 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. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

Sheet 2 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 Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		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	Rivest 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	Rabbani	
		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	Waggener	
		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.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 9744736	11/27/1997	Wehrenberg		
		WO 9952271	10/14/1999	Moskowitz		
		WO 9963443	12/09/1999	Ho, Anthony Tung Shuen		

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. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

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 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 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.

PTO/SB/08A (09-06)
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 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)

Sheet 4 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: Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,640,569	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-5,745,569	04/28/1998	Moskowitz, et.al	
		US-5,506,795	04/09/1996	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	Sharma, et.al	
		US-6,530,021	03/04/2003	Epstein, et.al.	
		US-6,425,081	07/23/2002	Iwamura	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

Substitute 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

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,522,769	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	Choy	
		US-6,493,457	12/10/2002	Quackenbush	
		US-5,629,980	05/13/1997	Stefik, et al.	
		US-5,943,422	08/24/1999	Van Wie, et al.	
		US-5,636,276	06/03/1997	Brugger	
		US-5,341,429	08/23/1994	Stringer, et.al.	
		US-6,754,822	06/22/2004	Zhao	
		US-6,131,162	10/10/2000	Yoshiura et.al.	
		US-7,058,570	06/06/2006	Yu, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

Sheet 6 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 Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,930,369	07/27/1999	Cox, et al.	
		US-6,415,041	07/02/2002	Oami, 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	Stefik, et al.	
		US-2006/0013395	01/19/2006	Brundage, et.al.	
		US-7,043,050	05/09/2006	Yuval	
		US-5,809,160	09/15/1998	Powell, et.al.	
		US-6,272,634	08/07/2001	Tewfik, et.al.	
		US-6,282,650	08/28/2001	Davis	
		US-6,557,103	04/29/2003	Boncelet, 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	Honsinger, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

Sheet 7 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 Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,061,793	05/09/2000	Tewfik, et.al	
		US-5,809,139	09/15/1998	Girod, 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	Cox	
		US-5,943,422	08/24/1999	Van Wie, 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	Jones, 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	Gennaro, et.al.	
		US-6,081,587	06/27/2000	Hoffstein, et.al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] "Number[4] "Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

Sheet 8 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 Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,598,162	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	06/29/1999	Hirose	
		US-6,775,772	08/10/2004	Binding, et al.	
		US-6,668,246	12/23/2003	Yeung, et al.	
		US-6,351,765	02/26/2002	Pietropaolo, et al.	
		US-6,049,838	04/11/2000	Miller, et al.	
		US-5,398,285	03/14/1995	Borgelt, et al.	
		US-5,737,733	04/07/1998	Eller	
		US-2002/0103883	08/01/2002	Haverstock, 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	Laroche	
		US-5,077,665	12/31/1991	Silverman, et al.	
		US-5,136,581	08/04/1992	Muehrcke	
		US-5,341,477	08/23/1994	Pitkin, et al.	
		US-5,581,703	12/03/1996	Baugher, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

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 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 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.

PTO/SB/08A (09-06)
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 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)

Sheet 9 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 (Number-Kind Code[2] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,548,579	08/20/1996	Lebrun, et al.	
		US-5,905,975	05/18/1999	Ausubel	
		US-6,457,058	09/24/2002	Ullum 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	Poole et al.	
		US-5,884,033	03/16/1999	Duvall 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-6,606,393	08/12/2003	Xie et al.	
		US-6,584,125	06/24/2003	Katto	
		US-6,442,283	08/27/2002	Tewfik 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	Malvar	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document (Country Code[3] Number[4] Kind Code[5] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

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 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 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.

PTO/SB/08A (09-06)
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 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)

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.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		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-5,790,677	08/04/1998	Fox et al.	
		US-5,243,515	09/07/1993	Clearwater	
		US-4,339,134	07/13/1982	Macheel	
		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	Follendore, III	
		US-5,406,627	04/11/1995	Thompson et al.	
		US-5,410,598	04/25/1995	Shear	
		US-5,469,536	11/21/1995	Blank	
		US-5,497,419	03/05/1996	Hill	
		US-5,513,261	04/30/1996	Maher	
		US-5,530,739	06/25/1996	Okada	
		US-5,598,470	01/28/1997	Cooper et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

PTO/SB/08A (09-06)
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 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)

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: Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,625,690	04/29/1997	Michel et al.	
		US-5,633,932	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	Conley	
		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	Saito	
		US-5,999,217	12/07/1999	Berners-Lee	
		US-6,041,316	03/21/2000	Allen	
		US-6,081,251	06/27/2000	Sakai 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	Senoh	
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] -Number[4] -Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

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 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 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.

PTO/SB/08A (09-06)
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 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)

Sheet 12 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 Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,088,455	07/11/2000	Logan et al.	
		US-5,634,040	05/27/1997	Her et al.	
		US-6,381,747	04/30/2002	Wonfor et al.	
		US-4,969,204	11/06/1990	Melnychuck et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [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.

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 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 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.

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.

P.D. 08.11.98
p. 684-689 = 6

BG235120

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.

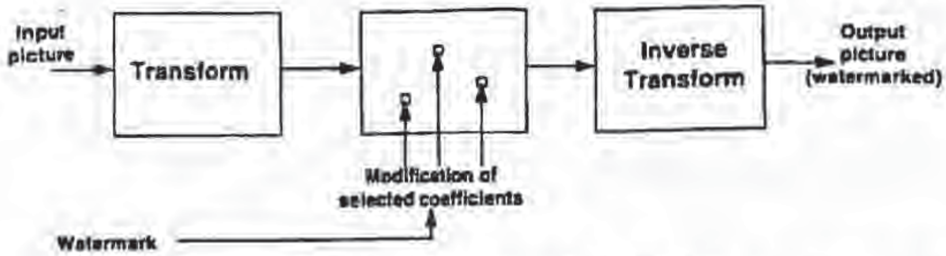


Figure 1. Transform based watermark write operation.

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 Daubechy 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.

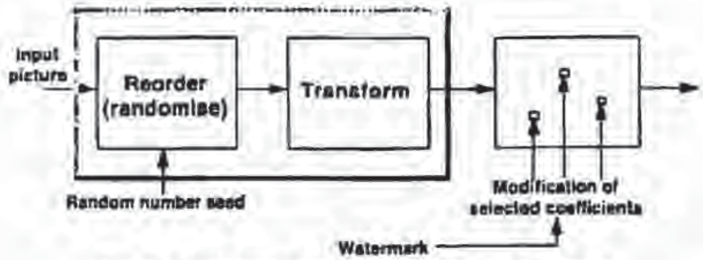


Figure 2. Transform permuted watermark write operation

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.

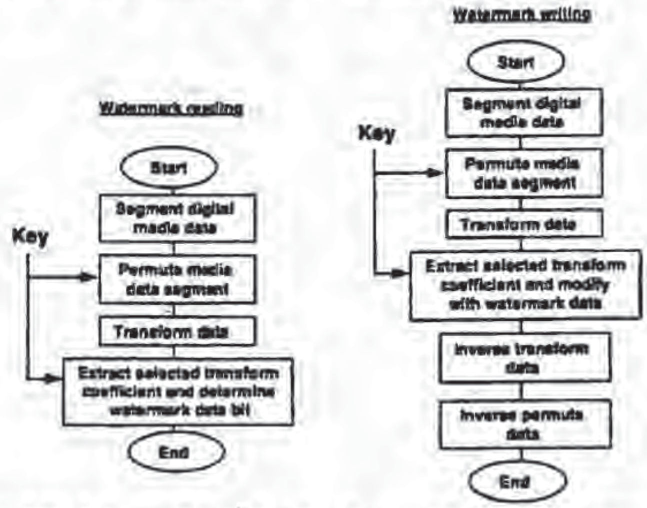


Figure 3 Block diagram for transform based watermark read and write operation

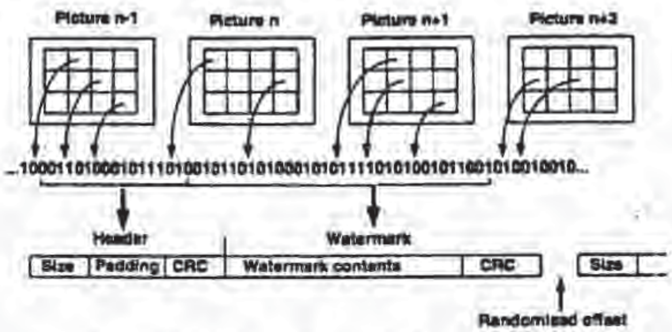


Figure 4 Packet based structure of watermark data.

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

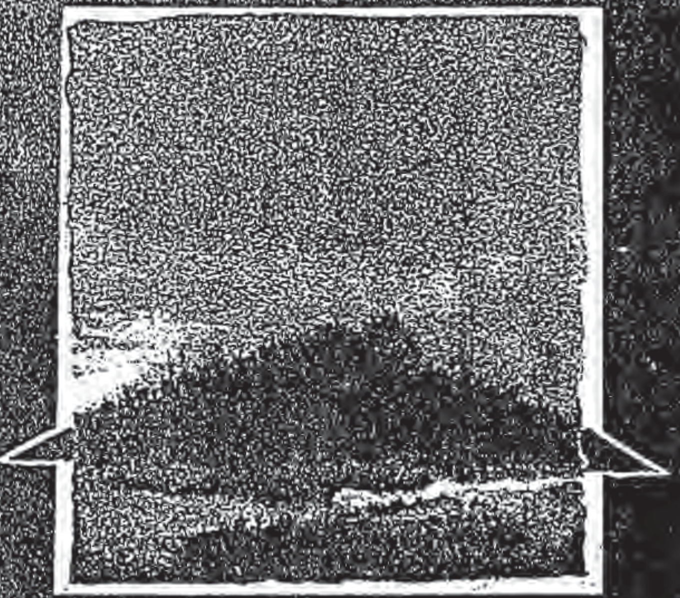
While the original picture might be watermarked at a high resolution near the production end of the delivery chain, it is important to protect against two common processes which would otherwise compromise the ability to read the watermark:

- 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

ever seen .... The book the National Security Agency wanted never to be published...
—Wired Magazine

SECOND EDITION

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.

k of

APPLIED CRYPTOGRAPHY

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone

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
005.8'2--dc20

96-27609
CIP

International Standard Book Number 0-8493-8523-7
Library of Congress Card Number 96-27609
Printed in the United States of America 3 4 5 6 7 8 9 0
Printed on acid-free paper

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 Bosselaers, 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. Salomaa [1089], Stinson [1178], and Rivest [1054] present more mathematical approaches. Davies and Price [308] provide a very readable presentation suitable for the practitioner.

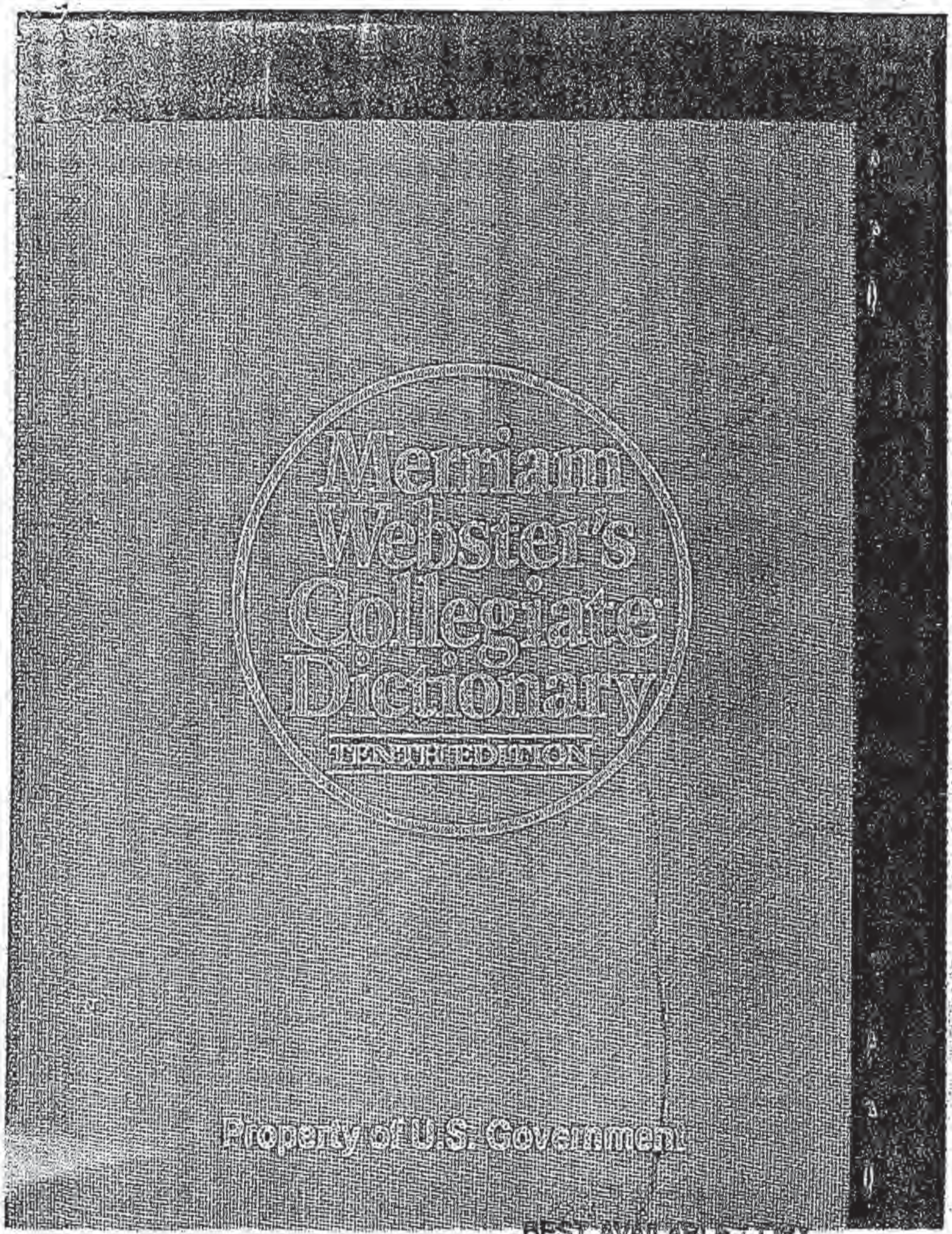
The comparison of an encryption scheme to a resettable combination lock is from Diffie and Hellman [347]. Kerckhoffs' desiderata [668] were originally stated in French. The translation stated here is given in Kahn [648]. Shannon [1121] also gives desiderata for encryption schemes.

§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 Konheim [705]. Beker and Piper [84] give an indepth 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



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.

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 (deluxe : alk. paper). — ISBN 0-87779-707-2 (laminated cover).
1. English language—Dictionaries. I. Merriam-Webster, Inc.
PE1628.M36 1997
423—dc20 96-42529
CIP

Made in the United States of America

1718192ORMcN97

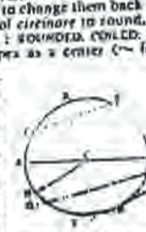
Abbrevia

BEST AVAILABLE COPY

garden or potted plants derived from a perennial composite
(Senecio cruentus) of the Canary Islands and having heart-shaped
leaves and clusters of bright flower heads
cin-e-rar-i-um \-ē-əm\ n, pl -ia \-ē-ə\ [L, fr. ciner-, cinis] (1880) : a
place to receive the ashes of the cremated dead — cin-er-ary \'si-nə-
rer-ē\ adj
ci-ne-re-ous \sə-'nir-ē-əs\ adj [L cinereus fr. ciner-, cinis] (1661) 1
: gray tinged with black 2 : resembling or consisting of ashes
cin-er-in \'si-nə-rən\ n [L ciner-, cinis] (1948) : either of two oily liquid
esters $C_{20}H_{28}O_3$ and $C_{21}H_{28}O_5$ occurring esp. in the flowers of pyre-
thrum and possessing insecticidal properties
cin-gu-lum \'siŋ-gyə-ləm\ n, pl -la \-lə\ [NL, fr. L, girdle, fr. cingere to
gird — more at CINCTURE] (1843) : an anatomical band or encircling
ridge — cin-gu-late \-lət\ adj
cin-na-bar \'si-nə-,bär\ n [ME cynabare, fr. MF & L; MF cenobre, fr. L
cinnabaris, fr. Gk kinnabari, of non-IE origin; akin to Ar zinjafr cinna-
bar] (14c) 1 : artificial red mercuric sulfide used esp. as a pigment 2
: native red mercuric sulfide HgS that is the only important ore of
mercury — cin-na-bar-ine \-,bä-,rīn, -,bär-ən\ adj
cinnabar moth n (ca. 1893) : a European moth (Tyria jacobaeae) that
has been introduced into the western U.S. in attempts to control the
tansy ragwort on which its larvae feed — called also cinnabar
cin-na-mic acid \sə-'na-mik-\ n [F cinnamique of cinnamon, fr. cin-
name cinnamon, fr. L cinnamomum] (ca. 1864) : a white crystalline
odorless acid $C_9H_8O_2$ found esp. in cinnamon oil and storax
cin-na-mon \'si-nə-mən\ n, often attrib [ME cynamone, fr. L cin-
namomum, cinnamon, fr. Gk kinnamōmon, kinnamon, of non-IE ori-
gin; akin to Heb qinnāmōn cinnamon] (14c) 1 a : any of several
Asian trees (genus Cinnamomum) of the laurel family b : an aromatic
spice prepared from the dried inner bark of a cinnamon (esp. C zeylani-
cum); also : the bark 2 : a light yellowish brown
cinnamon fern n (1818) : a large fern (Osmunda cinnamomea) with
cinnamon-colored spore-bearing fronds shorter than and separate from
the green foliage fronds
cinnamon stone n (1805) : ESSONITE
cinq-quain \'siŋ-,kān, 'saŋ-\ n [F, fr. cinq five, fr. L quinque — more at
FIVE] (1882) : a 5-line stanza
cin-que-cen-tist \,chiŋ-kwi-'chen-tist\ n (1871) : an Italian of the cin-
quecento; esp : a poet or artist of this period
cin-que-cen-to \,chiŋ-kwi-'chen-(,)tō\ n [It, lit., five hundred, fr. cinque
five (fr. L quinque) + cento hundred, fr. L centum — more at HUN-
DRED] (1760) : the 16th century esp. in Italian art and literature
cinque-foil \'siŋk-,fȯil, 'saŋk-\ n [ME sink foil, fr.
MF cincfoille, fr. L quinquefolium, fr. quinque five +
folium leaf — more at BLADE] (14c) 1 : any of a
genus (Potentilla) of herbs and shrubs of the rose
family with 5-lobed leaves and 5-petaled flowers —
called also potentilla 2 : a design enclosed by five
joined foils

cinquefoil 2

cio-pi-no \chə-'pē-(,)nō\ n [perh. fr. It dial.] (1936)
: a dish of fish and shellfish cooked usu. with toma-
toes, wine, spices, and herbs
ci-pher \'sī-fər\ n, often attrib [ME, fr. MF cifre, fr.
ML cifra, fr. Ar ṣifr empty, cipher, zero] (14c) 1 a
: ZERO 1a b : one that has no weight, worth, or influence : NONENTITY
2 a : a method of transforming a text in order to conceal its meaning
— compare CODE 3b b : a message in code 3 : ARABIC NUMERAL 4
: a combination of symbolic letters; esp : the interwoven initials of a
name
cipher vb ci-phered; ci-pher-ing \-f(ə-)riŋ\ vi (ca. 1530) : to use
figures in a mathematical process ~ vt 1 : ENCIPHER 2 : to compute
arithmetically
ci-pher-text \'sī-fər-,tekst\ n (1939) : the enciphered form of a text or
of its elements — compare PLAINTEXT
cir-ca \'sər-kə\ prep [L, fr. circum around — more at CIRCUM-] (1861)
: at, in, or of approximately — used esp. with dates (born ~ 1600)
cir-ca-di-an \,sər-'ka-dē-ən\ adj [L circa about + dies day + E -an —
more at DEITY] (1959) : being, having, characterized by, or occurring in
approximately 24-hour periods or cycles (as of biological activity or
function) (~ rhythms in activity)
Cir-cas-sian \(,)sər-'ka-sh(ē-)ən\ n [Circassia, region of the Caucasus]
(1555) 1 : a member of a group of peoples of the northwestern Cauca-
sus 2 : the language of the Circassian peoples — Circassian adj
Circassian walnut n (1914) : the light brown irregularly black-veined
wood of the English walnut much used for veneer and cabinetwork
Cir-ce \'sər-(,)sē\ n [L, fr. Gk Kirkē] : a sorceress who changes Odys-
seus' men into swine but is forced by Odysseus to change them back
cir-ci-nate \'sər-sə-,nāt\ adj [L circinatus, pp. of circinare to round, fr.
circinus pair of compasses, fr. circus] (1830) : ROUNDED, COILED; esp
: rolled in the form of a flat coil with the apex as a center (~ fern
fronds unfolding) — cir-ci-nate-ly adv
cir-cle \'sər-kəl\ n, often attrib [ME cercle, fr.
OF, fr. L circulus, dim. of circus circle, circus,
[illegible] kirkos ring; akin to
[illegible] RING] (14c) 1 a
[illegible] plane curve every
[illegible] from a fixed
[illegible] : the plane surface
[illegible] the orbit of a
[illegible] in the form of a
[illegible] a circle
[illegible] of the spots in a
[illegible] on the surface of a
[illegible] of a plane that
[illegible] influence : REALM
[illegible] has come full
[illegible] in which some-
[illegible] covertly assumed
[illegible] of persons sharing a common
[illegible] revolving about a common center
[illegible] of the church) (family —) (the



circle 1b: AB diameter; C center; CG, CA, CE radii; EF arc on chord EF; EFKL (area) segment on chord EF; ACD (area) sector; GH secant; TPM tangent at point P; EKFBDA circumference

gossip of court ~s) 7 : a territorial or administrative division or dis-
trict 8 : a curving side street
²circle vb cir-cled; cir-cling \-k(ə-)liŋ\ vt (14c) 1 : to enclose in or as
if in a circle 2 : to move or revolve around ~ vi 1 a : to move in
or as if in a circle b : CIRCULATE 2 : to describe or extend in a circle
— cir-cler \-k(ə-)lər\ n
circle graph n (1928) : PIE CHART
cir-clet \'sər-klət\ n (13c) : a little circle; esp : a circular ornament
¹cir-cuit \'sər-kət\ n, often attrib [ME, fr. MF circuite, fr. L circuitus, fr.
circumire, circuire to go around, fr. circum- + ire to go — more at
ISSUE] (14c) 1 a : a usu. circular line encompassing an area b : the
space enclosed within such a line 2 a : a course around a periphery
b : a circuitous or indirect route 3 a : a regular tour (as by a travel-
ing judge or preacher) around an assigned district or territory b : the
route traveled c : a group of church congregations ministered to by
one pastor 4 a : the complete path of an electric current including
usu. the source of electric energy b : an assemblage of electronic ele-
ments : HOOKUP c : a two-way communication path between points
(as in a computer) 5 a : an association of similar groups : LEAGUE b
: a number or series of public outlets (as theaters, radio shows, or
arenas) offering the same kind of presentation c : a number of similar
social gatherings (cocktail ~) — cir-cuit-al \-kə-tᵊl\ adj
²circuit vt (15c) : to make a circuit about ~ vi : to make a circuit
circuit board n (1948) : BOARD 9
circuit breaker n (1872) : a switch that automatically interrupts an
electric circuit under an infrequent abnormal condition
circuit court n (1708) : a court that sits at two or more places within
one judicial district
circuit judge n (1801) : a judge who holds a circuit court
cir-cu-i-tous \(,)sər-'kyü-ə-təs\ adj [perh. fr. ML circuitosus, fr. L cir-
cuitus] (1664) 1 : having a circular or winding course (a ~ route) 2
: not being forthright or direct in language or action — cir-cu-i-tous-
ly adv — cir-cu-i-tous-ness n
circuit rider n (1837) : a clergyman assigned to a circuit esp. in a rural
area
cir-cuit-ry \'sər-kə-trē\ n, pl -ries (1946) 1 : the detailed plan or
arrangement of an electric circuit 2 : the components of an electric
circuit
cir-cu-i-ty \(,)sər-'kyü-ə-tē\ n, pl -ities [circuitous] (ca. 1620) : lack of
straightforwardness : INDIRECTION
¹cir-cu-lar \'sər-kyə-lər\ adj [ME circuler, fr. MF, fr. LL circularis, fr.
L circulus circle] (15c) 1 a : having the form of a circle : ROUND b
: moving in or describing a circle or spiral 2 a : of or relating to a
circle or its mathematical properties (a ~ arc) b : having a circular
base or bases (a ~ cylinder) 3 : CIRCUITOUS, INDIRECT 4 : marked by
or moving in a cycle 5 : being or involving reasoning that uses in the
argument or proof a conclusion to be proved or one of its unproved
consequences 6 : intended for circulation — cir-cu-lar-i-ty \,sər-
kyə-'lar-ə-tē\ n — cir-cu-lar-ly \'sər-kyə-lər-lē\ adv — cir-cu-lar-
ness n
²circular n (1789) : a paper (as a leaflet) intended for wide distribution
circular dichroism n (ca. 1961) 1 : the property (as of an optically
active medium) of unequal absorption of right and left plane-polarized
light so that the emergent light is elliptically polarized 2 : a spectro-
scopic technique that makes use of circular dichroism
circular file n (1967) : WASTEBASKET
circular function n (1884) : TRIGONOMETRIC FUNCTION
cir-cu-lar-ise Brit var of CIRCULARIZE
cir-cu-lar-ize \'sər-kyə-lə-,rīz\ vt -ized; -iz-ing (1848) 1 a : to send
circulars to b : to poll by questionnaire 2 : PUBLICIZE — cir-cu-lar-
i-za-tion \,sər-kyə-lər-ə-'zā-shən\ n
circular saw n (1817) : a power saw with a circular cutting blade; also
: the blade itself
cir-cu-late \'sər-kyə-,lāt\ vb -lat-ed; -lat-ing [L circulatus, pp. of cir-
culare, fr. circulus] vi (ca. 1630) 1 : to move in a circle, circuit, or
orbit; esp : to follow a course that returns to the starting point (blood
~s through the body) 2 : to pass from person to person or place to
place: as a : to flow without obstruction b : to become well-known
or widespread (rumors circulated through the town) c : to go from
group to group at a social gathering d : to come into the hands of
readers; specif : to become sold or distributed ~ vt : to cause to circu-
late — cir-cu-lat-able \-,lā-tə-bəl\ adj — cir-cu-la-tive \-,lā-tiv\ adj
— cir-cu-la-tor \-,lā-tər\ n
circulating decimal n (1768) : REPEATING DECIMAL
cir-cu-la-tion \,sər-kyə-'lā-shən\ n (1654) 1 : orderly movement
through a circuit; esp : the movement of blood through the vessels of
the body induced by the pumping action of the heart 2 : FLOW 3 a
: passage or transmission from person to person or place to place; esp
: the interchange of currency (coins in ~) b : the extent of dissemina-
tion: as (1) : the average number of copies of a publication sold over a
given period (2) : the total number of items borrowed from a library
cir-cu-la-to-ry \'sər-kyə-lə-,tōr-ē, -,tȯr-\ adj (1605) : of or relating to
circulation or the circulatory system (~ failure)
circulatory system n (1862) : the system of blood, blood vessels,
lymphatics, and heart concerned with the circulation of the blood and
lymph
circum- prefix [OF or L; OF, fr. L, fr. circum, fr. circus circle — more
at CIRCLE] : around : about (circumpolar)
cir-cum-am-bi-ent \,sər-kə-'mam-bē-ənt\ adj [LL circumambient-,
circumambiens, prp. of circumambire to surround in a circle, fr. L cir-
cum- + ambire to go around — more at AMBIENT] (1633) : being on all
sides : ENCOMPASSING — cir-cum-am-bi-ent-ly adv
cir-cum-am-bu-late \-'am-byə-,lāt\ vt -lat-ed; -lat-ing [LL circumam-
bulatus, pp. of circumambulare, fr. L circum- + ambulare to walk] (ca.
1656) : to circle on foot esp. ritualistically — cir-cum-am-bu-la-tion
\-,am-byə-'lā-shən\ n

\ə\ abut \ᵊ\ kitten, F table \ər\ further \a\ ash \ā\ ace \ä\ mop, mar
\au̇\ out \ch\ chin \e\ bet \ē\ easy \g\ go \i\ hit \ī\ ice \j\ job
\ŋ\ sing \ō\ go \ȯ\ law \ȯi\ boy \th\ thin \t͟h\ the \ü\ loot \u̇\ foot
\y\ yet \zh\ vision \à, k, ⁿ, œ, ue, ue, ʸ\ see Guide to Pronunciation

BEST AVAILABLE COPY

iomy

ion of Wealth

Finance

ries

SECOND EDITION

PRINCIPLES OF CORPORATE FINANCE

Richard Brealey
London Business School

Stewart Myers
Massachusetts Institute of Technology

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

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

7890DOCDOC8987

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.
1. Corporations—Finances. I. Myers, Stewart C.
II. Title. III. Series.
HG4026.B667 1984 658.1'5 83-19585
ISBN 0-07-007383-X

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.

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,

Ex.

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

$$\text{Asset value} \div \frac{160}{(1.12)^4} = 1.4$$

- 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

[21] These tables are grouped with the present value tables at the back of the book.

Real Options

a practitioner's guide

TOM COPELAND
VLADIMIR ANTIKAROV
MONITOR GROUP

FINANCE/INV

Determinir
potential inv
making. A n
of investmen
over the trac
present val
Vladimir An
options will
for investmer
This book
understandin
everyday dec
years of exper
implementin
Copeland
flawed and t
portunities. N
to consider tl
has over the
Such options
project if resu
ing down or
out to be wor
There are ch
types of simpl
ment, expansi
more advance
switching opti
Industrie uses
and discusses t
menting real
write an Excel
combinations
Chapters 9 and
tainties.
The analysis
case solutions.
problems provi
insights into tl
authors also off
in the book, as
to the would-l
www.corpfinor

This book is printed on acid-free paper.

Published by

TEXERE LLC
55 East 52nd Street
New York, NY 10055

Tel: +1 (212) 317 5106
Fax: +1 (212) 317 5178
www.etexere.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.etexere.co.uk

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 be
and hundreds
for a "how to
can take off y
theory to ever
teen years of e
our clients ap
our experience
tool by more c

WHY READ T

The central pa
present value.
values every i
pected future c
illustrate a typ
evaluating an $
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:

$$C_0 = S_0 N(d_1) - Xe^{-r_f T} N(d_2)$$

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 = 2.1728 . . .

$$d_1 = \frac{\ln(S/X) + r_f T}{\sigma\sqrt{T}} + \frac{1}{2\sigma\sqrt{T}}$$

$$d_2 = d_1 - \sigma\sqrt{T}$$

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

$$MAX[0, u^n d^{T-n} V_0 - X]$$

Using the expression for binomial probabilities that was developed earlier, the probability of each payoff is:

$$B(n \mid T, p) = \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n}$$

Multiplying the payoffs by the probabilities and summing across all possible payoffs, we have

$$C_0 = \left\{ \sum_{n=0}^{T} \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} MAX[0,\ u^n d^{T-n} V_0 - X] \right\} \div (1+r_f)^T$$

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:

$$C_0 = \left\{ \sum_{n=a}^{T} \frac{T!}{(T-n)!n!} p^n (1-p)^{T-n} [u^n d^{T-n} V_0 - X] \right\} \div (1+r_f)^T$$

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, $B(n \geq a \mid T, p)$. 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

$$X(1+r_f)^{-T}B\left(n \geq a \mid T, p\right) = 250(1.10)^{-7}(.260668) = \$33.44$$

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

$$p' \equiv \left[\frac{u}{(1+r_f)}\right]p$$

Exhibit 7.6 Seven-period binomial example.

Parameters: $V_0 = \$100$
$u = 1.5$, $d = 1/u = .667$

and

$$1 - p' \equiv \left[\frac{d}{(1+r_f)}\right](1-p)$$

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:

$$C_0 = V_0 B\left(n \geq a \,\middle|\, T, p'\right) - X(1+r_f) B\left(n \geq a \,\middle|\, T, p\right)$$

where

$$p \equiv \frac{(1+r_f) - d}{u - d}$$

$$p' = \left[\frac{u}{1+r_f}\right]p$$

$a \equiv$ *The smallest nonnegative integer greater than* $\ln(X/V_0 d^n)/\ln(u/d)$

$B(n \geq a \mid T, p) =$ *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 $B(n \geq 6 \mid 7, .7091)$ is .6676. Therefore, the value of the option, using a binomial approach for 7 time periods is

$$C_0 = V_0\, B\left(n \geq a \middle| T,\ p'\right) - X(1+r_f)^{-T} B\left(n \geq a \middle| T,\ p\right) = \$100(.6676) - \$250(1.1)^{-7}(.2606)$$
$$= \$66.75 - \$33.44 = \$33.32$$

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:

$$C_0 = V_0 B\left(n \geq a \middle| T, p\right) - X(1+r_f) B\left(n \geq a \middle| T, p'\right)$$

where

$$p = \frac{(1 + r_f - d)}{u - d}$$
$$p' = \frac{u}{1 + r_f} p$$

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

$$\lim_{N \to \infty}\left(1+\frac{j}{n/T}\right)^{n/T} = e^{j} = (1+r_f)$$

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, 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:

$$B(n \geq a \mid T,\ p') \to N(d_1)$$
$$B(n \geq a \mid T,\ p) \to N(d_2)$$

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,

The Black-
rate. The cc

Next we esti
tive normal,

Finally, substi
the value of d

$$u = e^{\sigma\sqrt{T/n}}$$
$$\ln(u) = \sigma\sqrt{\frac{T}{n}} = \sigma\sqrt{7 \div 7}$$
$$\sigma = \ln(u) = \ln(1.5) = .4055$$

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 $N(d_2)$:

$$d_1 = \frac{\ln\left(\frac{V}{X}\right) + r_f T}{\sigma\sqrt{T}} + \frac{1}{2}\sigma\sqrt{T}$$
$$= \frac{\ln\left(\frac{100}{250}\right) + .0953(7)}{.4055\sqrt{7}} + \frac{1}{2}.04055\sqrt{7}$$
$$= \frac{-.9163 + .6672}{.4055(2.646)} + .5(.53638)$$
$$= \frac{-.2491}{1.0728} + .53638 = .3042$$
$$N(d_1) = .5 - .1195 = .6195$$
$$d_2 = d_1 - \sigma\sqrt{T} = -.3042 - .4055\sqrt{7} = -.7686$$
$$N(d_2) = .5 - .27894 = .22106$$

Finally, substituting these values into the Black-Scholes model, we find the value of the option:

$$C_0 = VN(d_1) - Xe^{-r_f T}N(d_2) = 100(.61950) - 250e^{-.0953(7)}(.22106)$$
$$= 61.95 - 250(.5132)(.22106) = 61.95 - 28.36 = 33.59$$

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	

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
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE 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.

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 strucutres 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" (Bernier, 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 backbones 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.

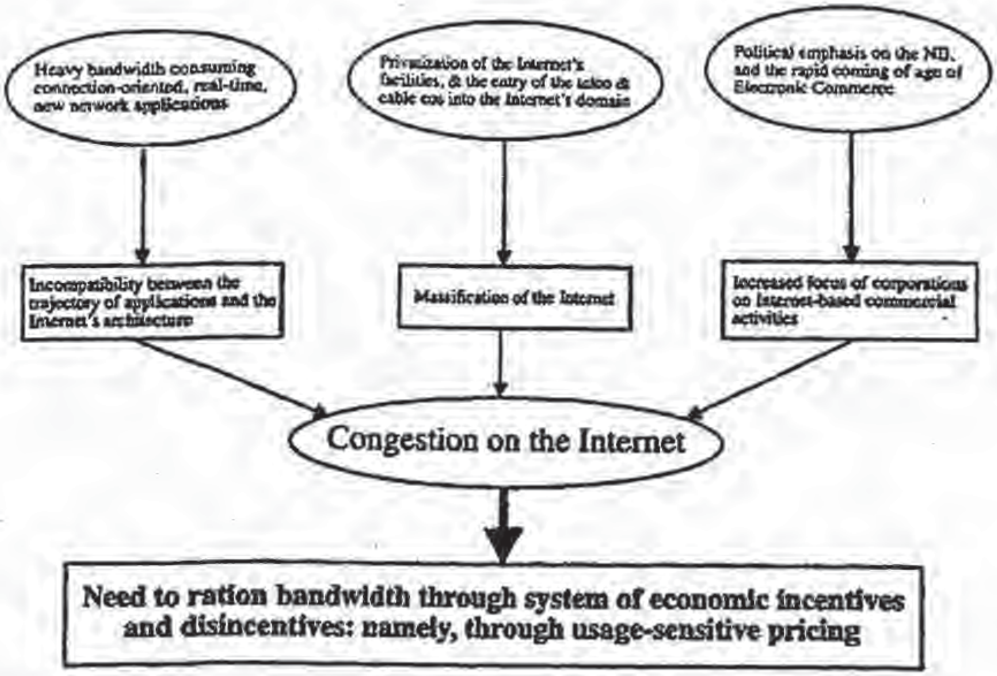


Figure 1

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 CUSeeMe, 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 M arch 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 Rosall, 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 fileserver 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 T 1 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 (Tenney, telecomreg, 4 May 1994, 18:42:09). However, the Internet is not designed to allow most users to fill their lines 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. Bohn et al. have proposed the "Precedence" model, while Varian & MacKie-Mason have developed the "Smart Market" mechanism.

4.4.2.1 The Precedence Model

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.

4.4.2.2 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 of a listserv 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 systemic incentives to conserve on 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 how 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 ftp://ftp.sdsc.edu/pub/sdsc/anr/papers/precedence.ps.Z.

Business Editors. (March 11,1994). Competition, controversy ahead in era of Internet commercialization. Business Wire.

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.ls a.umich.edu.

Campbell, A. (April 4, 1994). Distributed testing: 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. Alleman & 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. (1993). Pricing the Internet. Tech rep., University of Michigan, Department of Economics. Available via Web from http://gopher.econ.ls a.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.ls a.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. Alleman & 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

Mitrabarun 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

(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 Wolff, 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

---

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 act 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.

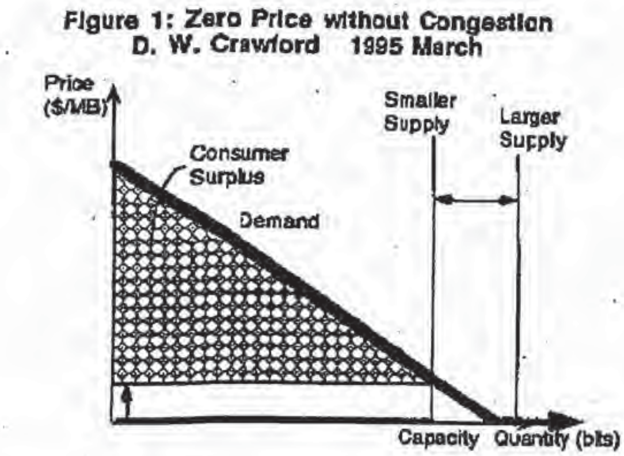


Figure 1.

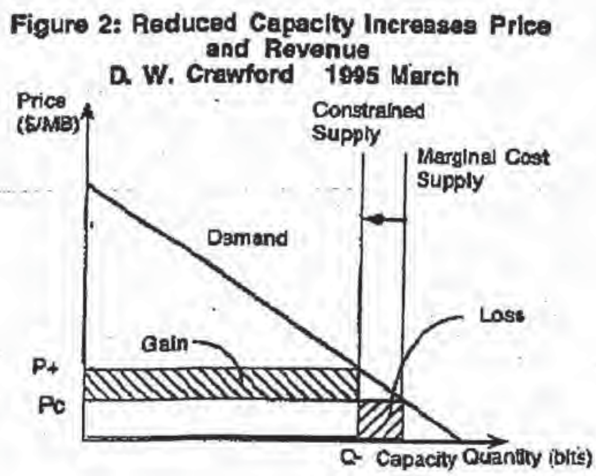


Figure 2.

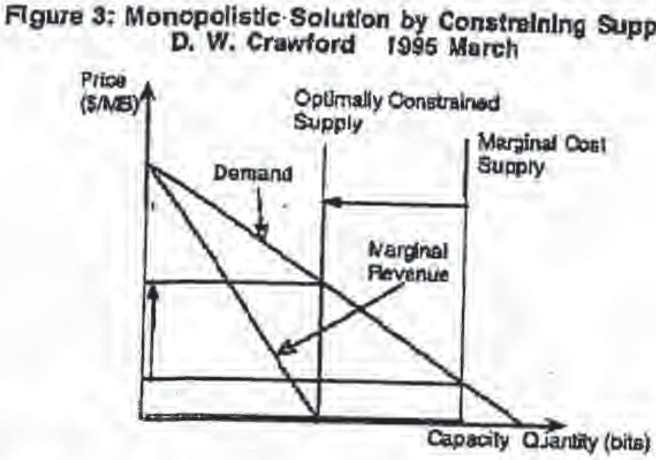


Figure 3.

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.

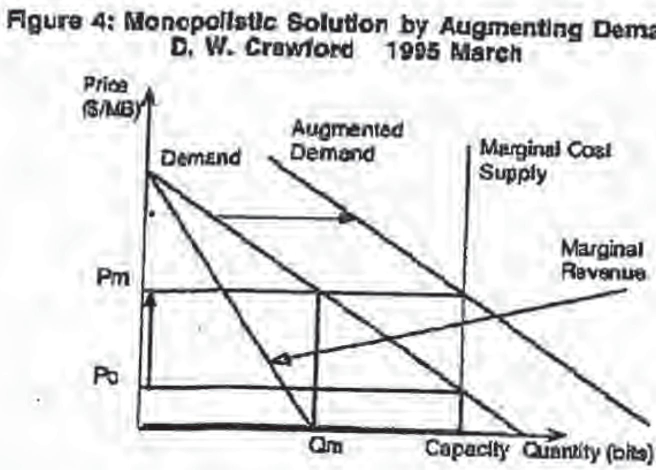


Figure 4.

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 procure 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] Unitizing 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 unitized 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, Pb, and the price the seller receives for the information, Ps, so

$$Pb - Ps = T$$

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 (Pb - P) and the sellers see their price decrease by (P - Ps) upon imposition of a tax T.

Seller incidence IS refers to the portion of the tax paid by the seller:

$$IS = \frac{P - Ps}{T} = \frac{P - Ps}{Pb - Ps}$$

Buyer incidence IB refers to the portion of the tax paid by the buyer:

$$IB = \frac{Pb - P}{T} = \frac{Pb - P}{Pb - Ps}$$

Note that IS + IB = 1 is an identity.

$$IS + IB = \frac{P - Ps}{Pb - Ps} + \frac{Pb - Ps}{Pb - Ps} = \frac{(P - Ps) + (Pb - P)}{Pb - Ps} = \frac{-Ps + Pb}{Pb - Ps} = 1$$

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 or 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 Pt and the seller keeps Ps. 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-liable 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 t1
- output: y = water at node B at time t2
- production function: f(x,t) = y

Note that in the water network example above, both the input and the output are time stamped. If t1< t2 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 2 is a perfect substitute for watching the State of the Union Address delivered on station 3. *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 are 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 < 26 = 64). A modern computer which is using display PostScript with a character set of 220 needs 8 bits per character (220 < 28 = 256). These example 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 unitized 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 to 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., Shenker, 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-Collel, 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

---

Equilibrium Allocation and Pricing of Variable Resources among User-Suppliers (1998) (Correct) (2 citations)

Steven H. Low

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 MI where the nonnegativity constraint on (x n ; 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 Traffics - Steven H. Low (2000) (Correct)
Optimization Flow Control, I: Basic Algorithm and Convergence - Steven Low (1999) (Correct)

Active bibliography (related documents): More All
0.5: 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 - Sanjeewa Athuraliya, Steven.. (2000) (Correct)
0.1: Optimization Flow Control with Newton--Like Algorithm - Sanjeewa Athuraliya 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: Sanjeewa Athuraliya, 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, 34(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 = "34",
    number = "4",
    pages = "207-225",
    year = "1998",
    url = "citeseer.nj.nec.com/low98equilibrium.html"
}
```

Citations made in this document:

Doc Context [1] Dimitri P. Bertsekas. *Necessary and sufficient conditions for existence of an optimal portfolio*. Journal of Economic Theory, 8:235–247, 1974. 19

Doc Context [2] A. K. Choudhury and E. L. Hahne. *Dynamic queue length thresholds for shared– memory packet switches*. IEEE/ACM Transactions on Networking, 6(2):130--140, April 1998.

Doc Context [3] R. Cocchi, 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 to heterogeneous*, regulated traffic in an atm node. IEEE Journal on Selected Area 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. Jarrow. 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 Maulloo, and David Tan. *Rate control for communication networks: Shadow 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.oz.au/staff/slow/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.). Spinger, 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. Labetoulle 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 deisgn 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. Zappla. *RSVP: A new Resource reSerVation Protocol*. IEEE Network, 7(5):8--18, September 1993.

Institut für Technische Informatik und Kommunikationsnetze

Published in the proceedings of 'reliable IT systems' VIS '95, H.H. Brüggemann and W. Gerhardt-Häckl (Ed.), Vieweg Publishing Company, Germany, 1995

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 images[1] 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 **tag**[2] 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[13] 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 unrecoverable[3], 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

[3] 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 4x4 up to 16x16 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

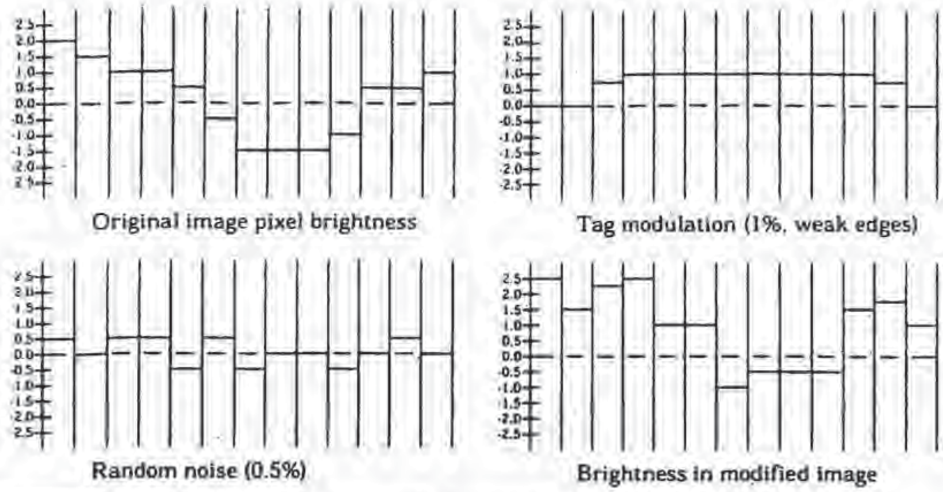


Figure 2: Modulation of an image by tagging information

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 $2n \cdot 2n$ 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 displayed, 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. ±1%Noise
bud (640x480)	690	427	254	156	.9998552	.9998131	.9997896	.9997647	.9988916
zurlim (512x512)	1593	606	282	156	.9999024	.9998786	.9998695	.9998585	.9994244
pic3 (502x900)	614	445	293	204	.9998595	.9998270	.9997997	.9997749	.9988591
ystone (1152x779)	1208	1076	683	453	.9995562	.9994302	.9993338	.9992625	.9964358
lake (512x512)	1530	608	299	175	.9998826	.9998515	.9998394	.9998352	.9993038

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 enemy[4].

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).

Tagged Image A Tagged Image B Difference

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 ($2^N \geq$ 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 ± 2%, respectively ±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 Q75	JPEG Q30	FSQUANT 32
bud	256 col	.9969303	.9879267	.9941969	.9749811	.9900836
zurlim	>99999 col	.9983958	.9935527	.9971826	.9918425	.9949042
pic3	76540 col	.9968435	.9875711	.9984049	.9965283	.9725430
ystone	>99999 col	.9901941	.9624366	.9959695	.9912676	.9583207
lake	>99999 col	.9980696	.9923478	.9971620	.9942864	.9911683

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	63	83	93	100	76	91	94	98
	1,2%	84	98	100	100	70	85	93	99	85	100	100	100	65	86	96	100	72	91	94	99
	1,4%	86	99	100	100	73	90	97	100	89	100	100	100	68	92	99	100	82	96	95	98
zurlim	1,0%	81	98	100	100	68	87	93	97	82	99	100	100	65	83	96	98	75	90	92	94
	1,2%	85	99	100	100	70	89	96	99	86	100	100	100	66	87	98	99	78	93	94	94
	1,4%	88	100	100	100	73	92	99	100	89	100	100	100	69	90	99	100	81	95	95	96
pic3	1,0%	83	98	100	100	69	84	96	98	83	99	99	100	66	85	96	99	68	84	86	92
	1,2%	85	99	100	100	71	86	96	99	84	99	100	100	66	89	96	100	71	84	88	94
	1,4%	88	100	100	100	74	91	99	99	88	100	100	100	69	94	99	100	76	89	94	94
ystone	1,0%	82	97	99	100	68	83	94	98	85	99	100	100	67	89	96	99	72	86	87	90
	1,2%	85	98	100	100	70	86	95	99	85	100	100	100	68	91	98	100	76	88	89	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	68	86	96	99	69	85	88	94
	1,2%	83	99	100	100	69	90	96	100	86	99	100	100	69	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 (`ftp://ftp.cs.princeton.edu/reports/1994/468.ps.Z`), 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.

In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Neuve, Belgium, May 1996

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.fhg.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 makes 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 presented 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.

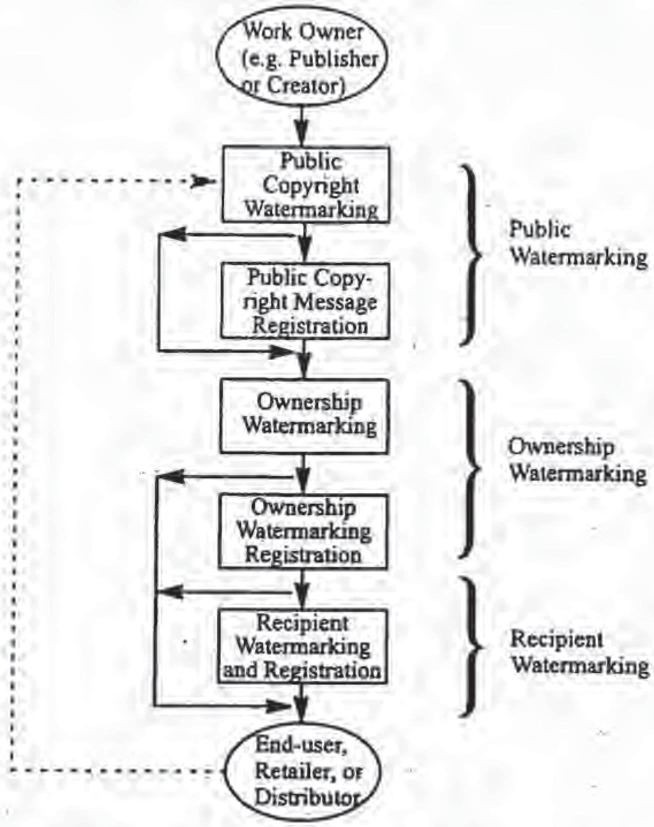


Figure 1. A digital copyright watermarking scheme

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.

In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Neuve, Belgium, May 1996

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 8 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 b 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.

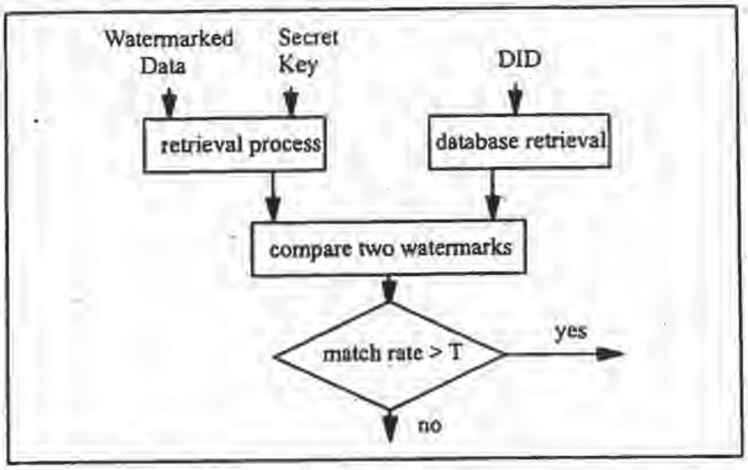


Figure 2. Copyright verification by the Watermarking Server

A watermarking server may also use watermarking time to determine which watermark is "original" if both watermarkings 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 became 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):

http://www.igd.fhg.de/~zhao/building.ppm

The label to be embedded into the image (max. 8 characters):

fhgigda8

Secret key (max. 9 digits):

****

Submit Clear Fields

Figure 3. Image watermark-embedding form

The complete URL of the image (ppm, gif, tiff, jpeg):

http://www.igd.fhg.de/~zhao/building.marked.ppm

Secret key (max. 9 digits):

****

Document identifier (DID):

1003248

Submit Clear Fields

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-1 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.

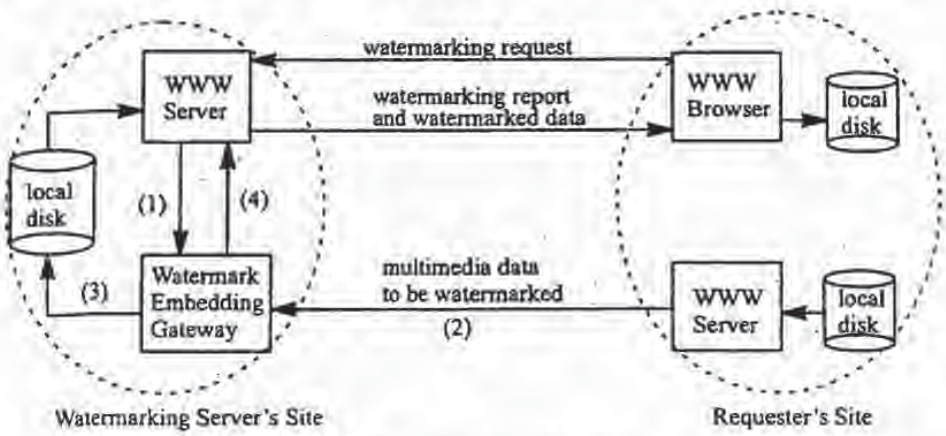


Figure 5. Watermark-embedding process

(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:

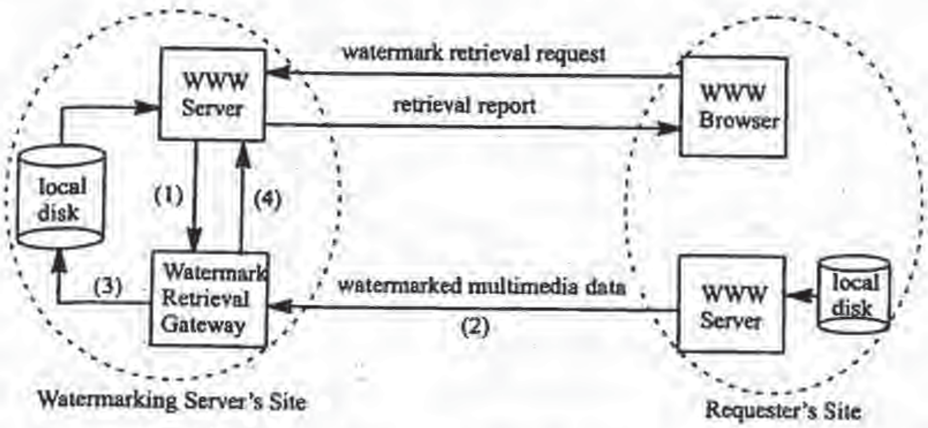


Figure 6. Watermark-retrieval process

(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 preforms 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).
Cryptology 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).

[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] Shttpd.
The Secure NCSA httpd. See http://www.commerce.net/software/Shttpd.

[16] SMosaic.
The Secure NCSA Mosaic. See http://www.commerce.net/software/SMosaic.

[17] TALISMAN. (1996).
Common Funtional 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, J.1, K.4.1, K.5.1, H.4.3

ISSN 0302-9743
ISBN 3-540-61996-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10549111 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Sometime in early 1[...]
research communities do[...]
mostly unaware of each o[...]

Firstly, recent moves [...]
other intellectual proper[...]
digital objects can be es[...]
— embedding hidden co[...]
in the event of a dispute.[...]
pictures or music, and ye[...]
technological challenge.

Secondly, a number o[...]
cations, digital cash, onli[...]
for third parties to trace.[...]
properties of everyday tr[...]
whether technological pro[...]

Thirdly, computer sec[...]
over twenty years about c[...]
shared resource (such as a[...]
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 fiel[...]
various governments' rece[...]
programs have appeared [...]
in a digital picture.

Finally, a number of es[...]
have been developed over[...]
the military. These inclu[...]
use of highly directional r[...]

These areas of study a[...]
the whole topic of inform[...]

A suitable opportunit[...]
curity, Cryptology and C[...]
year at the Isaac Newto[...]
tee was put together, co[...]

r Multimedia Data,
ledia and Electronic
ction for Electronic
1994
Copyright Labelling,
age Processing,Neos
o secretly embed a
oceedings, vol. 1, no.
381-000-8
079061-0
ractals for the Class
pplication, Springer-
sion Using Iterated
ns Center, San Diego
pplication, Chapter1,
sion Using Iterated
ns Center, San Diego
Course Notes
pplication, Chapter1.
pplication, Chapter1,

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 imperceivably 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 perceivably 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 imperceivable artifacts, including

[1] At the Information Hiding Workshop held in Cambridge, England, the adjectives *cover*, *embedded*, and *stego* were choosen 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 stegonagraphic 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 imperceivable 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 imperceivable 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.

2 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 steam. 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 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-objectionably 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 exponentia
impulses.

In this exam
copy the cover a
We let the l
encoding a bina
encode a zero. F
encoded signal (
The delay be
or system functi
with a delay of
delay. In order
smaller portions
bit by consideri
several bits) is t
In Figure 5,
labeled a, b, c,

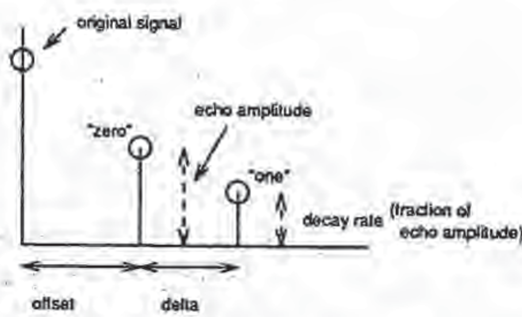


Fig. 1. Adjustable parameters

time exponentials (as depicted in Figure 2) differing only in the delay between impulses.

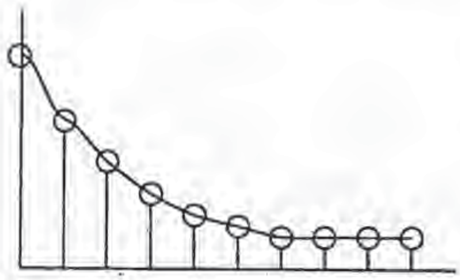


Fig. 2. Discrete time exponential

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

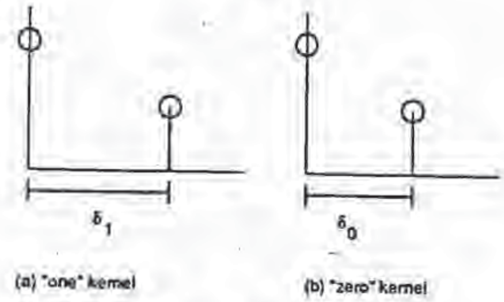


Fig. 3. Echo kernels

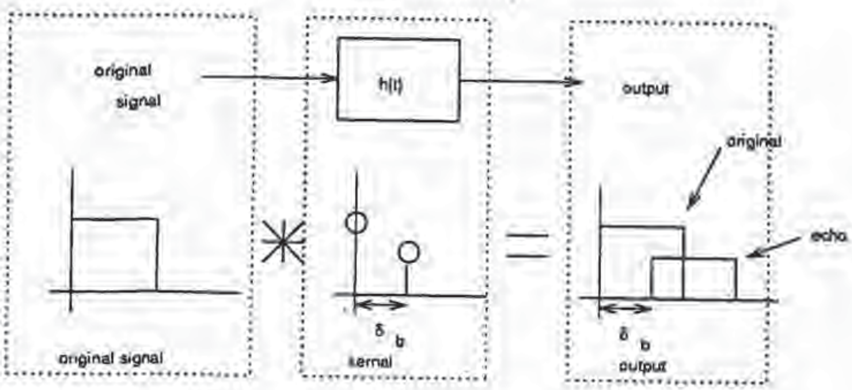


Fig. 4. Echoing example

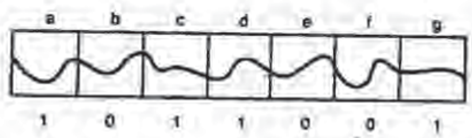
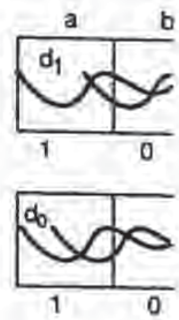


Fig. 5. Divide the cover audio into smaller portions to encode information

one. Therefore, we
each of these porti
system function. T
a similar manner u
been individually
are recombined. W
something slightly
using each of the sy
or all zeroes. The r



In order to com
The mixer signals
hide in that porti
different bits.

The "one" mixe
mixer signal is mu
signals are scaled
number in-betweer
Note that the "zer
and that the trans
sum of the two mi
between portions
the resonance of t
representing the er

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.

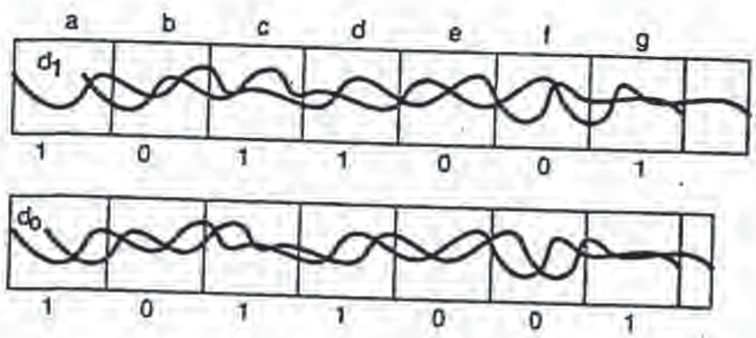


Fig. 6. First step in encoding process

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.

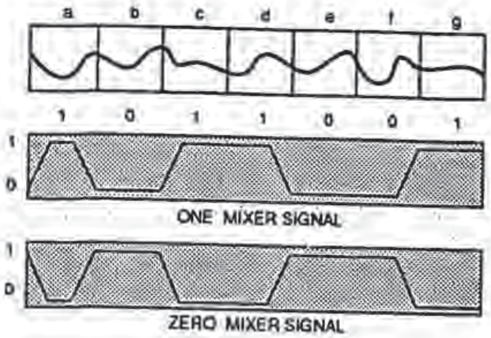


Fig. 7. Mixer Signals

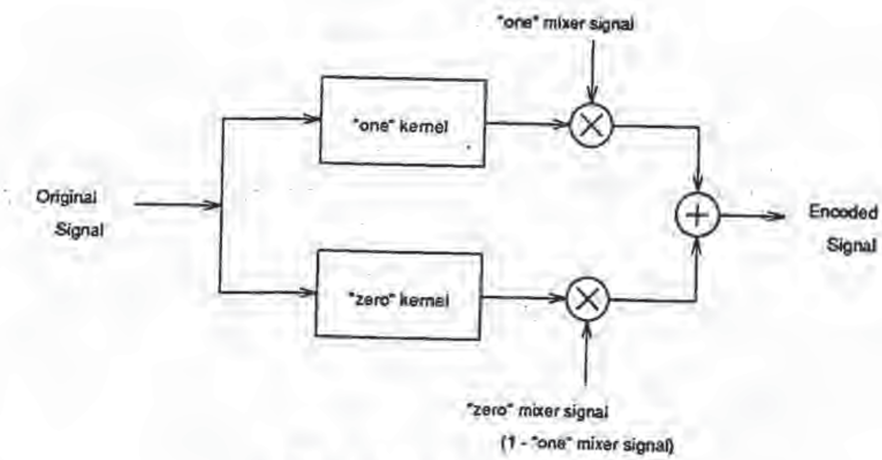


Fig. 8. Encoding process

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 e
elsewhere (Figure 9).

Fig. 9. Exa

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).

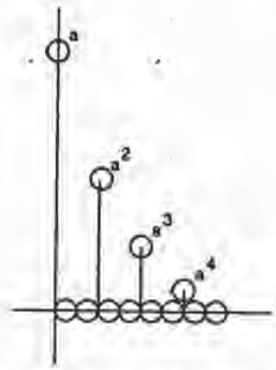


Fig. 9. Example signal: $x[n] = a^n u[n]$; $0 < a > 1$

Encoded
Signal

We echo the signal once with delay δ using the kernel depicted in Figure 10. The result is illustrated in Figure 11.

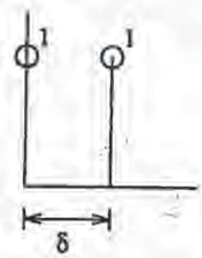


Fig. 10. Echo kernel used in example

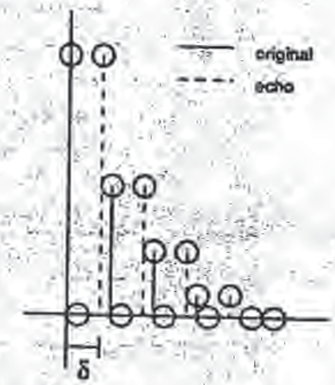


Fig. 11. Echoed version of the example signal

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 bit. As a result, we know that the echoes are in one of two possible locations (with a little periodicity).

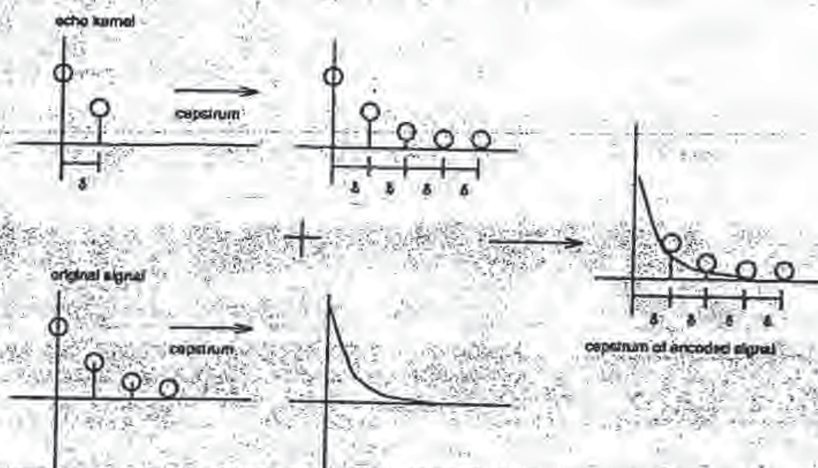
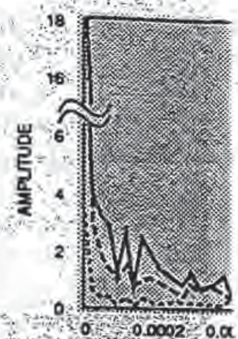
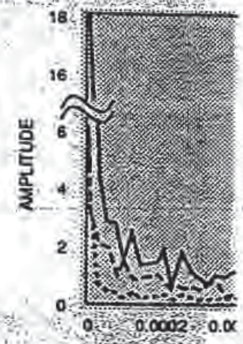


Fig. 12. Cepstrum of the echo-encoded signal

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 mag
relative to the cover a
this problem is to tak





The autocorrelati
With the echoes spac
at either δ_1 or δ_0 in t
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.

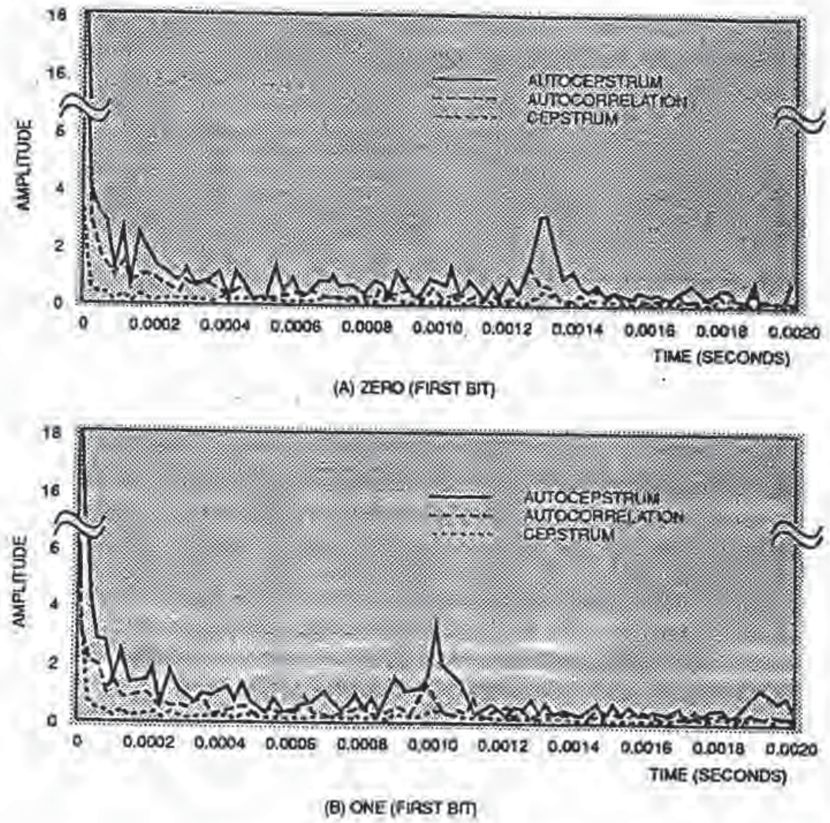


Fig. 13. Result of autocorrelation

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).

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[3] 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.

$$recovery\ rate = \frac{(number\ of\ bits\ correctly\ decoded) * 100}{number\ of\ bits\ placed} \qquad (1)$$

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 0.8. **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.

[3] 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 enc
an analog wire (with
another machine (Fig
0.8. Both **a1** and **a14**
relative volumes, but
approximately the san

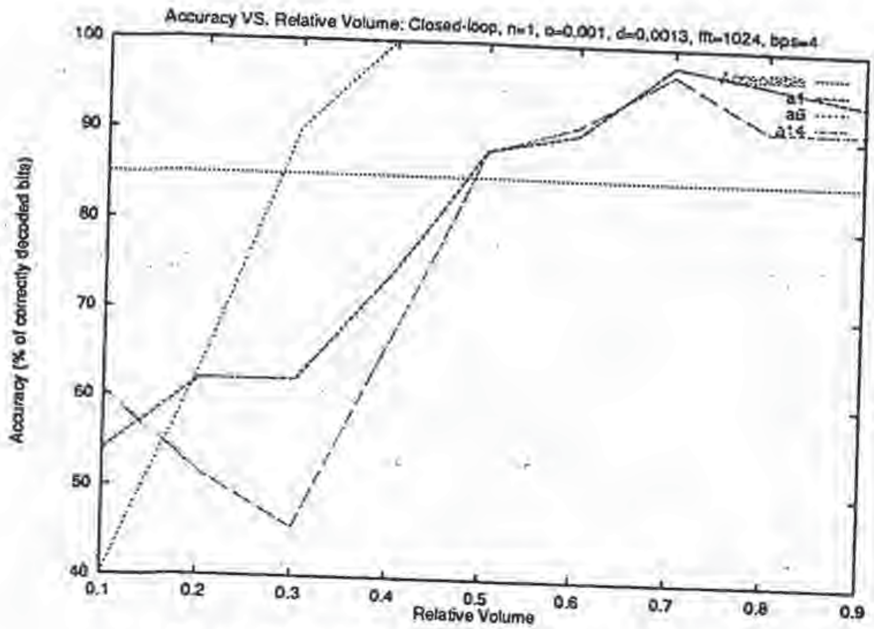


Fig. 14. Accuracy vs. relative volume: closed-loop

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.

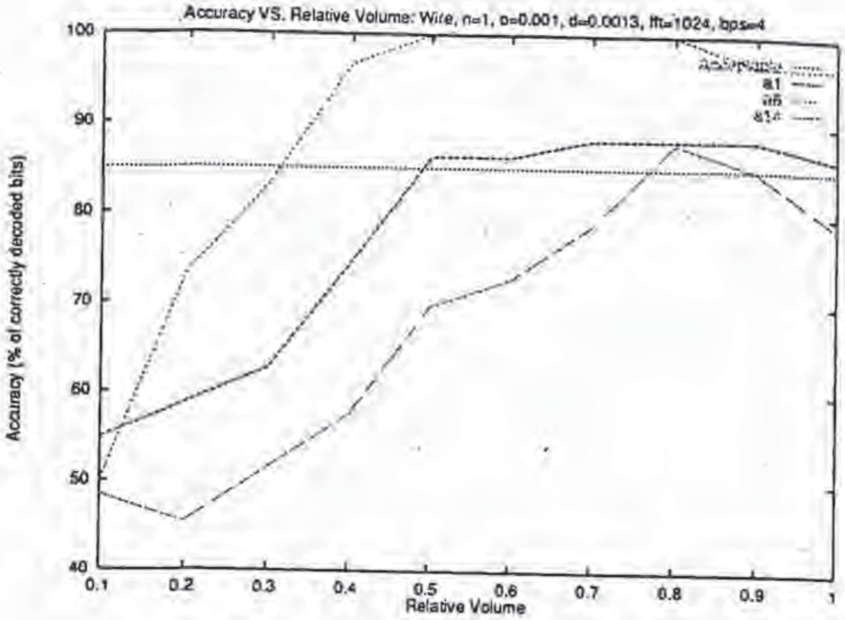


Fig. 15. Accuracy vs. relative volume: Analog wire

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-

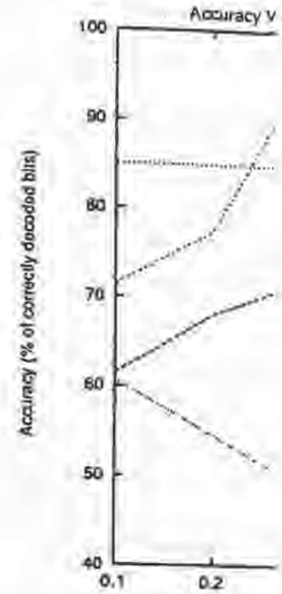


Fig. 16. Accur

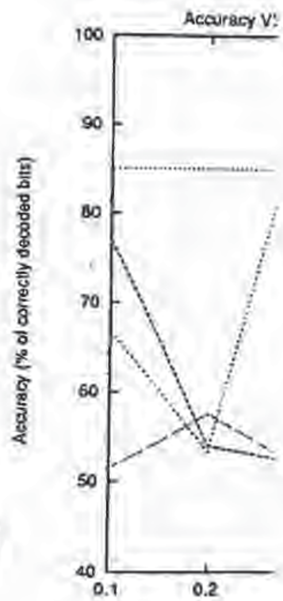


Fig. 17. Accur

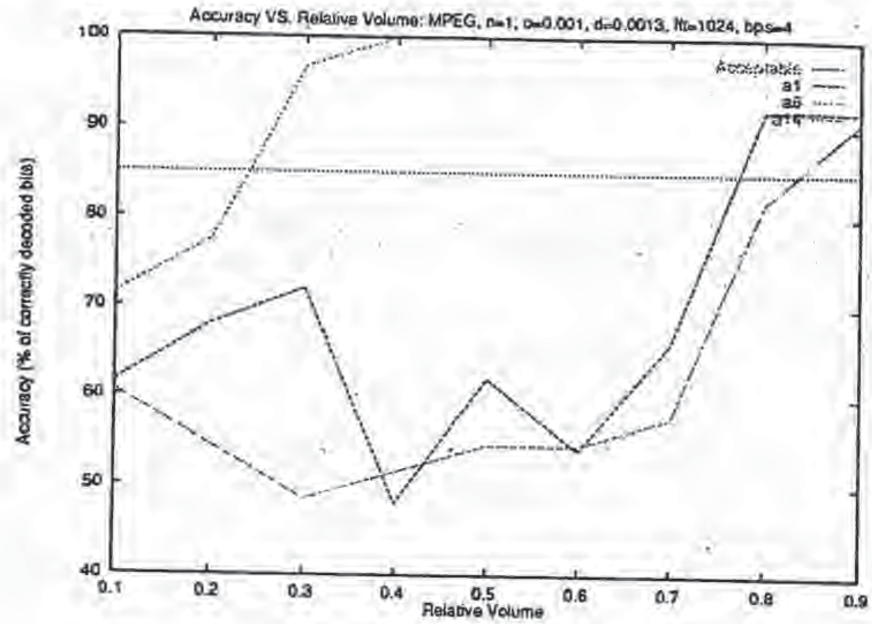


Fig. 16. Accuracy vs. relative volume: analog wire and MPEG

erimented
mpression
mpression
e recovery
ted by the

ed to pro-
ny means,
play a sig-
teractions
n area of
and delta
dio mak-

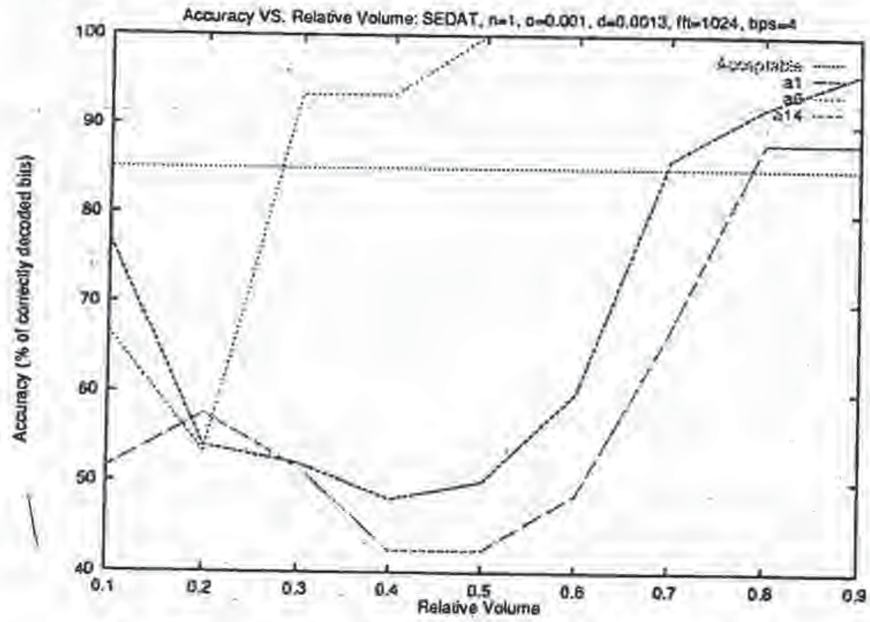


Fig. 17. Accuracy vs. Relative volume: analog wire and SEDAT

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. It's 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 perceivability. 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. Gruhl, N. Morimoto, "Techniques for Data Hiding," Proc. of the SPIE, 2420:40, San Jose, CA., 1995.

2. W. Bender, D. Gruhl, 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. Oppe
Prentice Hall, Inc.,

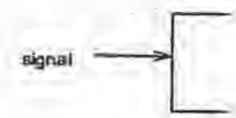
7. Conversatio
Fixture.

Append

Much of the fol
fer's Discrete-Time
complete discussio

A Cepstrum

Cepstral analysis
convolution operat
systems, the cepstr
sisting of a cascad
transform ($\mathcal{F}$), the
transform ($\mathcal{F}^{-1}$) a



Fi

The operationa
The log of a produ
frequency domain i
fact, we use the fi
to place us in the f
quency domain, the
time-invariant (LTI
two functions. This
to using a slide rul
simple addition by

.he echo and the
nilliseconds pro-
esolve the echoes
even the decoder

› parameters are
.rols the recovery
he modifications.
ned at sampling
SEDAT). Other
l yielding similar

is where there is
ersion, line noise
.o many existing
ren in the much

es without gaps
i recover echoes
: are working on
by encoding only
completely.

an audio stream.
a examining the
curacy and echo
ulti-echo kernels
oing in negative
ocess to be self-
ding program to
the user's con-
we will use echo
tion in real time

iding," Proc. of

r Data Hiding,"

ial, pp 391-394,

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.

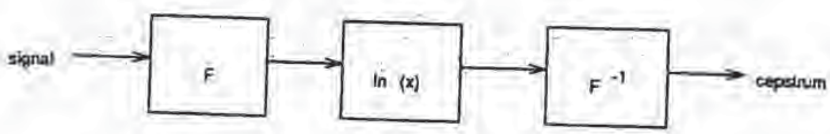


Fig. 18. Canonical representation of a cepstrum

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.

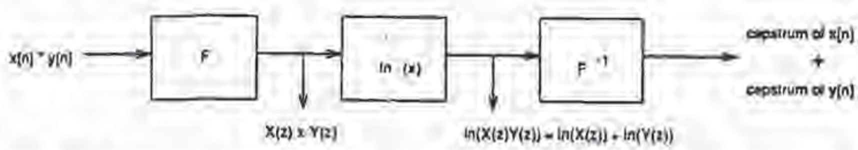


Fig. 19. Conversion of convolution in the time domain to the equivalent cepstral addition while still in the time domain

The inverse cepstrum is the reverse of the process described above and is depicted in Figure 20.

Fig. 20. Inverse cepstrum (canonical representation)

B Autocorrela

Autocorrelation can l
correlation of any fun

With a change of
equation for the auto

Now let's rearran
that:

Recall that convol

There is a similar
the "modified" autoc
negation of time in th
ically speaking, the a

If a signal is self-s
the autocorrelation of

In the frequency d
this becomes:

Using cepstrums,
found by first taking
The steps in this pro
Before we square
wards, we take the in
were finding the ceps
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:

$$R_{xx}[n] = \sum_{m=-\infty}^{+\infty} x[n+m]x[m] \tag{7}$$

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:

$$R_{xx} = \sum x[k]x[k-n] \tag{8}$$

Now let's rearrange the second term in the summation (the x[k-n] term) so that:

$$R_{xx} = \sum x[k]x[-(n-k)] \tag{9}$$

Recall that convolution is defined as:

$$x[n] * h[n] = \sum_{k=-\infty}^{+\infty} x[k]h[n-k] \tag{10}$$

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:

$$R_{xx} = x[n] * x[-n] \tag{11}$$

If a signal is self-symmetric, x[-n] is identical to x[n] by definition. Therefore, the autocorrelation of a self-symmetric signal becomes:

$$R_{xx} = x[n] * x[n] \tag{12}$$

In the frequency domain (i.e. after taking the fourier transform of the inputs), this becomes:

$$S_{xx}(e^{j\Omega}) = (X(e^{j\Omega}))^2 \tag{13}$$

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

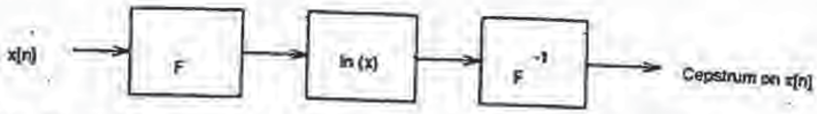


Fig. 21. The first step in finding the Cepstral Autocorrelation is to find the cepstrum of x[n]

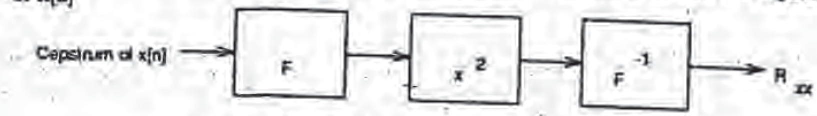


Fig. 22. Once we have the cepstrum, we square it

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.

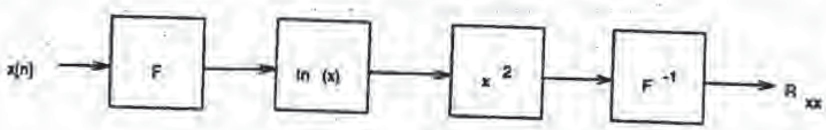


Fig. 23. Systems representation of Cepstral Autocorrelation

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:

$$X(e^{j\Omega}) = |X(e^{j\Omega})|e^{jARGX(e^{j\Omega})} \tag{14}$$

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:

$$e^{j(x+2n\pi)} = e^{jx}e^{j2n\pi} = e^{jx}(\cos 2n\pi + j\sin 2n\pi) = e^{jx} \tag{15}$$

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:

$\log X(e^{j}$

Once again (as in Appen
is identical to the sum of th

$\log X(e^{j\Omega}) =$

Exploiting that log and e

$\log X(e^{j\Omega}$

In order to further motiv
dition, let's mathematically r
arithm. We begin by first co

Convolution becomes mul

$Y($

Taking the complex log:

$\log Y($

Finding the mathematical

$\log Y(e^{j\Omega})$

Now, we can substitute th

$\log Y(e^{j\Omega}) = (\log|X_1(e^{j\Omega})|+\mathrm{lc}$

The use of the complex log
signal components instead of

$$\log X(e^{j\Omega}) = \log(|X(e^{j\Omega})|e^{jARGX(e^{j\Omega})}) \quad (16)$$

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:

$$\log X(e^{j\Omega}) = \log(|X(e^{j\Omega})|) + \log(e^{jARGX(e^{j\Omega})}) \quad (17)$$

Exploiting that log and e^x are inverses, we get:

$$\log X(e^{j\Omega}) = \log|X(e^{j\Omega})| + jARGX(e^{j\Omega}) \quad (18)$$

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:

$$\log Y(e^{j\Omega}) = (\log|X_1(e^{j\Omega})| + \log|X_2(e^{j\Omega})|) + (jARG(X_1(e^{j\Omega})) + jARG(X_2(e^{j\Omega}))) \quad (23)$$

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

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☐ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE 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.

A Variable-Bit-Rate Buried-Data Channel for Compact Disc

3833 (P9.4)

*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

Presented at the 96th Convention 1994 February 26 - March 01 Amsterdam

AES

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 to 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.

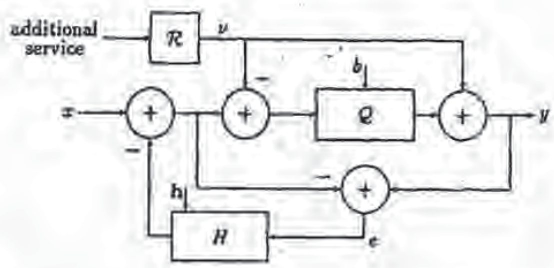


Figure 1: *A subtractively dithered noise-shaped quantizer used as buried-data encoder [1].*

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 ν is produced from the additional service by randomizer $\mathcal{R}$ [1]. The dither signal ν is subtracted before and added[1] after the quantizer. The result of this action is that, under the condition that the dither ν complies with the proper statistical properties [4], the quantizer error signal e is statistically independent of the input signal x. In a subtractively dithered quantizer, ν must have a uniform probability density function (pdf) of width Δ [4]. In this particular case the pdf of ν 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 ν. The decoder can simply recover the dither by extracting the b LSBs from y. Furthermore, the dither ν 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

$$y = x + e, \tag{1}$$

[1]Normally the dither is added prior to quantization. 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

$$Y(\theta) = X(\theta) + (1 - H(\theta))E(\theta). \tag{2}$$

The encoded signal y is thus equal to the sum of the input signal x and a noise signal with psd

$$|1 - H(\theta)|^2 \frac{\Delta^2}{12}. \tag{3}$$

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

$$\int_{-\pi}^{\pi} \log |1 - H(\theta)|^2 d\theta = 0, \tag{4}$$

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.

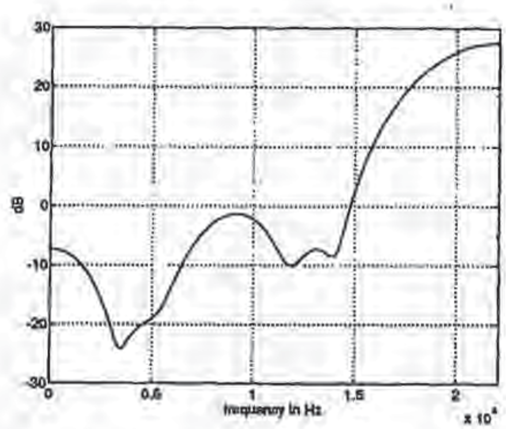


Figure 2: *Psd of a minimum phase filter matching the threshold in quiet.*

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 $2(bits) \times 44.1(kHz) \times 2(channels) = 176.4$ 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

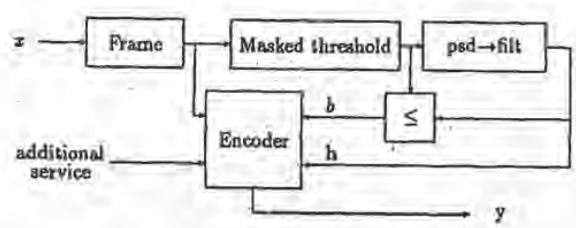


Figure 3: *Algorithm block diagram.*

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

$$\bar{b} = \frac{1}{N}\sum_{i=1}^{N} b_i, \tag{6}$$

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 has q coefficients. We thus have

$$H(\theta) = \sum_{l=1}^{q} h_l e^{-jl\theta}. \tag{7}$$

The filter coefficients h_l 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

$$Q(\mathbf{h}) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{1}{S(\theta)}|F(\theta)|^2 d\theta, \tag{8}$$

by calculation of

$$\frac{\delta Q(\mathbf{h})}{\delta h_l} = 0, \quad l \in \{1, \cdots, q\}. \tag{9}$$

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

$$\frac{1}{S(\theta)} \approx \sum_{k=1}^{m} t_k S_k(\theta). \tag{10}$$

For the windows $S_k(\theta)$ we choose cosine-shape windows

$$S_k(\theta) = \begin{cases} \frac{\pi}{2\Delta_k}(1 + \cos(\frac{\pi}{\Delta_k}(|\theta| - \theta_k)), & \theta_k - \Delta_k \leq |\theta| < \theta_k + \Delta_k \\ 0, & \text{otherwise} \end{cases} \tag{11}$$

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

$$\sum_{l=1}^{q}\sum_{k=1}^{m} t_k \frac{1}{2\pi}\int_{-\pi}^{\pi} S_k(\theta) e^{j\theta(n-l)} d\theta = -\sum_{k=1}^{m} t_k \frac{1}{2\pi}\int_{-\pi}^{\pi} S_k(\theta) e^{j\theta n} d\theta, \quad n \in \{1, \cdots, q\}, \tag{12}$$

and can be reduced to

$$\sum_{l=1}^{q} h_l \rho_{n-l} = -\rho_n, \quad n \in \{1, \cdots, q\}, \tag{13}$$

with

$$\begin{aligned} \rho_n &= \sum_{k=1}^{m} t_k g_{k,n}, \quad n \in \{1, \cdots, q\}, \\ g_{k,n} &= \frac{1}{2\pi}\int_{-\pi}^{\pi} S_k(\theta) e^{j\theta n} d\theta, \quad n \in \{1, \cdots, q\}. \end{aligned} \tag{14}$$

Defining the $q \times q$ matrix $\mathbf{R}$ by

$$r_{i,j} = \rho_{i-j}, \quad i, j \in \{1, \cdots, q\}, \tag{15}$$

and the vector $\mathbf{r}$ of length q by

$$r_i = \rho_i, \quad i \in \{1, \cdots, q\}, \tag{16}$$

we can rewrite (13) into the matrix vector equality

$$\mathbf{R}\mathbf{h} = -\mathbf{r}. \tag{17}$$

The noise-shaping filter coefficients h_l can now be solved from (17) by applying the Levinson-Durbin algorithm [11]. The $g_{k,n}$ 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.

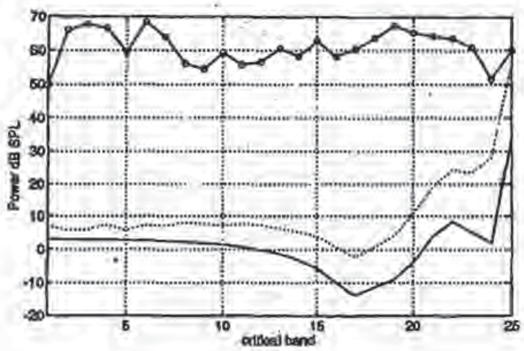
Since the decoder has no a priori knowledge of b_i, the side information must be decodable independently of b_i for every frame. The capacity of the buried-data channel can vary between 2 and a maximum b_{max} bits. Hence a capacity of two LSBs is always available and of this, a fixed portion can be 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 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_i is somewhat arbitrarily set to 8.



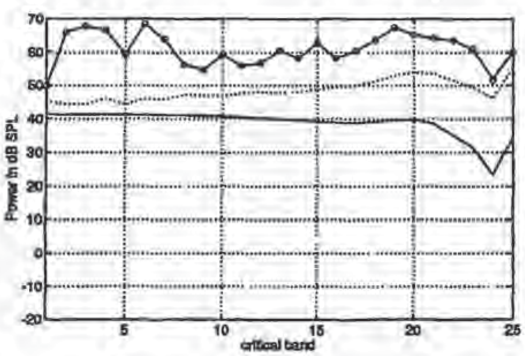


Figure 4: *Fixed noise-shaping filter H with $b_i = 4$ (top graph) and adaptive noise-shaping filter H with $b_i = 8$ (bottom graph). The curve marked with dots is the masked threshold, the solid curve is the psd of $(1 - H)$ and the dotted curve is the +3 dB per octave tilted version of the solid line.*

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.

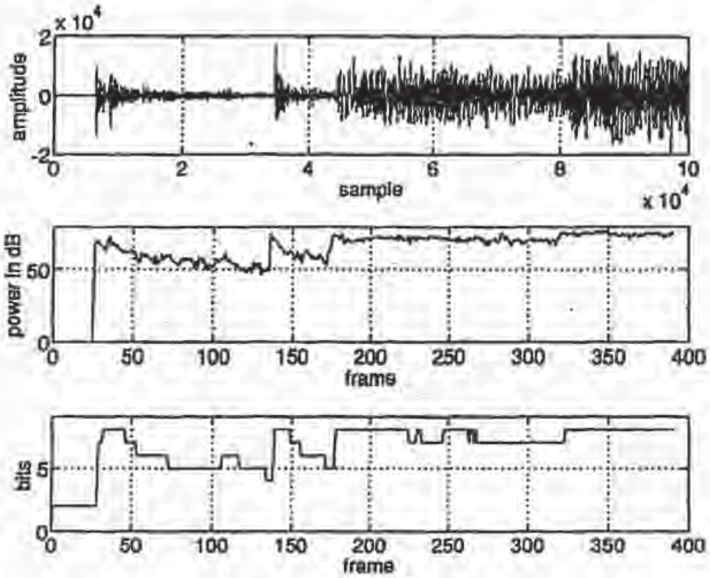


Figure 5: *The upper graph is the time signal of 2.26 sec audio. The lower graph represents the bit rate b_i as a function of the frame number i. For reference the power in blocks of 256-samples is shown in the middle graph. Its correlation with b_i is striking.*

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.F.M. Zijderveld,
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 P. 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 KERKHOF, 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 receiver 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 *RTM*, vol. 35, pp. 10–16 (1991).