

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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;

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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

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

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

means to receive a copy of the content data set;

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

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

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:

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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 securing 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. (previously presented) 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;

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. (previously presented) 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. (previously presented) 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. (previously presented) 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),

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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. (previously presented) 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. (previously presented) 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. (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. (previously presented) 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, 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.

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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 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

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

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

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

REMARKS/ARGUMENTS

The Applicants thank Examiner Avery for the time and consideration in providing the Advisory Action Before the Filing of an Appeal Brief dated July 31, 2007 (Paper No. 200070725). Applicants further appreciate the Examiner's suggestion to file a Request for Continued Examination ("RCE") on or about August 8, 2007. The Advisory Action is quoted here for reference [emphasis added]:

"Continuation of 11. does NOT place the application in condition for allowance because: Though the Applicant provides further explanation with regards to the terminology found within the claim language (e.g., 'legacy content' and predetermined quality level'), said terminology can possess more than one broad interpretation. Although the claims are interpreted in light of the specification, limitations from the specification are not read in the claims. See *in re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Additional language from the Specification inserted into the claim language and/or supplementary language would further elaborating upon said terminology would help further narrow the level of interpretation of said 'legacy content' and 'predetermined quality level'."

Clarification is earnestly sought for the contention that "said terminology can possess more than one broad interpretation". Applicants submit that under MPEP § 2111.01, "...during examination the USPTO must give claims their broadest reasonable interpretation." *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002) (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)) ("In examining a patent claim, the PTO must apply the broadest reasonable meaning to the claim language, taking into account any definitions presented in the specification."). Additionally, cited here for reference:

See MPEP § 2111.01 "While the claims of issued patents are interpreted in light of the specification, prosecution history, prior art and other claims, this is not the mode of claim interpretation to be applied during examination. During examination, the claims must be interpreted as broadly as their terms reasonably allow. *In re American Academy of Science Tech Center*, **>367 F.3d 1359, 1369, 70 USPQ2d 1827, 1834 (Fed. Cir. 2004)< (The USPTO uses a different standard for construing claims than that used by district courts; during examination the USPTO must give claims their broadest reasonable interpretation.)"

For at least the reason that the Advisory Action contends there is *at least one* broad interpretation, there can be no doubt there is support for the claim elements in the application as originally filed.

App'l'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

Second, it is further submitted that Applicants are not "arguing limitations which are not claimed" (please see *In re Van Geuns* as presented at MPEP § 2145 VI & MPEP § 707.07(f) ¶ 7.37.08) as is apparently being asserted by the Office in referencing *In re Van Geuns*:

See MPEP § 2145 VI "VI. ARGUING LIMITATIONS WHICH ARE NOT CLAIMED Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993) (Claims to a superconducting magnet which generates a "uniform magnetic field" were not limited to the degree of magnetic field uniformity required for Nuclear Magnetic Resonance (NMR) imaging. Although the specification disclosed that the claimed magnet may be used in an NMR apparatus, the claims were not so limited.); *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571-72, 7 USPQ2d 1057, 1064-1065 (Fed. Cir.), cert. denied, 488 U.S. 892 (1988) (Various limitations on which appellant relied were not stated in the claims; the specification did not provide evidence indicating these limitations must be read into the claims to give meaning to the disputed terms.); *Ex parte McCullough*, 7 USPQ2d 1889, 1891 (Bd. Pat. App. & Inter. 1987) (Claimed electrode was rejected as obvious despite assertions that electrode functions differently than would be expected when used in nonaqueous battery since "although the demonstrated results may be germane to the patentability of a battery containing appellant's electrode, they are not germane to the patentability of the invention claimed on appeal.")"

In fact, the pending application provides *in haec verba* support for the claims, exemplary embodiments and definitions for the claim terminology. It is also the contention of the Applicants that one of ordinary skill in the art would readily understand the language of the claims as presented. Thus, it is respectfully requested that for at least these reasons the pending rejections be withdrawn.

Third, as described in the MPEP and cited below, Applicants' choice of language is not a proper grounds for rejection. Applicants respectfully note that amendments to the claims were made as expressly suggested by the Office in at least one Interview (e.g., as best understood by the Applicants, suggestion of this nature conforms with MPEP 2173.02, cited below for reference). Applicants respectfully submit the clarification of the claim terminology should not result in prosecution history estoppel. However, it is unclear what standard the Office is applying "to narrow the level of interpretation", as directed by the Advisory Action. Applicants, thus, respectfully direct the Office to the following:

See MPEP § 2173.01 "A fundamental principle contained in 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers.

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

They can define in the claims what they regard as their invention essentially in whatever terms they choose so long as "any special meaning assigned to a term is clearly set forth in the specification. See MPEP § 2111.01. Applicant may use functional language, alternative expressions, negative limitations, or any style of expression or format of claim which makes clear the boundaries of the subject matter for which protection is sought. As noted by the court in *In re Swinehart*, 439 F.2d 210, 160 USPQ 226 (CCPA 1971), a claim may not be rejected solely because of the type of language used to define the subject matter for which patent protection is sought."

&

See MPEP § 2173.02 "The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. When the examiner is satisfied that patentable subject matter is disclosed, and it is apparent to the examiner that the claims are directed to such patentable subject matter, he or she should allow claims which define the patentable subject matter with a reasonable degree of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement."

For the additional reasons outlined in the MPEP above, Applicants respectfully request the Office to reconsider the claims as currently presented and withdraw all outstanding rejections. Applicants respectfully seek clarification in the interests of expediting allowance of the pending claims.

Last, as MPEP § 707.07(j) states: "When, during the examination of a *pro se* application it becomes apparent to the examiner that there is patentable subject matter disclosed in the application, the examiner should draft one or more claims for the applicant and indicate in his or her action that claims would be allowed if incorporated in the application by amendment." Applicants are proceeding *pro se* and request clarification on how the cited claims can be rewritten if the terms "legacy content" and "predetermined quality level" continue to be objectionable.

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

Prior Asserted Rejections under 35 U.S.C. § 102

§ 102 Rejections based on U.S. Patent 5,341,429 ("Stringer")

Claims 1-31 stand rejected as allegedly anticipated by U.S. Patent No. 5,341,429 issued to Stringer et al. (hereafter "Stringer"). See Page 2 of the final Office Action dated May 9, 2007.

Claims 1-31

In order for a reference to anticipate a claim, the reference must disclose each and every feature 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, 1478, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Previously Presented Independent Claim 1 recites [emphasis added]: "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 Stringer fails to disclose or anticipate (1) "legacy content" or (2) "predetermined quality level".

The final Office Action contends that Stringer discloses a conventional local content server ("LCS"), May 9, 2007 final Office Action at Page 2. This contention is respectfully traversed. First, Stringer allegedly teaches a third party that "[t]ransforms the original ephemeral material to its denatured version and wrapper and delivers both to user" (Col. 5 ll. 58-60). Content received by users as taught by Stringer, is identical to that created by the author. Thus, there can be no anticipation that Stringer's alleged LCS could differentiate between users and authors, let alone legacy content and/or content prepared at some time after an LCS was in use. Specifically, Stringer teaches that a third party "convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-57; Col. 12 ll. 4-12; and Col. 12 ll. 40-48). Thus, the alleged authorization process of Stringer is apparently directed at a transaction without

App'l'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

regards to the content's provenance, Stringer thus cannot anticipate an LCS as claimed.

Applicants respectfully direct the Office to Stringer's expressly defined "parties" at Col. 5 ll. 24-67: (1) "Authors: Authors, composers, producers, or creators of original material *who have access to components needed to build original material*" (2) "Third Party: *Transforms original ephemeral material to its denatured version and wrapper and delivers both to user; does not need to be the author*"; and, (3) "User: *Neither a third party, nor an author, uses the trial, evaluation, and enabled versions of the ephemeral material; engages a transaction, either alone or in conjunction with a third party*". Stringer's parties inherently undermine the asserted rejections of the claims, for at least the reason that a user can be an author and a third party. A practical example demonstrates why-- access to the World Wide Web via a conventional PC by a user who may have uploaded user-generated content further demonstrates anecdotal defects in the Stringer reference as asserted art. At the filing date of Stringer, it is not even clear a *prima case* for anticipation can be made for Internet browsers let alone an LCS for handling legacy content or digital watermarks. Applicants respectfully request clarification on how the Office interprets Stringer's express definitions.

Second, Stringer fails to disclose any means to differentiate content *already* owned by users— even newly transacted content received by users under Stringer is of "unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48). As disclosed in the originally filed specification, "it is the user's prerogative to decide how the system will treat non-authenticated content, as well as legacy content". Even, where Stringer allegedly provides identification— it is controlled by *the* third party and made without regards to the content. In fact, it is not possible to differentiate between parties, argued above, as no identifying information is made persistent under Stringer for the express reason that every transacted copy is of "unlimited use and ownership". No matter, identifying information is removed anyway, "To remove the watermark or other material and enable unlimited use of the material, the denatured version of the material is subjected ... to ... any other technique that would serve to erase the watermark from the original material" (Col. 7 ll. 51-57). Thus, the alleged parties of Stringer, whether they can even be identified as authors, third parties or users, can subsequently move content that is expressly disclosed as being identical to the original material – in any manner they choose. This undermines the alleged utility of Stringer relating to an alleged ability to limit access to materials and any *prima facie* case for anticipation based on Stringer of the instant claims.

Third, Applicants respectfully note that the "watermark[s]" of Stringer are *not* the "watermark[s]" of the instant invention[s], including the various types of watermarks described in the specification and claims, for at least the reason that the watermarks claimed herein are *not* removed or erased as expressly described by Stringer. Further, assuming for argument's sake, Stringer's alleged "digital watermark"

App'l'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

is expressly "erased", the result would be an alleged conventional LCS that could not logically act on watermark information. Thus, Stringer does not teach, suggest or anticipate the digital watermarks of the claim[s]. If the Office continues to assert Stringer's "watermarks" as being the watermarks of the claims, Applicants respectfully request clarification on the interpretation being relied upon. Applicants respectfully point to 37 C.F.R. § 1.104 ("In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. ... The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified").

Fourth, by teaching removal of identifying information, Stringer cannot anticipate the LCS of the claims which provides an environment for materials that are essentially identical save the version or status of the data (e.g., *inter alia*, initial, free, legacy, secure, compressed, unsecure, purchased, original, watermarked, signed, hashed, validated, etc.). It logically follows that Stringer fails to anticipate the claim element[s] "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". For these additional reasons, Applicants respectfully request the Section 102 rejections be withdrawn.

Additional significant benefits over Stringer and the art are provided by example and reference to the originally filed specification and are intended to be exemplary not limiting in scope (*please see for example* Pages 11, 12, 15, 16, 23, 24, 26 & 27 of the originally-filed specification):

"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. 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."

Finally, one of ordinary skill in the art can readily appreciate the widespread existence of content in any number of formats— an example, data released prior to a particular protection scheme or without any use restrictions. Thus, the Applicants additionally traverse the assertion that Stringer or the cited art teaches or anticipates the claim feature: "said predetermined quality level having been set for legacy content". For exemplary purposes, in the case of music, though the present invention[s] are not limited to audio, a "predetermined quality level" (i.e., 44.1 kHz 16 bit) is an example of "legacy content". For purposes of argument, this legacy content is arguably *not* of

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

lesser quality than MP3 or AAC—which were introduced after compact discs and are also compressed. And, Windows 95 may have arguably less features than Windows XP. But, Windows 95, being legacy content, is not arguably of lesser quality than Windows XP. The instant invention[s] can handle legacy content and verifiable or secure content seamlessly enabling a more diverse market for information. This is why the Applicants' claims offer significant advantages over Stringer and the cited art.

Because Stringer fails to disclose or anticipate all of the features of the claims, Claims 1, 3, 16, 17, 24 & 31 (and all claims that depend therefrom, respectively) is patentable over Stringer and the cited art. For these additional reasons the Section 102 rejections of Claims 1, 3, 16, 17, 24 & 31 (and all claims depending therefrom, respectively, namely Claims 2, 4-15, 18-23 & 30) based on Stringer should be withdrawn. Applicants respectfully request all outstanding rejections be withdrawn.

Additional Comments

It is respectfully pointed out that the final Office Action relies on Stringer for all asserted rejections applied to the dependent claims. Generally, it appears the Office contends that Stringer:

- (1) "provides a secure system which limits unauthorized access to the materials" (Col. 7 ll. 23-57) for dependent Claims 2, 3, 5, 7, 9, 10, 11, 12 & 13
- (2) "a watermark or copyright notice that is inserted into the original material" (Col. 7 ll. 43-57) for dependent Claims 3, 4, 5, 6, 9, 11, 12, 13, 18, 19, 21, 22, 25, 26, 27, 28, 29 & 30

As argued in connection with Independent Claim 1 it is not clear how these general assertions specifically relate to the claim elements of the dependent claims. For instance, where more than one watermark is claimed, recitation of the same Stringer watermark iteratively applied each claim feature, makes the asserted rejections unclear to the Applicants. As argued above, Stringer fails to teach, suggest or anticipate a means for (1) differentiating between original work and non-original work as applied to the pending claims; (2) differentiating between parties as applied to the pending claims; and (3) inclusion of *persistent* information with content (e.g., a digital watermark, including the various types of digital watermarks presented), the Applicants respectfully request reconsideration and withdrawal of the asserted rejections. Additional comments are presented below in connection with each of the pending claims.

Claim 2 (depending from Claim 1)

Claim 2 stands as allegedly anticipated by Stringer. Dependent Claim 2 includes the claim element, "said SUs ["satellite unit"] capable of receiving and transmitting digital content". The Office Action contends Stringer discloses this

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

additional element, yet the Applicants traverse as Stringer expressly teaches that only authors "... *have access to components needed to build original material*" (Col. 5 ll. 24-25). For the reasons presented with regards to Claim 1 and at least the additional claim element, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 2.

Independent Claim 3 (and all claims depending therefrom, namely Claims 4-15)

Independent Claim 3 includes at least the additional claim element absent in Stringer and the cited art: "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". For the reasons presented with regards to Claim 1 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Independent Claim 3 and the claims depending therefrom, namely Claims 4-15.

Claim 4 (depending from Claim 3)

Claim 4 stands as allegedly anticipated by Stringer. Stringer does not disclose digital watermarks and thus cannot anticipate the additional element, "said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred". As argued previously, Stringer requires removal of his alleged watermark, also argued previously, not extraction to determine whether the content "is authorized for use". For the reasons presented with regards to Claim 1 & Claim 3 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 4. Applicants respectfully request the rejection of Claim 4 (and all claims depending therefrom) be withdrawn.

Claim 5 (depending from Claim 3)

Claim 5 stands as allegedly anticipated by Stringer. Stringer fails to disclose "authentication data is embedded in the content" as claimed for at least the reason that Stringer expressly teaches that only authors "... *have access to components needed to build original material*" (Col. 5 ll. 24-25). A prima facie case for anticipation cannot be made for the additional claim element: "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". For the reasons presented with regards to Claim 1 & Claim 3 and at least the additional claim elements, Applicants

App'l'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

respectfully request the Examiner withdraw the Section 102 rejections for Claim 5. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 5 (and all claims depending therefrom).

Claim 6 (depending from Claim 4)

Claim 6 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "... convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12, and Col. 12 ll. 40-48), as argued previously, it cannot logically be anticipated that Stringer anticipates the following element: "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". For the reasons presented with regards to Claim 1 & Claim 4 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 6. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 6 (and all claims depending therefrom).

Claim 7 (depending from Claim 4)

Claim 7 stands as allegedly anticipated by Stringer. For at least the reason that Stringer expressly teaches that only authors "... have access to components needed to build original material" (Col. 5 ll. 24-25), a prima facie case for anticipation cannot be made for the additional claim element: "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". For the reasons presented with regards to Claim 1 & Claim 4 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 7. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 7 (and all claims depending therefrom).

Claim 8 (depending from Claim 4)

Claim 8 stands as allegedly anticipated by Stringer. For at least the reason that Stringer expressly teaches that only authors "... have access to components needed to build original material" (Col. 5 ll. 24-25), a prima facie case for anticipation cannot be made for the additional claim feature: "further comprising at least one SU, each such SU being capable of communicating with the LCS". For the reasons presented with regards to Claim 1 & Claim 4 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 8. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 8 (and all claims depending therefrom).

Claim 9 (depending from Claim 8)

Claim 9 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks, expressly teaches that only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12, and Col. 12 ll. 40-48); and, expressly teaches that only authors "...have access to components needed to build original material" (Col. 5 ll. 24-25), as argued previously, it cannot logically be anticipated that Stringer anticipates the following features: (1) "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 (2) "means to deliver the watermarked content data set to the SU for its use". For the reasons presented with regards to Claim 1 & Claim 4 & Claim 8 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 9. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 9 (and all claims depending therefrom).

Claim 10 (depending from Claim 8)

Claim 10 stands as allegedly anticipated by Stringer. For at least the reason that Stringer expressly teaches that only authors "...have access to components needed to build original material" (Col. 5 ll. 24-25), a prima facie case for anticipation cannot be made for the additional claim element: "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". Stringer inherently requires a third party to transact further undermining a prima facie case for anticipation based on Stringer. For the reasons presented with regards to Claim 1 & Claim 4 & Claim 8 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 10. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 10 (and all claims depending therefrom).

Claim 11 (depending from Claim 10)

Claim 11 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim feature: "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". For the reasons presented with regards to Claim 1 & Claim 4 & Claim 8 & Claim 10 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 11. For at least these

Appl'n No: 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

reasons, Applicants respectfully request the rejections be withdrawn from Claim 11 (and all claims depending therefrom).

Claim 12 (depending from Claim 8)

Claim 12 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: (1) "means to determine if a robust open watermark is embedded in the content data set"; (2) "to extract the robust open watermark if it is determined that one exists"; and (3) "means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated". For the reasons presented with regards to Claim 1 & Claim 4 & Claim 8 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 12. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 12 (and all claims depending therefrom).

Claim 13 (depending from Claim 4)

Claim 13 stands as allegedly anticipated by Stringer. For at least the reason that Stringer expressly teaches that only authors "... *have access to components needed to build original material*" (Col. 5 ll. 24-25) and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48), a prima facie case for anticipation cannot be made for the additional claim limitation: "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". For the reasons presented with regards to Claim 1 & Claim 4 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 13. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 13 (and all claims depending therefrom).

Claim 14 (depending from Claim 3)

Claim 14 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "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". For the reasons presented with regards to Claim 1 & Claim 3 & Claim 5 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 14. For at least these reasons, Applicants respectfully

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

request the rejections be withdrawn from Claim 14 (and all claims depending therefrom).

Claim 15 (depending from Claim 5)

Claim 15 stands as allegedly anticipated by Stringer. Because Stringer expressly discloses that only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim element: "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". For the reasons presented with regards to Claim 1 & Claim 3 & Claim 5 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 15. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 15 (and all claims depending therefrom).

Independent Claim 16

Independent Claim 16 includes at least the additional claim element absent in Stringer and the cited art: "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. For the reasons presented with regards to Claim 1 and at least the additional claim element, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Independent Claim 16.

Independent Claims 17, 20 & 24 (and all claims pending therefrom, namely Claims 18-19, 21-23, 25-30)

Independent Claim 17 includes at least the additional claim element absent in Stringer and the cited art: (1) "embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated" – (2) "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"; Independent Claim 20 includes at least the additional claim element absent in Stringer and the cited art: "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"; Independent Claim 24 includes at least the additional claim element absent in Stringer and the cited art: (1) "embedding a watermark into

App'l'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS" & (2) "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".

For the reasons presented with regards to Claim 1, at least the additional claim elements, respectively, and the additional reason that the watermark of Stringer and the cited art is not the watermark of the claims, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Independent Claims 17, 20 & 24 and the claims depending therefrom, namely Claims 18-19, 21-23 & 25-29.

Claim 18 (depending from Claim 17)

Claim 18 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user". For the reasons presented with regards to Claim 1 & Claim 17 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 18. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 18 (and all claims depending therefrom).

Claim 19 (depending from Claim 17)

Claim 19 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim features: "embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU". For the reasons presented with regards to Claim 1 & Claim 17 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 19. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 19 (and all claims depending therefrom).

Claim 21 (depending from Claim 20)

Claim 21 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim limitations: "embedding an open watermark into the content data to permit enhanced

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

usage of the content data by the user". For the reasons presented with regards to Claim 1 & Claim 20 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 21. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 21 (and all claims depending therefrom).

Claim 22 (depending from Claim 21)

Claim 22 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "... convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "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". For the reasons presented with regards to Claim 1 & Claim 20 & Claim 21 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 22. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 22 (and all claims depending therefrom).

Claim 23 (depending from Claim 20)

Claim 23 stands as allegedly anticipated by Stringer. For at least the reason that Stringer expressly teaches that only authors "... *have access to components needed to build original material*" (Col. 5 ll. 24-25) and only a third party "... convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48), a prima facie case for anticipation cannot be made for the additional claim limitation: "wherein the content data can be stored at a level of quality which is selected by a user". For the reasons presented with regards to Claim 1 & Claim 20 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 23. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 23 (and all claims depending therefrom).

Claim 25 (depending from Claim 24)

Claim 25 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "... convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "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,

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

said watermark indicating that the copy is authenticated". For the reasons presented with regards to Claim 1 & Claim 24 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 25. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 25 (and all claims depending therefrom).

Claim 26 (depending from Claim 25)

Claim 26 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "wherein the robust watermark is embedded using any one of a plurality of embedding algorithms". For the reasons presented with regards to Claim 1 & Claim 24 & Claim 25 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 26. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 26 (and all claims depending therefrom).

Claim 27 (depending from Claim 26)

Claim 27 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim features: "embedding a watermark which includes a hash value from a one-way hash function generated using the content data". Logically speaking why include a hash in watermark if identifying information is expressly removed under Stringer? For the reasons presented with regards to Claim 1 & Claim 24 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 27. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 27 (and all claims depending therefrom).

Claim 28 (depending from Claim 25)

Claim 28 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] purchased products to unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "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". For the reasons presented with regards to Claim 1 & Claim 24 & Claim 25 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

Claim 28. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 28 (and all claims depending therefrom).

Claim 29 (depending from Claim 24)

Claim 29 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "re-saving the newly watermarked copy to the LCS". For the reasons presented with regards to Claim 1 & Claim 24 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 29. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 29 (and all claims depending therefrom).

Claim 30 (depending from Claim 24)

Claim 30 stands as allegedly anticipated by Stringer. Because Stringer fails to disclose digital watermarks and only a third party "...convert[s] *purchased products to unlimited use and ownership*" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48) a prima facie case for anticipation cannot be made for the additional claim elements: "saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS". For the reasons presented with regards to Claim 1 & Claim 24 and at least the additional claim elements, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Claim 30. For at least these reasons, Applicants respectfully request the rejections be withdrawn from Claim 30 (and all claims depending therefrom).

Independent Claim 31

Independent Claim 31 includes at least the additional claim element absent in Stringer and the cited art: "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". For the reasons presented with regards to Claim 1 and at least the additional claim element, Applicants respectfully request the Examiner withdraw the Section 102 rejections for Independent Claim 31.

Appl'n No. 10/049,101
Request for Continued Examination ("RCE") &
Reply to Advisory Action of July 31, 2007 dated August 9, 2007

Conclusion

Applicants maintain that this application is in condition for allowance, and such disposition is earnestly solicited. Applicants' silence as to the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection. 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: August 9, 2007

By:



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

For Blue Spike, Inc.



Scott A. Moskowitz
President



PTO/SB/21 (04-07)

Approved for use through 09/30/2007. OMB 0551-0031
 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FORM	Application Number	10049,101
	Filing Date	July 23, 2007
	First Named Inventor	Scott A. MOSKOWITZ
	Art Unit	2131
	Examiner Name	Jeremiah L. AVERY
Total Number of Pages in This Submission		Attorney Docket Number
		82488.00111

(to be used for all correspondence after initial filing)

ENCLOSURES <i>(Check all that apply)</i>		
<input checked="" type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input checked="" type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input checked="" type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavit/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below)
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> CD / Number of CD(s) _____	
<input type="checkbox"/> Reply to Missing Parts/Incomplete Application	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	Remarks:	
	REQUEST FOR CONTINUED EXAMINATION ("RCE")	

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name		
Signature		
Printed name	Scott A. MOSKOWITZ	
Date	August 9, 2007	Reg. No.

CERTIFICATE OF TRANSMISSION/MAILING		
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:		
Signature		
Typed or printed name	Scott A. MOSKOWITZ	Date
		August 9, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 192 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form 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-5199 and select option 2.

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Demand Number 10/049101	
APPLICATION AS FILED - PART I					SMALL ENTITY OR OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))						
SEARCH FEE (37 CFR 1.16(a), (b), or (c))						
EXAMINATION FEE (37 CFR 1.16(a), (b), or (c))						
TOTAL CLAIMS (37 CFR 1.100)	minus 20 =	=	X	=	X	=
INDEPENDENT CLAIMS (37 CFR 1.100)	minus 3 =	=	X	=	X	=
APPLICATION SIZE FEE (37 CFR 1.101)	If the specification and drawings exceed 100 sheets of paper, 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(a).					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.101)						
* If the difference in column 1 is less than zero, enter "0" in column 2.						
APPLICATION AS AMENDED - PART II					SMALL ENTITY OR OTHER THAN SMALL ENTITY	
AMENDMENT A	RECE	(Column 1)	(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.100)	31	MINUS	31	=	=
	Independent (37 CFR 1.100)	7	MINUS	7	=	=
	Application Size Fee (37 CFR 1.101)					
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.101)						
TOTAL ADD'L FEE						
AMENDMENT B	(Column 1)	(Column 2)	(Column 3)	(Column 4)	RATE (\$)	ADDITIONAL FEE (\$)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.100)	-	MINUS	**	=	=
	Independent (37 CFR 1.100)	-	MINUS	**	=	=
	Application Size Fee (37 CFR 1.101)					
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.101)						
TOTAL ADD'L 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 4.						

This collection of information is required by 37 CFR 1.16. 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 12 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 proposed 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.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	48	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:19
L2	37	11 and (safe\$ or secur\$ or protect\$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:28
L3	35	12 and (store or storage or storing or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L4	34	13 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:29
L5	26	14 and author\$	US-PGPUB; USPAT	OR	ON	2007/10/23 10:30
L6	2	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 10:34
L7	49	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 14:16
L8	41	17 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:34
L9	41	18 and (authori\$ or allow\$ or permits)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:51
L10	37	19 and (store or storing or storage or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:35
L11	6	(legacy and (legacy with content)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:39
L12	6	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:39
L13	0	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality adj level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:40

EAST Search History

L14	7	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality with level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:41
L15	33	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and quality	US-PGPUB; USPAT	OR	ON	2007/10/23 10:42
L16	26	l15 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:42
L17	26	l16 and (authori\$ or allow\$ or permit\$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:51
L22	23	(legacy with content) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:11
L23	14	l22 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 14:04
L24	3	(legacy near content) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L25	1607	((legacy or old or older) near (version or content)) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L26	513	l25 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L27	510	l26 and (store or storage or storing or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L28	13	l27 and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 14:17
L29	6	l28 and authori\$	US-PGPUB; USPAT	OR	ON	2007/10/23 14:18
L30	1	(legacy adj (content or version)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:21
L31	26	(legacy adj (content or version)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and quality	US-PGPUB; USPAT	OR	ON	2007/10/23 15:01

EAST Search History

L32	1367	((quality near resolution) or (hierarch\$ near quality)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/10/23 15:02
L33	680	l32 and filter\$	US-PGPUB; USPAT	OR	ON	2007/10/23 15:02
L34	18	l33 and (store or storing or storage or database) and server and authori\$	US-PGPUB; USPAT	OR	ON	2007/10/23 15:03
S1	69	watermark\$ and ((second near watermark\$) and (third near watermark\$))	US-PGPUB; USPAT	OR	ON	2006/10/03 09:14
S2	11	S1 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/08/28 12:12
S3	0	S2 and server	US-PGPUB; USPAT	OR	ON	2006/10/03 09:15
S4	7	S2 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:17
S5	0	S4 and legacy	US-PGPUB; USPAT	OR	ON	2006/10/03 09:16
S6	470	watermark\$ and (second near watermark)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:17
S7	80	S6 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S8	25	S7 and server	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S9	24	S8 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S10	22	S9 and (low\$5 or degrad\$)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S11	0	S10 and (add?in)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S12	19	S10 and remote	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S13	19	S12 and address	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S14	19	S12 and address\$	US-PGPUB; USPAT	OR	ON	2006/10/03 09:20
S15	19	S14 and stor\$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S16	19	S15 and domain	US-PGPUB; USPAT	OR	ON	2006/10/03 09:22
S17	3	S16 and legacy	US-PGPUB; USPAT	OR	ON	2006/10/03 09:20

EAST Search History

S18	17	S16 and authenticat\$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S19	17	S16 and authentic\$	US-PGPUB; USPAT	OR	ON	2006/10/03 09:34
S20	153	baum.xa.	US-PGPUB; USPAT	OR	ON	2006/10/03 09:34
S21	61	S20 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:35
S22	12	S21 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S23	10	("5195135" "5715316" "5805700" "5845088" "5898779" "5953506" "6026164" "6216228" "6449718" "6557102").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/10/03 09:35
S24	74	watermark\$ and ((second near watermark\$) and (third near watermark\$))	US-PGPUB; USPAT	OR	ON	2007/01/03 09:29
S25	0	S24 and (try near buy)	US-PGPUB; USPAT	OR	ON	2007/01/03 09:31
S26	162	(try near buy)	US-PGPUB; USPAT	OR	ON	2007/01/03 09:31
S27	50	S26 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S28	23	S27 and authori\$	US-PGPUB; USPAT	OR	ON	2007/01/03 09:33
S29	2	S28 and watermark	US-PGPUB; USPAT	OR	ON	2007/01/03 09:46
S30	710	colvin.in.	US-PGPUB; USPAT	OR	ON	2007/01/03 09:46
S31	13	S30 and revak.xa.	US-PGPUB; USPAT	OR	ON	2007/01/03 09:47
S32	170	(try near buy)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S33	50	S32 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S34	171	baum.xa.	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S35	64	S34 and quality	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S36	12	S35 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S37	524	watermark\$ and (second near watermark)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S38	84	S37 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20

EAST Search History

S39	27	S38 and server	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S40	26	S39 and quality	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S41	24	S40 and ((low\$5 or degrad\$)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S42	20	S41 and remote	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S43	20	S42 and address\$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S44	20	S43 and stor\$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S45	20	S43 and stor\$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S46	20	S45 and domain	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S47	18	S46 and authenticat\$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:22
S48	0	S47 and ((try near buy)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:22
S49	0	S47 and ((try near buy) or demo)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:23
S50	16	S47 and temp\$5	US-PGPUB; USPAT	OR	ON	2007/04/26 19:23
S52	2933	((legacy or early or earlier or previous\$) near (content or data)) and (@ad<"19990804" @prad<"19990804") and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 14:57
S53	1513	S52 and (secur\$ or safe\$2)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:15
S54	1788	S52 and (secur\$ or safe\$2 or protect\$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:16
S55	929	S54 and (authori\$ or authenticat\$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:17
S56	28	S55 and (quality near level)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:17
S57	31	S55 and ((quality or condition\$) near level)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:22
S58	3	S57 and watermark and identi\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:18

EAST Search History

S59	5	((legacy or early or earlier or previous\$) near (content or data)) and moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:24
S60	0	scott-moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:24
S61	616	moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:25
S62	1	moskowitz-scott.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:25
S63	576	S54 and domain	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S64	26	S63 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S65	23	S64 and (author\$ or authentic\$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S66	88	((((legacy or early or earlier or previous\$) near (content or data)) and server and (transmi\$ or send\$) and (data or information or info) and (authori\$ or authentic\$)).clm;	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:33
S67	7	S66 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:33
S68	2972	((legacy or early or earlier or previous\$) near (content or data or multimedia)) and (@ad<"19990804" @prad<"19990804") and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:40
S69	1251	S68 and (quality or degrad\$6)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:41
S70	31	S69 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:41
S71	195640	(quality) and (audio or video or multimedia or media) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:10
S72	4057	S71 and (qps or (quality near service))	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:01

EAST Search History

S73	46	S72 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:01
S74	1181	S71 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:04
S75	17	S74 and legacy	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:04
S76	37328	(quality) and (geograph\$ or map or maps or mapping) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:10
S77	645	S76 and watermark\$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:11
S78	16	S77 and legacy	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:12
S79	16	S78 and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:12



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 10/29/2007			
Scott A. Moskowitz #2505 16711 Collins Avenue Miami, FL 33160			EXAMINER AVERY, JEREMIAH L.	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 10/29/2007	DELIVERY MODE PAPER

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

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/049,101	MOSKOWITZ, SCOTT A.	
	Examiner	Art Unit	
	Jeremiah Avery	2131	

- The MAILING DATE of this communication appears on the cover sheet with the correspondence address -
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 09 August 2007.
- 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) 1-31 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) 1-31 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 08 February 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) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other _____ |

DETAILED ACTION

1. Claims 1-31 have been examined.
2. Responses to Applicant's remarks have been given.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/09/07 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 3 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 3 cite, inter alia, "said SECD capable of storing a plurality of data sets", "capable of receiving a request..." and "capable of transmitting...". Claim 1 further cites "the LCS may be stored and retrieved". Claim 3 further cites, "e or more Satellite Unites (SU) which may be connected to the system through the interface"

Claim 16 cites "can be authorized..." and "can be programmed...".

It has been held that the recitation that an element is "capable of" performing a function is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in any patentable sense. Please see *In re Hutchison*, 69 USPQ 138.

Further, claim 16 uses the language "such that the data contains no additional information to permit authentication", the language "such that" is improper. Appropriate correction is required.

Claim Rejections - 35 USC § 102

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 -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 16 is rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 5,341,429 to Stringer et al., hereinafter Stringer.

3. Regarding claim 16, Stringer discloses a system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD) (column 3, lines 25-30, "floppy diskette copy protection", column 4, lines 49-57, column 5, lines 35-40 and 53-60, column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 13-59);

a Local Content Server (LCS) (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system");

a communications network interconnecting the SECD to the LCS (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);
a Satellite Unit (SU) capable of interfacing with the LCS (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);
said SECD comprising:

a storage device for storing a plurality of data sets (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system and column 10, lines 53-59);

an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets (column 4, lines 33-57, column 7, lines 22-33, column 10, lines 60-68, column 11, lines 1-25 and column 12, lines 4-12 and 40-59);

a transaction processor for validating the request to purchase and for processing payment for the request (column 4, lines 33-57, column 7, lines 22-33, column 10, lines 60-68, column 11, lines 1-25 and column 12, lines 4-12 and 40-59);

a security module for encrypting or otherwise securing the selected at least one data set (column 2, lines 65-68, column 3, lines 1-5, column 5, lines 26-32, column 6, lines 4-11 and 17-33, column 9, lines 14-24 and 43-52 and column 11, lines 33-37);

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 (column 5, lines 26-32, column 6, lines 4-11 and 17-33, column 9, lines 14-24 and 43-52 and column 11, lines 33-37);

said LCS comprising:

a domain processor (column 10, lines 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)");

a first interface for connecting to a communications network (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);

a second interface for communicating with the SU (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);

a memory device for storing a plurality of data sets (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system");

a programmable address module which can be programmed with an identification code uniquely associated with the LCS (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52);

said SU being a portable medium 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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 53-68, "If the code fails the verification step, the process is halted (21) and additional use of the product is disabled" and column 10, lines 1-20 and 43-52, "When the software application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation");
an interface for communicating with the LCS (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68, column 11, lines 1-9, column 12, lines 4-63);
a programmable address module which can be programmed with an identification code uniquely associated with the SU (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52).

Claim Rejections - 35 USC § 103

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 negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-15 and 17-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,341,429 to Stringer et al., hereinafter Stringer and further in view of United States Patent No. 6,148,333 to Guedalia et al., hereinafter Guedalia.

Stringer substantially discloses the claimed invention, however fails to disclose the limitations pertaining to "accepting the digital content at a predetermined quality level". Guedalia discloses this limitation as cited below.

4. Regarding claim 1, Stringer and Guedalia disclose a local content server (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 (column 3, lines 25-30, "floppy diskette copy protection", column 4, lines 49-57, column 5, lines 35-40 and 53-60, column 9, lines 53-63, "transaction

code is given to a vendor sales representative at a remote location" and column 12 (lines 13-59);

b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved (column 5, lines 35-40 and column 8, lines 39-44);

c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS (column 3, lines 55-61, "Time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48, column 6, lines 4-11, column 8, lines 39-44 and 63-68, column 9, lines 1-13, column 10, lines 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)" and column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use");

d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52); 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 (*Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the

authorizallon status of the user", column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy" ... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

5. Regarding claim 2, Stringer discloses 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 (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);

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 (column 4, lines 33-57, column 7, lines 22-33, "provides a secure system which limits unauthorized access to the materials" and column 9, lines 43-67).

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 (column 4, lines 33-57, column 7, lines 22-33, "provides a secure system which limits unauthorized access to the materials" and column 9, lines 43-67).

6. Regarding claim 3, Stringer and Guedalia disclose 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 (column 3, lines 25-30, "floppy diskette copy protection", column 4, lines 49-57, column 5, lines 35-40 and 53-60, column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);

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 (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9);

- c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved (column 5, lines 35-40 and column 8, lines 39-44);
- 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 (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48, column 6, lines 4-11, column 8, lines 39-44 and 63-68, column 9, lines 1-13, column 10, lines 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)" and column 11, lines 1-9; "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use");
- e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52); 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 (*Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user", column 8, lines 15-33;

column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy"... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

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 (*Guadala* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user"; column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy"... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve

the requested image data, since the resolution level requested is higher than that to which the user is entitled").

7. Regarding claim 4, Stringer discloses wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52).

8. Regarding claim 5, Stringer discloses wherein said domain processor comprises: means for obtaining identification code from an SU connected to the LCS's interface (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52);

an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

means for analyzing digital content received from an SU (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

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 (column 6,

lines 61-66, "verifying an enable code", column 9, lines 53-68 and column 10, lines 1-20),

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 (column 6, lines 61-66, "verifying an enable code", column 9, lines 53-68, "If the code fails the verification step, the process is halted (21) and additional use of the product is disabled" and column 10, lines 1-20 and 43-52, "When the software application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation").

9. Regarding claim 6, Stringer discloses 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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material").

10. Regarding claim 7, Stringer and Guedalia disclose 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 (*Stringer* – column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48 and 61-64, column 6, lines 4-11, column 7, lines 22-57, "provides a secure system which limits unauthorized access to

the materials", column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system" and lines 63-68, column 9, lines 1-13, column 10, lines 43-52 and 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)", column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use" and column 13, lines 10-58, "denatured audio that is of adequate quality for evaluation purposes, but not for regular listening" and "VCA drops the amplitude of the source audio signal by 20 dB for a series of 20 millisecond intervals" and *Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user", column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy" ... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

11 Regarding claim 8, Stringer discloses at least one SU, each SU being capable of communicating with the LCS (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a

vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9).

12. Regarding claim 9, Stringer discloses 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 (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

means to retrieve a copy of the requested content data set (column 4, lines 33-57, "remote transactions for delivery of the materials", column 7, lines 6-21,

column 9, lines 43-68, column 10, lines 1-8 and 53-68, column 11, lines 1-32 and column 13, lines 10-35);

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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

means to deliver the watermarked content data set to the SU for its use (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material").

13. Regarding claim 10, Stringer discloses 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 (column 4, lines 33-57, "remote transactions for delivery of the materials", column 7, lines 6-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68, column 10, lines 1-8 and 53-68, column 11, lines 1-32 and column 13, lines 10-35).

14. Regarding claim 11, Stringer discloses 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 (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system");

wherein the SECD comprises:

means to retrieve a copy of the requested content data set (column 4, lines 33-57, "remote transactions for delivery of the materials", column 7, lines 6-21, column 9, lines 43-68, column 10, lines 1-8 and 53-68, column 11, lines 1-32 and column 13, lines 10-35);

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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

means to deliver the watermarked content data set to the LCS for its use (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

means to receive a copy of the requested content data set as transmitted by the SECD (column 4, lines 33-57, "remote transactions for delivery of the materials", column 7, lines 6-21, column 9, lines 43-68, column 10, lines 1-8 and 53-68, column 11, lines 1-32 and column 13, lines 10-35);

means to extract at least one robust open watermark to confirm that the content data is authorized for use by the LCS (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 53-68 and column 10, lines 1-20);

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

means to deliver the watermarked content data set to the SU for its use (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material").

15. Regarding claim 12, Stringer discloses 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 (column 4, lines 33-57, column 7, lines 22-33, "provides a secure system which limits unauthorized access to the materials" and column 9, lines 43-67);

means to receive a copy of the content data set (column 4, lines 33-57, "remote transactions for delivery of the materials", column 7, lines 6-21, column 9, lines 43-68, column 10, lines 1-8 and 53-68, column 11, lines 1-32 and column 13, lines 10-35);

means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if it is determined that one exists (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

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 (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48 and 61-64, column 6, lines 4-11 and 61-66, "verifying an enable code", column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials" and "a watermark or copyright notice that is inserted into the original material", column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system" and lines 63-68, column 9, lines 1-13 and 53-68 and column 10, lines 1-20, 43-52

and 60-68, "lets customers work with the software on a 'trial' basis (e.g. up to ten times)"),

16. Regarding claim 13, Stringer discloses 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 (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48 and 61-64, column 6, lines 4-11 and 61-66, "verifying an enable code", column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials" and "a watermark or copyright notice that is inserted into the original material", column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system" and lines 63-68, column 9, lines 1-13 and 53-68 and column 10, lines 1-20, 43-52 and 60-68, "lets customers work with the software on a 'trial' basis (e.g. up to ten times)").

17. Regarding claim 14, Stringer discloses 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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");
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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material");

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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material").

18. Regarding claim 15, Stringer discloses 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 (column 2, lines 65-68, column 3, lines 1-5, column 5, lines 26-32, column 6, lines 4-11 and 17-33, column 9, lines 14-24 and 43-52 and column 11, lines 33-37).

19. Regarding claim 17, Stringer and Guedalia teach 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 (column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);
retrieving a copy of the requested content data set (column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);
embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

transmitting the watermarked content data set into a Local Content Server (LCS) of the user (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

extracting at least one watermark from the transmitted watermarked content data set (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

permitting use of the content data set if the LCS determines that use is authorized (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials" and column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use");

permitting use of the content data set at a predetermined quality level, said predetermined quality level has been set for legacy content if the LCS determines that use is not authorized (*Guedalia* – column 7, lines 37-53, “controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user”, column 8, lines 15-33, column 11, lines 21-57, “if a user is not authenticated, then unit 250 applies the default policy”... “Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image” and “if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display”, column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, “the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled”).

20. Regarding claim 18, Stringer teaches 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 (column 6, lines 61-66, “verifying an enable code”, column 7, lines 43-57, “a watermark or copyright notice that is inserted into the original material”, column 9, lines 43-68 and column 10, lines 1-20);

permitting the storage of the content data set in a storage unit for the LCS (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system").

21. Regarding claim 19, Stringer teaches connecting a Satellite Unit (SU) to an LCS, 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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU (column 6, lines 61-66, "verifying an enable code", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

delivering the content data set to the SU for its use (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9).

22. Regarding claim 20, Stringer and Guedalia teach a method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to a local content server (LCS) (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9), 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 (column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);

analyzing the message to confirm that the SU is authorized to use the LCS (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

retrieving a copy of the requested content data set (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48, column 6, lines 4-11, column 8, lines 39-44 and 63-68, column 9, lines 1-13, column 10, lines 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)" and column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use");

assessing whether a secured connection exists between the LCS and the SU (column 6, lines 61-66, "verifying an enable code", column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 53-68, "If the code fails the verification step, the process is halted (21) and additional use of the

product is disabled" and column 10, lines 1-20 and 43-52, "When the software application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation");

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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 22-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

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 (*Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user", column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy"... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

23. Regarding claim 21, Stringer teaches embedding an open watermark into the content data to permit enhanced usage of the content data by the user (column 7, lines 22-57, "a watermark or copyright notice that is inserted into the original material", column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use").

24. Regarding claim 22, Stringer teaches embedding at least one additional watermark into the content data (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52); 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 (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52);.

25. Regarding claim 23, Stringer teaches wherein the content data can be stored at a level of quality which is selected by a user (column 11, lines 2-15, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use").

26. Regarding claim 24, Stringer and Guedalia teach a method for creating a secure environment for digital content for a consumer, comprising the following steps: connecting a Satellite Unit (SU) to a local content server (LCS) (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63,

"transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9), 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 (column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);

analyzing the message to confirm that the SU is authorized to use the LCS (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

retrieving a copy of the requested content data set (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48, column 6, lines 4-11, column 8, lines 39-44 and 63-68, column 9, lines 1-13, column 10, lines 60-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)" and column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use"),

assessing whether a secured connection exists between the LCS and the SU (column 8, lines 61-66, "verifying an enable code", column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 53-68, "If the code fails the verification step, the process is halted (21) and additional use of the product is disabled" and column 10, lines 1-20 and 43-52, "When the software

application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation");

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 (column 6, lines 61-66, "verifying an enable code", column 7, lines 22-57, "a watermark or copyright notice that is inserted into the original material", column 9, lines 43-68 and column 10, lines 1-20);

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 having been set for legacy content if the LCS determines that use is not authorized (*Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user", column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy"... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

27. Regarding claim 25, Stringer teaches 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 (column 7, lines 22-57, "a watermark or copyright notice that is inserted into the original material").

28. Regarding claim 26, Stringer teaches wherein the robust watermark is embedded using any one of a plurality of embedding algorithms (column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52).

29. Regarding claim 27, Stringer teaches embedding a watermark which includes a hash value from a one-way hash function using the content data ((column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 14-24, "denaturing process is a unique, check-summed operation using any of the many known encryption algorithms, such as the data encryption standard published by the U.S. government ("DES")" and lines 43-52).

30. Regarding claim 28, Stringer teaches 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 (column 6, lines 52-66, "hidden portion A1", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52).

31. Regarding claim 29, Stringer teaches 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 (column 6, lines 52-66, "hidden portion A1", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52);

re-saving the newly watermarked copy to the LCS (column 6, lines 52-66, "hidden portion A1", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material" and column 9, lines 43-52).

32. Regarding claim 30, Stringer teaches saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS (column 6, lines 52-66, "hidden portion A1", column 7, lines 43-57, "a watermark or copyright notice that is inserted into the original material", column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system" and column 9, lines 43-52).

33. Regarding claim 31, Stringer and Guedalia teach a method of creating a secure environment for digital content for a consumer, comprising the following steps: connecting a Satellite Unit (SU) to a local content server (LCS) (column 4, lines 33-57, column 5, lines 35-40 and 53-64, column 6, lines 1-3 and 61-66, column 9, lines 43-63, "transaction code is given to a vendor sales representative at a remote location (61), e.g. over the telephone lines (65)", column 10, lines 53-68 and column 11, lines 1-9), 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 (column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59).

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 (column 8, lines 39-44, "placed on a temporary medium, such as a random access memory in a computer system", column 9, lines 53-63, "transaction code is given to a vendor sales representative at a remote location" and column 12, lines 3-59);

analyzing the message to confirm that the SU is authorized to use the LCS (column 7, lines 22-57, "provides a secure system which limits unauthorized access to the materials", column 9, lines 43-68 and column 10, lines 1-8);

receiving a copy of the content data set (column 3, lines 55-61, "time-limited and/or function limited use of the data", column 4, lines 6-22, column 5, lines 41-48, column 6, lines 4-11, column 8, lines 39-44 and 63-68, column 9, lines 1-13; column 10, lines 80-68", lets customers work with the software on a 'trial' basis (e.g. up to ten times)" and column 11, lines 1-9, "Upon credit approval, the sales representative gives the customer a special code number(s) that 'unlocks' the software products(s) for unrestricted use");
assessing whether the content data is authenticated (column 6, lines 61-66, "verifying an enable code", column 9, lines 53-68, "If the code fails the verification step, the process is halted (21) and additional use of the product is disabled" and column 10, lines 1-20 and 43-52, "When the software application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation");

if the content data is unauthenticated, denying access to the LCS storage unit (column 6, lines 61-66, "verifying an enable code", column 9, lines 53-68, "If the code fails the

verification step, the process is halted (21) and additional use of the product is disabled" and column 10, lines 1-20 and 43-52, "When the software application is run without using the present invention (in this case, process P0), the application gives an error message and terminates program operation");

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 (*Guedalia* – column 7, lines 37-53, "controlling access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user", column 8, lines 15-33, column 11, lines 21-57, "if a user is not authenticated, then unit 250 applies the default policy"... "Examples of possible default policies are: issue message; display low resolution image; display partial image; display marked image" and "if access is denied to an authenticated user, image data to which the user is entitled and which is closest to the image data requested by the user is sent for display", column 12, lines 10-21, column 13, lines 50-57 and column 15, lines 1-14, "the user is not permitted to retrieve the requested image data, since the resolution level requested is higher than that to which the user is entitled").

34. The motivation to combine would be to provide a "multiplicity of images stored on the image server at plural levels of resolution include images for which access is provided to a user at all of the plural levels of resolution irrespective of the authorization statue of the user" (*Guedalia* – column 6, lines 5-10).

35. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Guedalla within the teachings of Stringer in order to control "access to the multiplicity of images stored on the image server based on the level of resolution of the image to which the user seeks access and the authorization status of the user" (*Guedalia* – column 5, lines 34-44).

Response to Arguments

36. Applicant's arguments with respect to claims 1-31 have been considered but are moot in view of the new ground(s) of rejection.

37. Further, on page 11 of the Applicant's Specification, "content" is defined as "is used to refer generally to digital data, and may comprise video, audio, or any other data that is stored in a digital format". Thus, the Examiner broadly interpreted the claimed "digital content" to pertain to image data and is not limited to said interpretation. The Examiner recommends specifying the type of "digital content" within the claim language that is to be utilized within the claimed invention.

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

39. The following United States Patents are cited to further show the state of the art with respect to secure delivery of content, such as:

United States Patent No. 6,966,002 to Torrubia-Saez which is cited to show methods and apparatus for secure distribution of software.

United States Patent No. 6,263,313 to Milsted et al., which is cited to show a method and apparatus to create encoded digital content.

United States Patent No. 7,093,295 to Saito which is cited to show a method and device for protecting digital data by double re-encryption.

United States Patent No. 6,587,837 to Spagna et al., which is cited to show a method for delivering content from an online store.

United States Patent No. 6,931,534 to Jandel et al., which is cited to show a method and a device for encryption of images.

United States Patent No. 6,587,837 to Spagna et al., which is cited to show a method for delivering electronic content from an online store.

United States Patent No. 6,389,538 to Gruse et al., which is cited to show a system for tracking end-user electronic content usage.

United States Patent No. 5,513,128 to Harkins et al., which is cited to show a network having selectively accessible recipient prioritized communication channel profiles.

United States Patent No. 5,657,461 to Harkins et al., which is cited to show a user interface for defining and automatically transmitting data.

40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

Application/Control Number: 10/049,101
Art Unit: 2131

Page 37

41. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz 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.

42. 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). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA


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 Jeremiah Avery	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,341,429	08-1994	Stringer et al.	705/52
*	B	US-6,148,333	11-2000	Guedalla et al.	709/219
*	C	US-6,587,837	07-2003	Spagna et al.	705/26
*	D	US-6,263,313	07-2001	Milsted et al.	705/1
*	E	US-6,931,534	08-2005	Jandel et al.	713/176
*	F	US-7,093,295	08-2006	Saito, Makoto	726/26
*	G	US-6,966,002	11-2005	Torrubia-Saez, Andres	726/29
*	H	US-6,389,538	05-2002	Gruse et al.	713/194
*	I	US-5,513,126	04-1996	Harkins et al.	709/228
*	J	US-5,657,461	09-1997	Harkins et al.	715/733
	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, Part/rent Pages)
	U	
	V	
	W	
	X	


*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(e).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims 	Application/Control No. 10049101	Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A.
	Examiner Avery, Jeremiah	Art Unit 2131

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE									
Final	Original	10/23/2007									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									
	31	✓									

Search Notes 	Application/Control No. 10049101	Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A.
	Examiner Avery, Jeremiah	Art Unit 2131

SEARCHED			
Class	Subclass	Date	Examiner
none	none	10/23/07	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Updated EAST Search	10/23/07	JLA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
none	none	10/23/07	JLA



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 01/29/2008				
Scott A. Moskowitz #2505 16711 Collins Avenue Miami, FL 33160			EXAMINER AVERY, JEREMIAH L	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 01/29/2008	DELIVERY MODE PAPER

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

The time period for reply, if any, is set in the attached communication.

75

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) Syed Zia
(2) Scott Moskowitz (4) _____

Date of Interview: 24 January 2008

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: 1 and 16

Identification of prior art discussed: United States Patent No. 5,341,429 to Stringer et al. hereinafter Stringer and United States Patent No. 6,148,333 to Guedalia et al. hereinafter Guedalia.

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: See Continuation Sheet

(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 Syed Zia
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 if 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 and Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section B12.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiner's 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.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The Applicant explained his position that Stringer fails to disclose identification data and tagging of the digital content, as well as not providing authorization for using and watermarks embedded within the digital content. Also, differentiation between the watermarks of the claimed invention and those found within Guedalia was provided. Further discussion of the storing and transmission of authorized and unauthorized content was made to clarify the utilization of "legacy content" at a "predetermined quality level" within said storing and transmission from the local content server(s); as well as the definitions of what constitutes "authorized" and "unauthorized" content. The "digital content" within the context of the claimed invention was further elaborated upon with regards to the composition of the "fragile watermarks" as claimed by the Applicant. The 35 U.S.C. 112, 2nd paragraph rejections were discussed pertaining to the terms "can be", "may be" and "capable of". The Applicant will amend the claim language to remove the ambiguity that the previous claim language presented. Consideration of the topics discussed will be conveyed within the next office action, pending a formal written response regarding these topics from the Applicant.

PTOL-4 (Rev. 11-07-07)
Approved for use through 10/31/2017. OMB 2501-0121
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 10/d19/101 First Named Applicant: Scott Moskowitz
 Examiner: JEREMIAH AVERY Art Unit: 2231 Status of Application: REPLY IN HAND

Tentative Participants:
 (1) JEREMIAH AVERY (2) EDMUND
 (3) Scott Moskowitz (4) _____

Proposed Date of Interview: JAN 24, 2008 Proposed Time: 11:30 (AM/PM)

Type of Interview Requested:
 (1) Telephonic (2) Personal (3) Video Conference

Exhibit To Be Shown or Demonstrated: YES NO
 If yes, provide brief description: _____

Issues To Be Discussed					
Issues (Rej. Obj., etc)	Claim/ Fig. No		Discussed	Agreed	Not Agreed
(1) REJ 112 1-1/2	1/316	Prime Art N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2) REJ (1026)	11	capable of such that	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3) REJ (1026)	1-15/1231	CITATION: STRATEGIC CITATION: BROADWAY	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4) REJ 1026 1/2 1/2 1/2 1/2	1-15/1231	STRATEGIC AS 1026 & 1024 records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Confirmation Sheet Attached

Brief Description of Arguments to be Presented:
No PRIME ART RECORD FOR "Capable of such that"
TO ACCEPT CONTENT FROM USERS' LICENSING EXISTING COMMERCIAL AGREEMENTS
3 reasons for TRAVELER arguments STRATEGIC & OFFICIAL WORK 1/2
PRE-APPROVAL BRIEF COMMENTS RE: CLAIMS FOR AIRFARE

An interview was conducted on the above-identified application on _____
 NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
 This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

Applicant/Applicant's Representative Signature: Scott Moskowitz
 Examiner/SPE Signature: _____
 Typed/Printed Name of Applicant/ Representative: Scott Moskowitz
 Registration Number, if applicable: _____

This collection of information is required by 37 CFR 1.011. The collection is required to obtain or obtain a benefit by the public which is in the public interest (USPTO is present) an application. Confidentiality is provided by 35 U.S.C. 133 and 37 CFR 1.1, and 1.11. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual user, the amount of the amount of time you require to complete this form under supervision 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 1458, Alexandria, VA 22315-1458. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1458, Alexandria, VA 22315-1458.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 7.

03-03-08

JFW

2131

App'l'n No. 10/049,101

Amendment/Reply to Office Action of October 29, 2007 dated February 29, 2008



THE UNITED STATES PATENT AND TRADEMARK OFFICE

App'l'n No.	10/049,101	Confirmation No. 8028
Applicant	Scott A. MOSKOWITZ, et al.	
Filed	July 23, 2002	
TC/A.U.	2131	
Examiner	Jeremiah L. AVERY	
Docket No.	80408.0011	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR EXTENSION OF TIME & AMENDMENT/REPLY

Sir:

Applicant hereby requests a one (1) month extension of time to reply to the Office Action dated October 29, 2007. The time for response is therefore extended up to and including February 29, 2008. A credit card payment form in the amount of \$60.00 to cover the required fee is enclosed with this filing.

In response to the Office Action of October 29, 2007 the Applicants provide the following remarks:

03/04/2008 THUYEN2 00000012 10049101
02 FC:2251 ED.00 DP

In the Claims:

Applicants reserve the right to pursue the subject matter of the original claims in this application and in other applications. The amendments being made to the claims at the express instructions of the Office, namely Claims 1, 3 & 16 are being made with traverse. Applicants' remarks regarding the express instructions are respectfully presented below. The amendments to Claims 9 & 12 are being made for typographical or spelling errors and are not being made for reasons for 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]]~~ is stored and retrieved;
 - c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and
 - d) a programmable address module ~~[[which can be]]~~ programmed with an identification code uniquely associated with the LCS; andsaid domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

2. (original) The LCS of claim 1 further comprising

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]] is 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. (currently amended) The system of claim 8, wherein the SU has means to send[[ing]] 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 send[[ing]] a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

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

means to receive a copy of the content data set;

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

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

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. (original) 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 securing 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]] if 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. (previously presented) 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;

 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. (original) 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. (original) 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. (previously presented) 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, 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. (previously presented) 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. (previously presented) 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. (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. (previously presented) 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, 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 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

Applicants fully appreciate the time and consideration provided by Examiner Avery and Primary Examiner Syed Zia during the interview, on or about January 24, 2008 (Interview Summary dated January 29, 2008). During the interview Claims 1, 3, 16 and 31 were discussed. The Stringer and Guedalla references were discussed as not disclosing "predetermined quality level", "legacy content" and "watermarks" as disclosed and understood by one of ordinary skill in the art. Reference was made to the express definitions and drawings of the originally filed specification and interpretation of claim language in light of the specification. The 112 paragraph 2 rejections were also discussed with regards to "clarity and precision" and after final rejections (i.e., the Office Action was issued by the Office after a Request for Continued Examination). Additionally, "authorization" as that term is disclosed in the specification was also discussed. Applicants would like to thank Examiner Avery for affirming that Stringer does not teach or anticipate the instant claim[s] based on Section 102. Thus the pending claims patentably distinguish over Stringer and the cited references. The Section 102 rejection of Claim 16 and the newly asserted Section 103 rejections are traversed and will be addressed below.

Again with due and considered respect, several issues are discussed preliminarily, as follows:

Material Traversed

Applicants respectfully submit several arguments presented during prosecution lack written clarification and direct the Office to the following, cited here for reference, MPEP § 707.07(f) "Answer All Material Traversed":

In order to provide a complete application file history and to enhance the clarity of the prosecution history record, an examiner must provide clear explanations of all actions taken by the examiner during prosecution of an application.

Where the requirements are traversed, or suspension thereof requested, the examiner should make proper reference thereto in his or her action on the amendment.

Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it.

ANSWERING ASSERTED ADVANTAGES

After an Office action, the reply (in addition to making amendments, etc.) may frequently include arguments and affidavits to the effect that the prior art cited by the examiner does not teach how to obtain or does not inherently yield one or more advantages (new or improved results, functions or effects), which advantages are urged to warrant issue of a patent on the allegedly novel subject matter claimed.

If it is the examiner's considered opinion that the asserted advantages are not sufficient to overcome the rejection(s) of record, he or she should state the reasons for his or her position in the record, preferably in the action following the assertion or argument relative to such advantages. By so doing the applicant will know that the asserted advantages have actually been considered by the examiner and, if appeal is taken, the Board of Patent Appeals and Interferences will also be advised. See MPEP § 716 *et seq.* for the treatment of affidavits and declarations under 37 CFR 1.132.

The importance of answering applicants' arguments is illustrated by *In re Hertmann*, 261 F.2d 598, 120 USPQ 182 (CCPA 1958) where the applicant urged that the subject matter claimed produced new and useful results. The court noted that since applicant's statement of advantages was not questioned by the examiner or the Board of Appeals it was constrained to accept the statement at face value and therefore found certain claims to be allowable. See also *In re Soni*, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995) (Office failed to rebut applicant's argument).

Concretely, USPTO personnel begin examination by determining what, precisely, the applicant has invented and is seeking to patent, and how the claims relate to and define that invention. As the courts have repeatedly reminded the USPTO: "The goal is to answer the question 'What did applicants invent?'" *In re Abele*, 684 F.2d 902, 907, 214 USPQ 682, 687 (CCPA 1982). Accord, e.g., *Arrhythmia Research Tech. v. Corazonix Corp.*, 958 F.2d 1053, 1059, 22 USPQ2d 1033, 1038 (Fed. Cir. 1992). In accordance with MPEP § 2106II, quoted here, in part, for reference, Applicants requested and again request clarification on issues raised during prosecution as discussed during the interview:

It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, each claim should be reviewed for compliance with every statutory requirement for patentability in the initial review of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, USPTO personnel should state all reasons and bases for rejecting claims in the first Office action. Deficiencies should be explained clearly,

particularly when they serve as a basis for a rejection. Whenever practicable, USPTO personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application.

As will be presented below, Applicants seek written guidance on the Office's interpretation regarding at least the following: (1) Interpretation of the pending claims in view of the Advisory Action Before the Filing of an Appeal Brief dated July 31, 2007 (Paper No. 200070725) (2) The Office's interpretation of the claim[s] or suggestions to improve any *asserted* defects in the type of language used – in view of MPEP § 2173.02 & MPEP § 707.07(j) (3) The Office's interpretation of Stringer's express "Definition of Terms" in asserting a prima facie case under Section 102 and Section 103 – including, at least, "legacy content" and "predetermined quality level" & (4) Interpretation or declaration (e.g., Rule 130) in support of the Office's interpretation of Stringer's "watermarks" and Guedalia's "watermarks". Applicants contend neither reference discloses watermarks or corresponding subject matter as would be understood by a person having ordinary skill in the art. For these reasons, Applicants respectfully submit the claims are in condition for allowance and earnestly seek such disposition.

Rejections under 35 U.S.C. § 112 second paragraph

Claims 1, 3 and 16

Applicants respectfully traverse the rejections of Independent Claims 1, 3 and 16 (and all claims depending therefrom) under 35 USC § 112 2nd paragraph as allegedly "being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention" (October 29, 2007 non-final Office Action at Page 2). It is noted that a claim is read in view of the specification including any originally filed claims as well as drawings. One of ordinary skill in the art would readily understand the scope of the pending claims, thus, Applicants maintain Claims 1, 3 and 16 are allowable. Applicants have amended Claims 1, 3 & 16 at the express instructions of the Office, as discussed during the interview on or about January 24, 2008. However, the amendments are made with traverse for the following reasons, below.

Terminology – "Capable of"

To establish for the record that the claim amendments being *proffered* are not being made to create any prosecution history estoppel, Applicants respectfully submit the following points regarding the October 29, 2007 Office Action at Pages 2 & 3 – specifically, the following quoted statement, cited here for reference:

It has been held that the recitation that an element is 'capable of performing a function is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in any patentable sense. Please see *In re Hutchison*, 69 USPQ 138". Applicants respectfully traverse and request clarification in support of this contention. The MPEP apparently lacks reference to "*In re Hutchison*, 69 USPQ 138.

Respectfully, as recited, the argument and associated rejection does not appear to meet the standards of the Office. As per MPEP § 707.06 "Citation of Decisions, Orders Memorandums, and Notices":

In citing court decisions, the USPQ citation should be given and, when it is convenient to do so, the U.S., CCPA or Federal Reporter citation should also be provided.

The citation of manuscript decisions which are not available to the public should be avoided.

It is important to recognize that a federal district court decision that has been reversed on appeal cannot be cited as authority.

However, in the interests of compact prosecution, the Applicants performed an Internet search pointing to several Board of Patent Appeals and Interferences decisions – the quote cited above (i.e., as recited in the October 29, 2007 non-final Office Action) is *similarly* cited in the Internet searched decisions. One caveat is that "adapted to", not "capable of", appears to be the objectionable terminology. Notably, in each case the Board *reversed* and the applications issued as patents with the "adapted to" terminology. For instance, an Examiner's Supplemental Answer (*please see*, Appeal No. 94-3182, Application No. 07/899,707, page 3, which issued as U.S. Patent No. 5,935,806), as follows, in part, recites [emphasis added]:

The examiner notes that (Supplemental Examiner's Answer, page 2, second paragraph, to page 3, first paragraph): . . . it has been held by the courts that the recitation that an element is 'adapted to' perform a function is not a positive limitation but only requires the ability to so perform and does not constitute a limitation in any patentable sense. *In re Hutchinson*, 69 USPQ 138

Each case, paraphrased here for reference and cited below, recites: (1) not written for publication in a law journal and (2) not binding precedent of the Board in contrast with the Office standard as per MPEP § 707.06. In each case, the Board reversed and a patent issued with the original & objectionable "adapted to" language:

1) Appeal for Application No. 07/899,707 – which issued as U.S. Patent No. 5,935,806;

2) Appeal for Application 08/901,171 – labeled Examiner's Final Rejection at Page 4 & 5 of the Appeal Decision. The Application later issued as U.S. Patent No. 6,308,990;

3) 09/288,932, which issued as U.S. Patent No. 6,750,494; and

4) 09/484,604, which issued as U.S. Patent No. 6,666,754.

That the claims rejected in the non-final October 29, 2007 Office Action contain terminology that appears in claims for issued applications as reversed by the Board presents potential prejudice to the subject matter of the claims as originally presented herein. If express instructions by the Office to amend terminology eads the distinctiveness out of the words that the Applicants have used to claim the invention[s], the Office standard of applying the broadest reasonable interpretation of the claims in light of the specification would be undermined.

However, should the language continue to be objectionable, Applicants respectfully request the Office to provide guidance in light of the *per se* nature of evaluating claim terms, including, *inter alia*, "capable of", "such that", "may be", and, "can be". The following is presented for purposes of preserving broad interpretation of

the claims and establish that amendments made to the pending claims herein are made with traverse and are not being made to create any prosecution history estoppel.

MPEP "Per Se Rules"

Please see, for instance, MPEP § 2173.05(d) describing potentially indefinite claim language: "The above examples of claim language which have been held to be indefinite are fact specific and should not be applied as *per se* rules. See MPEP § 2173.02 for guidance regarding when it is appropriate to make a rejection under 35 U.S.C. 112, second paragraph." For reference, MPEP § 2173.02 "Clarity and Precision" is cited here [emphasis added]:

The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. When the examiner is satisfied that patentable subject matter is disclosed, and it is apparent to the examiner that the claims are directed to such patentable subject matter, he or she should allow claims which define the patentable subject matter with a reasonable degree of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement.

The essential inquiry pertaining to this requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. Definiteness of claim language must be analyzed, not in a vacuum, but in light of:

- (A) The content of the particular application disclosure;
- (B) The teachings of the prior art; and
- (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

...

If the language of the claim is such that a person of ordinary skill in the art could not interpret the metes and bounds of the claim so as to understand how to avoid infringement, a rejection of the claim under 35 U.S.C. 112, second paragraph, would be appropriate. See *Morton Int'l, Inc. v. Cardinal Chem. Co.*, 5 F.3d 1464, 1470, 28 USPQ2d 1190, 1196 (Fed. Cir. 1993). However, if the language used by applicant satisfies the statutory requirements of 35 U.S.C. 112, second paragraph, but the examiner merely wants the applicant to improve the clarity or precision of the language used, the claim must not be rejected under 35 U.S.C. 112, second paragraph, rather, the examiner should suggest improved language to the applicant.

For example, a claim recites "a suitable liquid such as the filtrate of the contaminated liquid to be filtered and solids of a filtering agent such as perlite, cellulose powder, etc." The mere use of the phrase "such as" in the claim does not by itself render the claim indefinite. Office policy is not to employ *per se* rules to make technical rejections. Examples of claim language which have been held to be indefinite set forth in MPEP § 2173.05(d) are fact specific and should not be applied as *per se* rules. The test for definiteness under 35 U.S.C. 112, second paragraph, is whether "those skilled in the art would understand what is claimed when the claim is read in light of the specification." *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576, 1 USPQ2d 1081, 1088 (Fed. Cir. 1986). If one skilled in the art is able to ascertain in the example above, the meaning of the terms "suitable liquid" and "solids of a filtering agent" in light of the specification, 35 U.S.C. 112, second paragraph, is satisfied. If upon review of the claim as a whole in light of the specification, the examiner determines that a rejection under 35 U.S.C. 112, second paragraph, is not appropriate in the above-noted example, but is of the opinion that the clarity and the precision of the language can be improved by the deletion of the phrase "such as" in the claim, the examiner may make such a suggestion to the applicant. If applicant does not accept the examiner's suggestion, the examiner should not pursue the issue.

If upon review of a claim in its entirety, the examiner concludes that a rejection under 35 U.S.C. 112, second

paragraph, is appropriate, such a rejection should be made and an analysis as to why the phrase(s) used in the claim is "vague and indefinite" should be included in the Office action. If applicants traverse the rejection, with or without the submission of an amendment, and the examiner considers applicant's arguments to be persuasive, the examiner should indicate in the next Office communication that the previous rejection under 35 U.S.C. 112, second paragraph, has been withdrawn and provide an explanation as to what prompted the change in the examiner's position (e.g., examiners may make specific reference to portions of applicant's remarks that were considered to be the basis as to why the previous rejection was withdrawn)

By providing an explanation as to the action taken, the examiner will enhance the clarity of the prosecution history record. As noted by the Supreme Court in *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722, 122 S.Ct. 1831, 1838, 62 USPQ2d 1705, 1710 (2002), a clear and complete prosecution file record is important in that "[p]rosecution history estoppel requires that the claims of a patent be interpreted in light of the proceedings in the PTO during the application process." In *Festo*, the court held that "a narrowing amendment made to satisfy any requirement of the Patent Act may give rise to an estoppel." With respect to amendments made to comply with the requirements of 35 U.S.C. 112, the court stated that "[i]f a § 112 amendment is truly cosmetic, then it would not narrow the patent's scope or raise an estoppel. On the other hand, if a § 112 amendment is necessary and narrows the patent's scope—even if only for the purpose of better description—estoppel may apply." *Id.*, at 1840, 62 USPQ2d at 1712. The court further stated that "when the court is unable to determine the purpose underlying a narrowing amendment—and hence a rationale for limiting the estoppel to the surrender of particular equivalents—the court should presume that the patentee surrendered all subject matter between the broader and the narrower language. . .the patentee should bear the burden of showing that the amendment does not surrender the particular equivalent in question." *Id.*, at 1842, 62 USPQ2d at 1713. Thus, whenever possible, the examiner should make the record clear by providing explicit reasoning for making or withdrawing any rejection related to 35 U.S.C. 112, second paragraph.

That being said, Applicants thank the Examiner for providing detail concerning the 35 U.S.C. § 112 2nd paragraph rejections. The comments provide an appreciated opportunity to more fully satisfy the requirements of 35 U.S.C. § 112 2nd paragraph. Though the Applicants contend that one of ordinary skill in the art would readily understand the claims as originally presented, the Applicants have amended the claim[s] in view of the comments provided by the Examiner in the October 29, 2007 non-final Office Action as supplemented by the Interview, on or about January 24, 2008 with traverse. Thus, reconsideration and withdrawal of the rejections are respectfully requested.

Last, Applicant respectfully directs the Office to the following, *Please see* MPEP § 2173.01:

A fundamental principle contained in 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers. They can define in the claims what they regard as their invention essentially in whatever terms they choose so long as **>any special meaning assigned to a term is clearly set forth in the specification. See MPEP § 2111.01.< Applicant may use functional language, alternative expressions, negative limitations, or any style of expression or format of claim which makes clear the boundaries of the subject matter for which protection is sought. As noted by the court in *In re Swinehart*, 439 F.2d 210, 160 USPQ 226 (CCPA 1971), a claim may not be rejected solely because of the type of language used to define the subject matter for which patent protection is sought.

Prior Asserted Rejections under 35 U.S.C. § 102

Prior Asserted § 102(b) Rejections based on U.S. Patent 5,341,429 ("Stringer")

Independent Claim 16 stands rejected as allegedly anticipated by U.S. Patent No. 5,341,429 issued to Stringer et al. (hereafter "Stringer"). See Page 3 of the non-final Office Action dated October 29, 2007.

Claims 16

In order for a reference to anticipate a claim, the reference must disclose each and every feature 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 (with traverse) Independent Claim 16 recites [emphasis added]: "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 securing 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]] if 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." A prima case for anticipation cannot be made for at least the reason that Stringer neither teaches nor anticipates (1) "legacy content". The Section 102 rejection of Claim 16 is also improper for at least the reason that Stringer fails to disclose or anticipate (2) "satellite unit" and (3) "an identification code uniquely associated with the LCS".

The non-final Office Action contends that Stringer discloses a conventional system for creating a secure environment for digital content, comprising at least a

Secure Electronic Content Distributor ("SECD"); a Local Content Server ("LCS"); and a Satellite Unit ("SU") (October 29, 2007 non-final Office Action at Page 3). This contention is respectfully traversed. Stringer cannot teach or anticipate the subject matter of the claims for at least the reason that Stringer expressly defines that only "authors" "build original material". Applicants respectfully direct the Office to Col. 5 ll. 24 - 67, Stringer's express definitions: (1) "Authors": Authors, composers, producers, or creators of original material who have access to components needed to build original material" (2) "Third Party": Transforms original ephemeral material to its denatured version and wrapper and delivers both to user; does not need to be the author"; and, (3) "User": Neither a third party, nor an author, uses the trial, evaluation, and enabled versions of the ephemeral material, engages a transaction, either alone or in conjunction with a third party". Thus, the parties of Stringer, whether they can even be identified as authors, third parties or users, can subsequently move content identical to the original material — *in any manner they choose*. Simply, Stringer cannot anticipate scenarios, by way of example, where all parties "have access to components needed to build original material". This undermines any prima facie case for anticipation of the claim[s] based on Stringer.

As the Office Action concedes, for each of the 1) SECD; 2) LCS; 3) SU; 4) "a first interface for connecting to a communications network"; 5) "a second interface for communicating with the SU", and, 6) "an interface for communicating with the LCS" recited in Claim 16, reference is made to the *same* "transaction code" described at Col. 9 ll. 43 - 63. This "transaction code", is additionally associated with Stringer's "... watermark or copyright notice ..." as allegedly the 7) "identification code uniquely associated with the SU" of Claim 16 (Office Action, at Pages 3 - 6). How this interpretation relates to Stringer's transaction flow, including the parties involved and the materials being transacted, is unclear. It is the contention of the Applicants that one transaction code is taught by Stringer and said transaction code reverses the wrapping of the denatured material to original material — removing all identifying information, one time. This is the express teaching of Stringer. For this very reason, there cannot logically be any satellite units ("SU") apart and separate from the SECD and/or the LCS as the transacted material is identical to the original material and can be transferred as an original to a satellite unit without identification or authorization of any Stringer "third party".

Second, as previously presented, Stringer fails to disclose any means to differentiate content *already* owned by users— even newly "transacted" content received by users under Stringer is of "unlimited use and ownership" (see Stringer at Col. 9 ll. 53-67; Col. 12 ll. 4-12; and Col. 12 ll. 40-48). As disclosed in the originally filed specification, "it is the user's prerogative to decide how the system will treat non-authenticated content, as well as legacy content". Even, where Stringer allegedly provides identification— it is controlled by *the* third party and made without regards to the content. In fact, it is not possible to differentiate between parties (i.e., users, authors, and third parties), argued above, as no identifying information is made persistent with content under Stringer's alleged "secure environment" for the express reason that every transacted copy is of "unlimited use and ownership". Subsequent

reuse, under Stringer, a previously purchased or legacy data set could not be differentiated from any other data set comprising the same content. No user can be reasonably expected to wrap content they already own to fit Stringer's requirement; no such user exists as per Stringer's express definitions as all users are assumed to have legacy content and the ability to create content under the teachings of the instant invention. As Stringer states: "To remove the watermark or other material and enable unlimited use of the material, the denatured version of the material is subjected . . . to . . . any other technique that would serve to erase the watermark from the original material" (Col. 7 ll. 51-57). Logically speaking, why would a user submit content already owned and perhaps in a currently available format agree to wrap said content? This represents a significant improvement over Stringer and the cited art as both legacy and new versions of content can be flexibly supported within the same environment. The instant specification provides ample non-limiting examples and diagrams.

Third, Applicants respectfully note that the "watermark(s)" of Stringer are not the "watermark(s)" of the instant invention[s], including the various types of watermarks described in the specification and claims, for at least the reason that the watermarks claimed herein are *not* removed or erased as expressly described by Stringer. Further, assuming for argument's sake, Stringer's alleged "watermark" is expressly "erased", the result would be an alleged conventional LCS that could not logically act on watermark information. Thus, Stringer does not teach, suggest or anticipate the digital watermarks of the claim[s]. By teaching removal of identifying information, Stringer cannot anticipate the LCS, let alone the SU, of the claims which provides an environment for materials that are essentially identical save the version or status of the data (e.g., *inter alia*, initial, free, legacy, secure, compressed, unsecure, purchased, original, watermarked, signed, hashed, validated, etc.). It logically follows that Stringer fails to anticipate the claim element[s] "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". For these additional reasons, Applicants respectfully request the Section 102 rejections be withdrawn.

A previously provided practical example demonstrates – access to the World Wide Web via a conventional PC by a user who may have uploaded content, with or without authorization, cannot be differentiated from the original creator or author under Stringer. At the filing date of Stringer, it is not even clear a prima case for anticipation can be made for Internet browsers let alone an LCS and/or SU for handling legacy content or watermarks. Stringer's third party wrapper *alone* " . . . [a]llows remote transaction to control bidirectional transformation between the original, evaluation, and trial versions of the material" (Col. 6 ll. 1 - 3). Applicants respectfully request clarification on the interpretation being relied upon for Stringer's express definitions and the pending claims in view of these definitions. Applicants respectfully point to 37 C.F.R. § 1.104 ("In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. . . The pertinence of

each reference, if not apparent, must be clearly explained and each rejected claim specified"). Thus, to establish for the record, it is respectfully requested a Rule 130 affidavit or its equivalent regarding Stringer's "watermarks" as they relate to the pending claim features.

Finally, one of ordinary skill in the art can readily appreciate the widespread existence of content in any number of formats— an example, data released prior to a particular protection scheme or without any use restrictions. Thus, the Applicants additionally traverse the assertion that Stringer or the cited art teaches or anticipates the claim feature: "said predetermined quality level having been set for legacy content". For exemplary purposes, in the case of music, though the present invention[s] are not limited to audio, a "predetermined quality level" (i.e., 44.1 kHz 16 bit) is an example of "legacy content". For purposes of argument, this legacy content is arguably *not* of lesser quality than MP3 or AAC—which *were introduced after compact discs* and are also compressed. And, Windows 95 may have *arguably* less features than Windows XP. But, Windows 95, being legacy content, is not arguably of lesser quality than Windows XP. The instant invention[s] can handle legacy content and verifiable or secure content seamlessly enabling a more diverse market for information. This is why the Applicants' claims offer significant advantages over Stringer and the cited art.

Because Stringer fails to disclose or anticipate all of the features of Claim 16 (and all claims that depend therefrom) is patentable over Stringer and the cited art. For these additional reasons the Section 102 rejections of Claim 16 (and all claims depending therefrom) based on Stringer should be withdrawn. Applicants respectfully request all outstanding rejections be withdrawn.

Rejections under 35 U.S.C. § 103

Similarly, per the Office's own analysis, Stringer alone does not make obvious Claims 1 - 15 & 17 - 31. In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 706.02(j):

"First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. 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 applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria

The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. 'To support the 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 to have been obvious in light of the teachings of the references.' *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985). See MPEP § 2144 - § 2144.09 for examples of reasoning supporting obviousness rejections."

Applicant submits that the Office Action has failed to establish a *prima facie* case of obviousness to the extent that the citations do not teach or suggest all of the claim elements. This was discussed during the Interview on or about January 24, 2008.

Second, there is no motivation or suggestion to make the proposed combinations of the citations as directed by the Office. More particularly, there is no motivation to combine Stringer with Guedalia. The Federal Circuit has 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).

Instead, it appears that the Office Action identifies citations without reference to the elements of the claims, 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 that would *allegedly* have been 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]. Applicant submits that the Office has not satisfied the initial burden "to provide some suggestion of the desirability of doing what the inventor has done" MPEP § 706.02(j):

It is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply. Furthermore, if an initially rejected application issues as a patent, the rationale behind an earlier rejection may be important in interpreting the scope of the patent claims. Since issued patents are presumed valid (35 U.S.C. 282) and constitute a property right (35 U.S.C. 261), the written record must be clear as to the basis for the grant. Since patent examiners cannot normally be compelled to testify in legal proceedings regarding their mental processes (see MPEP § 1701.01), it is important that the written record clearly explain the rationale for decisions made during prosecution of the application.

Last, *for argument's sake*, even if the claim elements did teach or suggest all of the claim elements there is no reasonable expectation of success in combining the citations as suggested by the Office Action. The suggested combination[s] are not a "predictable use of prior art elements according to their established functions" (*KSR* Opinion at Page 13 & MPEP § 2141 III - V). For at least these reasons, Applicant respectfully requests the Section 103 rejections of Claims 1- 15 & 17 - 31 be withdrawn.

1. a) 35 USC § 103(a) Rejections based on U.S. Patent No. 5,341,429 issued to Stringer et al. ("Stringer") in view of U.S. Patent No. 6,148,333 issued to Guedalia et al. ("Guedalia") as applied to Claims 1 - 15 & 17 - 31

Claims 1 - 15 & 17 - 31 have been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stringer further in view of Guedalia. Office Action *stafés*.

Stringer substantially discloses the claimed invention, however fails to disclose the limitations pertaining to "accepting the digital content at a predetermined quality level". Guedalia discloses this limitation as cited below (October 29, 2007 non-final Office Action at Page 7).

Applicant respectfully *traverses*. Without conceding the propriety of the asserted combination, Applicants submit that the asserted combination does not disclose at least the following feature of claims 1 & 3 (and all claims depending therefrom, respectively), among other features, "1) accepting the digital content at a predetermined quality level, 2) said predetermined quality level having been set for legacy content"; claim 17 (and all claims depending therefrom), among other features, "1) permitting use of the content data set at a predetermined quality level, 2) said predetermined quality level having been set for legacy content if the LCS determines use is not authorized"; claim 20 (and all claims depending therefrom), among other features, "1) if a secured connection exists, embedding a watermark into a copy of the requested content data set, 2) said watermark being created based upon information (transmitted by the SU and information about the LCS"; claim 24 (and all claims depending therefrom), among other features, "1) said watermarked content data set delivered at a predetermined quality level, 2) said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized", and claim 31 (and all claims depending therefrom), among other features, "1) if the content data is not capable of authentication, 2) accepting the data at a predetermined quality level said, predetermined quality level having been set for legacy content" for at least the following reasons. Stringer apparently teaches access restriction under the following express definitions: (1) "Authors'. Authors, composers, producers, or creators of original material who have access to components needed to build original material" (2) "Third Party' Transforms original ephemeral material to its denatured version and wrapper and delivers both to user; does not need to be the author"; and, (3) "User'. Neither a third party, nor an author; uses the trial, evaluation, and enabled versions of the ephemeral material; engages a transaction, either alone or in conjunction with a third party" (Stringer at Col. 5 & Col. 6 "Definition of Terms").

As is commonly understood by one of ordinary skill in the art, Stringer teaches wrapping content through a denaturing process, discussed previously. Once removed the content exists as original material with no identifying features. Thus, Stringer teaches away from the claim(s), as no "legacy content" can be identified or referenced as per the subject matter of the pending claims - including content already possessed by a user. Guedalia is cited for its alleged disclosure of various features of claims 1 -

15 and claims 17 - 31. Applicants respectfully submit that Guedalia does not add anything to Stringer that would remedy the deficiencies cited above. Guedalia too teaches access restriction, as described under at least Col. 9 ll. 7 - Col. 10 ll. 47, "Access Control" based on an "authorization status of a user" (see, for instance, Guedalia at Col. 8 ll. 10). The Office's assertion concerning legacy content is unclear as all materials cited in Guedalia are centralized in an image server and cannot be "accepted" as "legacy content" by a user - that inherently undermines the policy of access control as expressly disclosed by Guedalia. Further, Guedalia's watermarks are not the watermarks of the pending claims but visible overlays or logos (see Guedalia at Col. 10 ll. 30 - 64). Guedalia's access controls do not act on content that would be in the possession of the user and thus no "legacy content" is disclosed, anticipated or suggested. Content cannot flow up into an LCS as disclosed by the instant claims only down from an access restricted server. For this reason, Guedalia like Stringer teaches away from the pending claims.

Second, the Office has not presented "clear and particular" evidence of a motivating force. The Office Action appears to identify citations that allegedly disclose elements of the claims. This gives rise to impermissible hindsight, as there is clearly no motivation to combine Stringer with Guedalia. Even assuming, *for argument's sake*, there was a motivation to make the proposed combination of Stringer with Guedalia, the combination fails to disclose or suggest all of the terms of independent claims 1, 3, 17, 20, 24 & 31 (and all claims depending therefrom, respectively). Combining Stringer with Guedalia would be improper as Stringer's "denatured material" wraps data cryptographically. Again, this teaches away from making *legacy content* available to encourage broader access to information. In fact, the combination of Stringer with Guedalia would likely increase the computational complexity of distributing data without any established benefit. It is unclear how Stringer's users could be differentiated from Guedalia's users as neither reference permits "legacy content" to be provided from the "user". Third, there is no reasonable likelihood of success. Applying Stringer's "denatured material" would logically result in a cryptographic wrapping of Guedalia's access restricted image data - teaching away from the claims. In fact, denatured material makes transfer of *further access restricted data including* the wrapping itself computationally infeasible. For these additional reasons, it is respectfully submitted the Section 103 rejections should be withdrawn.

The Office's assertion at page 34 of the non-final Office Action, number 34, is respectfully traversed for these reasons and the reasons discussed in connection with Claim 16, above. A cursory review of Guedalia fails to reveal users having content locally stored and maintained on their own server, there is no LCS as disclosed. The additional assertion at Page 35, number 35, further undermines the argument of number 34, authorization of "a user" who already possesses content obtained or created by herself makes access control to a remote server irrelevant to the claim language. Let alone the claim language as interpreted in light of the specification. The further suggestion that amendment of the claim terms to fit the asserted art, Guedalia is directed at images alone, undermines the Office standard, argued previously, of broad interpretation of the claims and the Graham factual inquiries as understood and

cited at Page 7 of the Office Action. Further, Applicants traverse the basis for the Response to Arguments at Page 35 of the non-final Office Action, "Examiner recommends specifying the type of 'digital content' within the claim language that is to be utilized within the claimed invention". There has been no written response by the Office to the traversed arguments made to date argued previously, above. As per the Office standard the claims are readily understood by one possessing ordinary skill in the art. However, the suggested combination[s] are not a "predictable use of prior art elements according to their established functions" (KSR Opinion at Page 13 & MPEP § 2141 III - V) and fail to provide a prima facie case for obviousness. It is respectfully submitted that there is no reasonable likelihood of success in combining these two citations, at least as suggested by the Office and thus no prima facie case for obviousness can be made based on Stringer in view of Guedalia.

Last, a review of the Office Action makes clear that in each rejection, Stringer with Guedalia are relied upon for those elements that are present in the independent claims as well as the dependent claims. Because the citations, either alone or in combination fail to disclose all of the claim elements, the Office has failed to establish a prima facie case for obviousness for all claims that depend from Claims 1, 3, 17, 20, 24 & 31. See MPEP § 2143.03: "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). For at least this reason, the Office has failed to establish a prima facie case of obviousness for all claims that depend from Claims 1, 3, 17, 20, 24 & 31. See MPEP § 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious."). Accordingly, for at least these reasons, Applicants respectfully request withdrawal of the Section 103 rejections for Claims 1- 15 & 17 - 31.

Appl'n No. 10/049,101

Amendment/Reply to Office Action of October 29, 2007 dated February 29, 2008

Conclusion

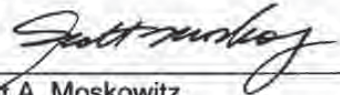
Applicants maintain that this application is in condition for allowance, and such disposition is earnestly solicited. Applicants' silence as to the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection. If the Examiner believes that an interview with the Applicants, 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,

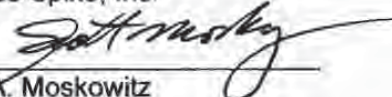
Date: February 29, 2008

By:



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

For Blue Spike, Inc.



Scott A. Moskowitz
President



PTO/SB/08A (10-07)

Approved for use through 10/31/2007. DMS 0651-0031
U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE

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

Substitute for form 1448P10

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete If Known

Application Number	12/049,601
Filing Date	July 23 2002
First Named Inventor	MILKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	30106-001

Sheet 1 of 1

U. S. PATENT DOCUMENTS

Examiner Initials*	Doc No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant, Paragraph or Figure Number
		Number-Kind Code ² (if known)			
		US-6,088,455	07/11/2000	Ligan et al.	
		US-5,634,040	05/27/1997	Har et al.	
		US-6,381,747	04/30/2002	Wynior et al.	
		US-4,969,204	11/06/1990	Melnichuk et al.	
		US-6,866,002	11/15/2005	Torricelli-Sabat	
		US-6,263,313	07/17/2001	Mitsuda, et al.	
		US-7,093,295	08/15/2006	Saito	
		US-6,587,897	07/01/2003	Speigne et al.	
		US-6,931,534	08/16/2005	Jandel et al.	
		US-2004/0049695	03/11/2004	Choi et al.	
		US-2004/0083369	07/25/2003	Erlingsson et al.	
		US-5,677,952	10/14/1997	Elakety et al.	
		US-5,768,396	06/16/1998	Sone	
		US-7,266,697	09/04/2007	Kirovski et al.	
		US-5,136,646	08/04/1992	Haller et al.	
		US-5,136,647	08/04/1992	Haller et al.	
		US-7,206,649	04/17/2007	Kirovski et al.	
		US-6,532,284	03/11/2003	Walker et al.	
		US-7,020,285	03/28/2006	Kirovski et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Doc No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant, Paragraph or Figure Number	T ³
		Country Code ⁴ Number ¹ Kind Code ² (if known)				

Examiner Signature	Date Considered
--------------------	-----------------

***EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 608. 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 designations number (optional). ² See Rules Governing the 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 31.3). 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 symbol as indicated on the document under WIPO Standard 31.16 (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. 132 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 this 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 (1-800-776-9199) and select option 2.

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

<p>Continuation for form 1449PTO</p> <h2 style="text-align: center;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT</h2> <p style="text-align: center;"><i>(Use as many sheets as necessary)</i></p> <p>Sheet <u>2</u> of <u>2</u></p>	<p style="text-align: center;">Complete If Known</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Application Number</td> <td>10/047 101</td> </tr> <tr> <td>Filing Date</td> <td>July 22 2002</td> </tr> <tr> <td>First Named Inventor</td> <td>MOOFALITE</td> </tr> <tr> <td>Art Unit</td> <td>2151</td> </tr> <tr> <td>Examiner Name</td> <td>AVEEY</td> </tr> <tr> <td>Attorney Docket Number</td> <td>104 09.0011</td> </tr> </table>	Application Number	10/047 101	Filing Date	July 22 2002	First Named Inventor	MOOFALITE	Art Unit	2151	Examiner Name	AVEEY	Attorney Docket Number	104 09.0011
Application Number	10/047 101												
Filing Date	July 22 2002												
First Named Inventor	MOOFALITE												
Art Unit	2151												
Examiner Name	AVEEY												
Attorney Docket Number	104 09.0011												

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number and Code ² if known			
		US 7,046,808	05/12/2006	Matojs et al.	
		US 6,430,301	08/06/2002	Petrovic	
		US 2004/0059918	03/25/2004	Xu	
		US 6,345,100	02/05/2002	Lavine	
		US 2004/0093521	05/13/2004	Hamedeh et al.	
		US 2007/0083467	04/12/2007	Lindahl et al.	
		US 7,231,524	06/12/2007	Burns	
		US 2005/024655A	11/03/2005	Batson	
		US 6,868,325	02/23/2003	Coffberg et al.	
		US 7,050,396	05/23/2006	Cohen et al.	
		US 6,842,862	01/11/2005	Chow et al.	
		US 7,051,208	05/23/2006	Venkatesan et al.	
		US 7,240,210	07/03/2007	Mctiak et al.	
		US 7,150,003	12/12/2006	Naumovich et al.	
		US 6,389,538	05/14/2002	Grusa et al.	
		US 5,513,126	04/30/1996	Hankins et al.	
		US 5,657,461	08/12/1997	Hankins et al.	
		US 4,390,896	06/28/1983	Bond et al.	
		US 5,471,533	11/28/1995	Wang et al.	

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

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw the 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 ninth Code of USPTO Patent Documents at www.uspto.gov or MPEP 1811.04. ³ Enter circle that codes the document, by the examiner code (WFO 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 WFO 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 1.07 and 1.08. The information is required in obtain or retain a benefit by the patent which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.16. This collection is estimated to take 2 hours in complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P. O. Box 1450, Alexandria, VA 22315-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22315-1450.

If you need assistance in completing the form, call 1-800-PTO-5199 (1-800-786-5199) and select option 2.



Approved for use through 10/31/2007. OMB 0651-0031
 U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
 Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it carries a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Substantive Patent Application No. 10/049,501			Complete if Known		
				Application Number	10/049,501	
				Filing Date	July 23, 2002	
				First Named Inventor	Moskowitz	
				Art Unit	2131	
				Examiner Name	AVERY	
Sheet	1	of	1	Attorney Docket Number	SCH08.0011	

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.†	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	†
		Rivest, et al., PayWord and MicroMint: Two simple micropayment schemes, MIT Laboratory for Computer Science, Cambridge, MA 02139, April 27, 2001, pp. 1-18.	
		Horowitz, et al., The Art of Electronics, 2nd Ed., 1989, pp.7.	
		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110 (Abstract).	
		Schneider, M., et al. "Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC Lausanne), Sept 16-19, 1996, pp. 227-230, IEEE ISBN: 0-7893-3711-1	
		Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	
		Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, Vol. 1, Oct 4-7, 1998, pp. 455-459.	
		Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, Vol. 1525, April 14-17, 1998, pp. 218-238, ISBN: 3-540-65386-4	
		Ross Anderson, "Stretching the Limits of Steganography," LNCS, Vol. 1174, May/June 1996, 10 pages, ISBN: 3-540-61996-8.	
		Joséph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997, 4 pages.	
		Joséph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing, August 21, 1997, 19 pages.	

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not obtainable in conformity with MPEP 808. Draw line through citation if not in conformity and not available. Include copy of the form with next communication to applicant.
 † Applicant's official citation designation number (optional). ‡ Applicant to fill in date a check mark here if English language Translation is attached.
 The collection of information is required by 37 CFR 1.85. The information is required to inform or return a benefit by the public which is in the (and by the USPTO to process an application). Confidentiality is governed by 35 U.S.C. 102 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the DIPTO. Time will vary depending upon the individual case. Any comments on the content of the form you require to complete the form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-RTX-9199 (1-800-758-9199) and send option 2.



PTO/SB/088 (04/07)

Approved for use through OMS/0007, OMB 0551-3031
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 carries a valid OMB control number.

Substitute for INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>	Complete if Known	
	Application Number	10/049,101
	Filing Date	July 23 2002
	First Named Inventor	MOSKOWITZ
	Art Unit	2121
	Examiner Name	AVEKLY
Sheet 1 of 2	Attorney Docket Number	80408 D011

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	Page Count
		PCT International Search Report, completed Sept. 13, 1995; authorized officer Huy D. Vu (PCT/US95/08159) (2 pages)	
		PCT International Search Report, completed June 11, 1996; authorized officer Salvatore Cangialosi (PCT/US96/10257) (4 pages)	
		Supplementary European Search Report, completed Mar. 5, 2004; authorized officer J. Hazel (EP 96 91 9405) (1 page)	
		PCT International Search Report, completed April 4, 1997; authorized officer Bernarr Earl Gregory (PCT/US97/00651) (1 page)	
		PCT International Search Report, completed May 6, 1997; authorized officer Salvatore Cangialosi (PCT/US97/00652) (3 pages)	
		PCT International Search Report, completed Oct. 23, 1997; authorized officer David Cain (PCT/US97/11455) (1 page)	
		PCT International Search Report, completed July 12, 1999; authorized officer R. Hubeau (PCT/US99/07262) (3 pages)	
		PCT International Search Report, completed June 30, 2000; authorized officer Paul E. Callahan (PCT/US00/06522) (7 pages)	
		Supplementary European Search Report, completed June 27, 2002; authorized officer M. Schoeyer (EP 00 91 9398) (1 page)	
		PCT International Search Report, date of mailing Mar. 15, 2001; authorized officer Marja Brouwers (PCT/US00/18411) (5 pages)	

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 600. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 † Applicant's unique citation designation number (optional). ‡ Applicant is to place a check mark here if English language Translation is attached.
 This collection of information is required by 37 CFR 1.89. The information is required to obtain or retain a patent by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, completing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing this form, call 1-800-PTO-9199 / 1-800-786-9199 and select option 1.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		<i>Complete if Known</i>			
		Application Number	10/049,101		
		Filing Date	July 23 2002		
		First Named Inventor	MOSKOWITZ		
		Art Unit	2131		
		Examiner Name	AVEEY		
Sheet	2	of	2	Attorney Docket Number	80108.001

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
		PCT International Search Report, completed July 20, 2001; authorized officer A. Sigolo (PCT/US00/18411) (5 pages)	
		PCT International Search Report, completed March 20, 2001; authorized officer P. Corcoran (PCT/US00/33126) (6 pages)	
		PCT International Search Report, completed January 26, 2001; authorized officer A. Sigolo (PCT/US00/21189) (3 pages)	
		European Search Report, completed October 15, 2007; authorized officer James Hazel (EP 07 11 2420) (9 pages)	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformity with MPEP 609. Draw line through citation if not in conformity and not considered. Include copy of this form with each 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 1.96. This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, encoding, 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-5192 (1-800-786-5192) 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 27 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVEEY
Attorney Docket Number	84/08.001

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.†	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		STAIN D (The Singles 1996-2006), Warner Music - Atlantic, Pre-Release CD image, 2006, 1 page	
		Arctic Monkeys (Whatever People Say I Am, That's What I'm Not), Domino Recording Co. Ltd., Pre-Release CD image, 2005, 1 page	
		Radiohead ("Hail To The Thief"), EMI Music Group - Capitol, Pre-Release CD image, 2003, 1 page.	

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 600. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 † Applicant's unique citation designation number (optional). ‡ Applicant is to place a check mark here if English language Translation is attached.
 This collection of information is required by 37 CFR 1.98. The information is required to allow or retain a benefit by the public which it 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 this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



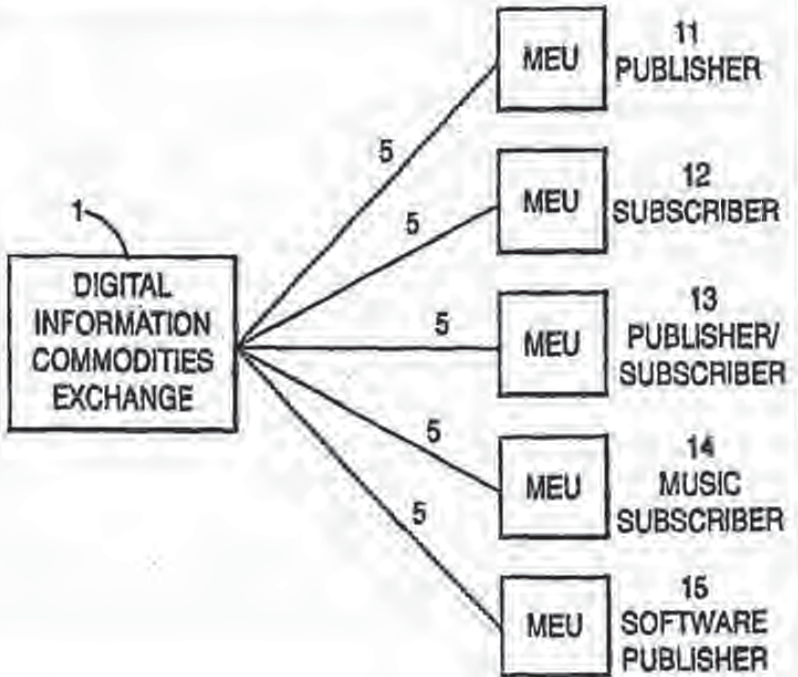
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04B 13/00, H04J 3/26, H04L 12/40	A1	(11) International Publication Number: WO 97/01892
		(43) International Publication Date: 16 January 1997 (16.01.97)
(21) International Application Number: PCT/US95/08159	(91) Designated States: CA, CN, JP, KR, SG, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 26 June 1995 (26.06.95)		
(60) Parent Application or Grant (63) Related by Continuation US 08/083,593 (CIP) Filed on 30 June 1993 (30.06.93)	Published <i>With international search report.</i>	
(71)(72) Applicant and Inventor: MOSKOWITZ, Scott, A. [US/US]; 20191 E. Country Club Drive, North Miami Beach, FL 33180 (US).		
(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).		

(54) Title: DIGITAL INFORMATION COMMODITIES EXCHANGE WITH VIRTUAL MENUING

(57) Abstract

A system for the exchange of digital information packets includes an exchange (1) with connectors to allow modular expandable units (11-15) to connect to the exchange over transmission media (5). The modular expandable units (11-15) send digital information packets from one to another over the exchange (1) in response to requests for these digital information packets. The exchange (1) allows for billing and other administrative functions. A virtual menuing system is disclosed for use with the exchange (1) allowing a simple choice of digital information packets to be published and/or subscribed to.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LJ	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

DIGITAL INFORMATION COMMODITIES EXCHANGE
WITH VIRTUAL MENUING

FIELD OF THE INVENTION

5 The present invention relates generally to an information network and menuing system, and more particularly to a digital information exchange system (DICE) where users can send and receive multiple types of data with a virtual menu.

10 BACKGROUND OF THE INVENTION

 A multitude of electronic bulletin boards are in use today. Such bulletin boards generally consist of a particular type of data and are geared to a particular market. Generally, a subscriber has an interest in a
15 particular subject, connects to a bulletin board corresponding to that subject, and retrieves information from it. Occasionally a subscriber may leave information on a bulletin board, either for use by another subscriber or to an administrator of the board. Generally, the flow
20 of information is downstream, i.e., from the board to the subscriber.

 For the purpose of this discussion, a person is referred to as subscriber if they are receiving information. A person or entity who is supplying
25 information is referred to as a publisher.

 The current paradigm under which these bulletin board systems operate requires that a subscriber own a computer system with which to connect to the bulletin

board. Such a computer system usually requires a CPU, a keyboard, and a CRT or other display device. A subscriber generally "downloads" information from the on-line system's service to his or her private computer system. The information is generally usable only within the context of the computer system. Examples of such information include executable computer software (particular to certain types of computers) and data files that are understood by programs which run on the subscriber's computer and which contain information (e.g., a graphical image or sound clip). It is very difficult, at best, for a subscriber to use the information received from the on-line system outside of the bounds of a computer system.

Different commercial embodiments of electronic bulletin boards vary in the types of digital data used. However, they are similar in the direction of the flow of data. For example, the Prodigy® and CompuServe® systems are popular news and entertainment services. With the exception of their electronic mail, shopping, and billing, the flow of information is towards the subscriber. Similarly, the Audio Archive in Syracuse, New York, provides hundreds of thousands of downloadable audio recordings to subscribers. The only information sent upstream by the subscriber to the Archive is the choice of recording.

Under present distribution systems, such as cable TV networks, downstream flow is the norm. A cable subscriber is simply presently incapable of sending the same type and quantity of data in the reverse direction. At best, current interactive cable systems in testing stages allow for a minimal backchannel to allow subscribers to send selection data to a collection or centrally located video server device. With on-line services such as CompuServe®, the parties involved in the transaction are forced to store their data on

Compuserve®'s computers. If Compuserve® computers went off-line, so would all of its subscribers.

There are also a number of prior art patents disclosing such a downstream, unidirectional flow of data, e.g., U.S. Patent No. 5,132,992 to Yurt et al., U.S. Patent No. 4,326,289 to Dickinson, and U.S. Patent No. 4,491,983 to Pinnow.

The above systems demonstrate a basic limitation of the traditional digital communications system, namely, the subscriber is limited to a particular library and is limited to a particular data type. In addition, the subscriber must access a library with a particular device such as a computer, or with a subscriber interface module (SIM).

There is a need for a system in which a vast number of participants can act as providers as well as consumers of data, in the manner of a commodities exchange. Such a system would give rise to a much larger number of producers of data than is presently available. This could ultimately provide a wider range of information topics available to information seekers and would provide more of an information marketplace.

It would also be desirable and possible to provide data for almost any and every interest. In essence, one could provide a multimedia system in which all types of digital data (music, text, moving video, virtual reality, etc.) could be published and subsequently subscribed to by consumers using their information or entertainment system, and which could be expanded to adapt to different data types thereby further expanding the digital information marketplace.

Such a system would be modular and provide that the failure of any one unit would not preclude other subscribers from making use of the system.

Three problems, at least, are addressed:

1. The difficulty encountered by individual subscribers who wish to publish data, whether for

commercial or private purposes, which are in part caused by the paradigm of archive/download and implemented in hub-oriented networks.

2. The limitation imposed by current systems wherein data addressed via the system is useless (digitally) outside the system and/or SIM, either because it has no meaning or because it cannot be easily transferred out.

3. The slowness of data transfer across only one transmission line. In particular, transmission times are made faster by using parallel transmission techniques across distinct transmission media.

The invention as disclosed and claimed further includes details of the specific processing method for implementing an information service menu (for computers and other similar devices) between the host device and a remote client device connected by an arbitrary telecommunications link.

The use of the disclosed menu invention represents an improvement in the art in, e.g., the specific areas of efficiency of transmission and flexibility of presentation.

The current state of the art in computer systems and telecommunications technology includes rapidly proliferating on-line services, remote operation and navigation of information systems, to provide a remote host or server which communicates via telecommunication lines with various clients. One aspect of such systems, from modern graphical interfaces to ASCII-only technologies, is the use of menus to facilitate interaction between the host and the users of the client machines. Typically, a menu has a list of items, characterized by an ASCII text label for each, which provides an intuitive description of the choices available to a user. The selection of such an item, which may be associated with a fixed numeral to provide a shorthand method of identifying it, is communicated

from the client to the host which then causes some action associated with the item in question to take place. In the context of a graphical user interface, such as Windows or the Macintosh OS, various embellishments such as special fonts or icons may be added to the presentation of such menus, and the display of the menu as a whole may be packaged into some graphical enclosure construct in order to separate menu items from surrounding information.

10 Menus can furthermore be hierarchical. That is, they may contain items which themselves represent submenus.

 A typical example of such a menuing system is that used by the on-line service America On-Line (AOL). AOL has two basic types of menus. In particular, AOL presents various screens having several icons (graphical devices used in place of traditional text labels). To select an item, the user clicks on an icon with a graphical pointing device such as a mouse. Although this looks much different from a traditional text based menu, it implements the same function. By clicking on the various icons, the user can navigate to various content-specific areas of the host information system in a trigger action such as query processing or the inputting of additional information from the user. In addition, and often in combination with the icon-based menu, AOL also uses more traditional text-based menus.

 One problem encountered with systems like AOL is that menus are typically of unpredictable length as they may change with added content and very often they are quite long. This may prove a liability if the communications medium between client and host is bandwidth limited. A noticeable delay occurs should the entire menu be sent from the host to the client. AOL works around this limitation by only transmitting only a portion of a long menu at a time. Thus, a long menu may be broken into several shorter chunks. Additional chunks

are sent only when the user attempts to navigate past the last item received. AOI also works around the platform-specific issues by arranging the storage of frequently used platform-specific icons and other such information with its client-local interface on the client. One way of accomplishing this is the use of coded information in the stream of host to client which specifies an icon to look up in the client's data base. The client software determines if it does not have the item, it asks the host to send it, at which time it is added to the client data base for future use and displayed accordingly.

This system also has several limitations. First, a user must often endure the delay should they wish to access a menu item at the end of a long menu. They must wait patiently as each chunk is downloaded in turn. They receive no direct indication as to how many more items they must transverse to reach the end of a menu, or how many more chunks must be downloaded. Second, should a user navigate to the end of a long menu, the entire menu is now in memory at the client, although the user may only be interested in a single item. On current PC platforms, the amount of memory occupied by a menu may seem insignificant compared to the total content, but in smaller, portable devices, any memory optimization is valuable. Third, the client is responsible for archiving menu embellishments such as icons, which may occupy valuable non-volatile storage space.

It is therefore an object of the present invention to implement a menuing system which has the properties of increased efficiency and having an information content which is independent of the modality of which the content will be presented. It is also desired to add contents specific to modality, without restricting the usefulness of the information stream as a whole. It is also an object to send an information stream (such as a menu) to a client running one of any number of different operating systems with graphical interfaces, or even to a client

who does not have the benefit of such a graphical interface, and to have the stream interpreted correctly, without the necessity of each client's platform-specific software having to interpret information specific to another platform. At the same time, the additional information for use in the system should be available to leverage any advantages inherent in the target system. For instance, a menu to be received by a Macintosh might contain information representing an icon associated with each item, and a screen position at which to display the icon, while this information would be useless to a non-Macintosh platform.

One benefit of such a system is that it can remove a significant amount of processing necessary at the host to deal efficiently with clients of varying platforms. The same menu information stream could be sent to various types of clients without the need to alter the information stream according to the client. A minimal level of functionality is guaranteed at the client, while the host can opt to provide additional functionality in the stream according to its resources (such as storage space or processing speed) or lack of them.

Summary of the Invention

The invention disclosed herein includes a method for employing software to use a virtual menuing system. Specific implementation of those common computer interface components such as menus is disclosed which possesses the properties discussed above and as such represents an improvement in the art.

The present invention is also directed to the problem of developing a digital information commodities exchange in which the data flow is bidirectional rather than unidirectional and in which subscribers can exchange information with each other through the system. A subscriber could just as easily send the same type and quantity of information as he can receive; thus, making

them a publisher. The present invention is also directed to the problem of accommodating different data types within the same modular system, thus allowing for an exchange of a virtually unlimited range of digital commodities. In addition, the present invention provides for the automated conversion and transfer of arbitrary formats beyond the SIM.

The present invention removes the limitations of the electronic bulletin boards described above in the following way. An exchange system is provided, but it is not the ultimate source of any data itself. The exchange system is simply a conduit through which users can perform digital transactions. To further support the development of a data marketplace, the exchange can provide administrative functions such as billing. In addition, transactions are not required to pass through a particular publisher or exchange, therefore, allowing any publisher and subscriber to also communicate directly.

These digital transactions are facilitated by modular expandable units (MEU) operated by publishers and subscribers. A publisher makes a publication available to the exchange via the publisher's own modular expandable unit. Likewise, a subscriber can then subscribe to this publication, using his or her own modular expandable unit, by contacting the exchange to receive the desired publication. Those who wish to use the system as publishers can attach electronic devices to the system which can act as archives specific to the information that the publishers wish to provide, on a case by case basis. However, in no case would subscribers be required to route their transactions through devices belonging to any particular publisher. Any such transaction (publication or subscription) may result in charges to both or neither or either of the parties involved. Because the system is a true bilateral exchange, any supplier can be a subscriber and similarly

any subscriber can be a supplier. The modular expandable units enable the publisher/subscriber to upload and download data in a variety of formats, such as music, text, and computer programs (e.g., personal computer programs, Nintendo programs, etc.) via their inherent expandability. The modular expandable units are also expandable with respect to the form of data transmission, so as to accommodate telephone, satellite, electric power lines, CATV, cellular or fiber optic communications.

10 In a DICE exchange network, if an MEU or general archival device goes off-line, only that device and any subscribers connected to it are affected. The affected subscribers are immediately free to try to obtain the desired data via another source, since their MEUs are still fully functional. This is clearly an improvement over the phone, cable, on-line, or digital packet switching networks described in the prior art.

20 The MEUs enable users to upload or download data in a variety of formats (such as music, text, computer programs, graphics, Nintendo games, etc.) through their expandable architecture. MEUs are electronic devices characterized by an internal data bus, (or multiple buses) connected to a multiplicity of expansion interface slots. A specific protocol is used to move data between a variety of expansion modules which may be connected to the bus via the expansion interface slots. This protocol is always the same no matter the specific circuitry of an expansion module plugged into a slot. Each of these modules, in turn, may be capable of converting data received from the MEU's internal bus to a specific format to be outputted from a plug, connector, or other external interface (also part of the expansion module). Similarly, the expansion module may receive data from an external device via the external interface, convert it to the MEU internal protocol, which then transmits it to another distinct expansion module attached to the MEU's bus(es).

For example, MEU expansion modules can be made available for each of the following data transmission standards: NTSC Video, Optical Digital, Audio, Two-channel Stereo, Audio, Appletalk, Ten Base-T Ethernet, Thin Ethernet, Thick Ethernet, Token Range, Coaxial Cable TV, Analog Cellular, TVMA Cellular, CVMA Cellular, and so on. The idea is to establish an internal standard capable of delivering a throughput sufficient for any digital application, and then to provide translators for any established standard deemed common enough to merit inclusion. The MEU itself speaks none of those standards internally, but merely moves raw data between one standard and another, at the will of its users. In short, the MEU is a device with an architecture that makes no assumptions about what type of data it is handling internally, but allows for additional specialized circuitry to be added as easily as inserting a bank card in an ATM machine, thus, providing an expandability to other and new data transmission formats as they gain acceptance, even though they may not have existed when the MEU design was finished.

The MEU design also anticipates benefits from multiprocessing. All data processing will occur in microprocessors attached to the expansion modules. Each expansion module may in fact house a complete, encapsulated data processing environment, including memory, microprocessors, and other special purpose IC's like digital signal processors. MEUs with one or several expansion modules containing microprocessors could take advantage of multiple data buses and multiple communication lines connected to the expansion modules' external interfaces to break up a large chunk of data into several smaller discrete component data chunks, and transmit them simultaneously over several distinct lines of communications, after which they may be reassembled into a single coherent chunk of data by a similarly equipped MEU which is receiving the data. This method of

simultaneous transmission should be distinguished from the parallel computer interface, which transmits simultaneous bit streams over several distinct strands of wire which are all bound together in a single cable. The difference is that each of those bit streams are governed by the same protocol and, if one wire breaks, any transmission over this interface is impossible. The method to be employed by MEUs splits a data stream over multiple channels, each having its own protocol, possibly distinct physical transport, and which may have distinct protocols. If any one of the multiple channels fails, the MEU can continue, simply by eliminating that channel from consideration.

15 BRIEF DESCRIPTION OF THE DRAWINGS

FIG 1 shows the layout of a small data exchange network in accordance with an embodiment of the present invention, as well as each consumer's intended use.

20 FIG 2 shows the implementation of a data exchange system with three hubs. Several networks are attached to each hub.

FIG 3 shows a typical publisher/subscriber connection in an embodiment of the present invention.

25 FIG 4 shows a modular expandable unit, including its base system, communications converters, and expansion modules according to an embodiment of the present invention.

DETAILED DESCRIPTION

30 The method and apparatus of the present invention will be described using an example of a digital information commodities exchange. However, the present invention is not limited to the exchange of the specific digital information described below.

35 In a digital information commodities exchange operating according to the present invention, the exchange commodity comprises digital information packets.

The information, which can represent a variety of different kinds of data, is encoded in a standard format by an expandable modular unit operated by the publisher/subscriber.

5 A commodities exchange includes a system capable of performing at least four functions: receiving/storing notification of the availability of a particular digital information packet, receiving/storing a digital information packet from a publisher, sending a digital information packet to a subscriber, and maintaining records of a subscriber and/or publisher transaction.

10 A publisher transmits a notification of the availability of a digital information packet to the exchange. The publisher may also notify subscribers directly of the availability of such information in a variety of ways. The publisher can, for example, advertise within the exchange itself or in any other medium such as print (e.g. newspapers). A subscriber can then request transmission of such a packet from the publisher. This publish/subscribe transaction could occur in real time, e.g., the subscriber could achieve access to a live concert, or it could be separated in time, e.g., a subscriber could access a video game that had been published weeks or months earlier. In either case, the publisher transmits the digital information packet over the selected transmission medium to the exchange. To perform the publication transmission, the publisher is connected to the exchange system using a modular expandable unit (MEU) and over the transmission medium of his or her choice. Likewise, the subscriber is connected to the exchange using a modular expandable unit and the medium of his or her choice. However, one MEU can send information directly to another MEU without being connected to the exchange over dedicated lines.

15 Furthermore, these lines do not have to be packet switched.

Upon receipt of a digital information packet from the publisher, the exchange system can send the packet to the requesting subscriber. The subscriber requests a particular packet using a simple menu-driven process jointly administered by the subscriber's modular expandable unit and the exchange system. To receive the transmission, the subscriber is also connected to the exchange system through his or her own modular expandable unit.

The exchange system includes a network of computers (that may be geographically dispersed) and the communications devices to send and receive various data over various media.

Fig. 1 exhibits a proposed embodiment where the digital information commodities exchange is connected to a number of publishers and subscribers. For the sake of illustration only five users are shown. Element 1 is a commodities exchange system which has the ability to handle many simultaneous publication/subscription sessions. Element 11 is a modular expandable unit of a publisher of digital information packets. In this instance the packets produced by publisher's unit 11 relate to audio data such as music. Element 12 is a modular expandable unit of a home subscriber who can receive data in a variety of forms, including text, audio, video or computer program data. Element 13 is the modular expandable unit of a user who intends to both subscribe and publish digital information packets, in particular audio information. Element 14 is the modular expandable unit of a subscriber who intends to receive music to dub onto his or her own home video tapes. Finally, element 15 is the modular expandable unit of a publisher of digital information packets for hand-held computer games. Initially the publisher 11, using his or her own modular expandable unit, contacts the exchange to make a publication request and to register the publication parameters: artist, title, pricing,

14

marketing plan, etc. This is accomplished via point selections from menus on the modular expandable unit which is interacting with the exchange. At this point the publisher may wait for a request from a subscriber.

5 Alternatively, depending on the storage capabilities of the exchange, the publisher may wish to store his or her publication on the exchange so that it would be immediately available to subscribers. In this situation a publication-recording session must occur. The

10 publisher might have recorded the audio publication on digital audio tape and would then play and transmit it to the exchange via his or her modular expandable unit and the transmission medium of his or her choice. Alternatively, the publisher may elect to transmit live

15 via an analog-to-digital conversion system to the exchange. In either case the session would be played to completion and stored on the exchange at an appropriate address whereupon the publisher would indicate termination by a signal from the modular exchange unit

20 and the exchange confirming the same.

The subscriber of element 14, after learning of the newly available digital information packet, in this example music, would then use his or her modular expandable unit to make a subscription request to the

25 exchange, using the transmission medium he or she prefers. Again, by moving through a series of menus that refine his or her choices, the subscriber chooses the desired music item. The first menu might list music as one category of available packets, the second menu might

30 list styles of music, the third might list particular artists, the fourth might list an artist's albums and the fifth menu might be a list of the songs on a particular album. A particular song, group of songs or an entire album may be subscribed to as a single digital

35 information packet.

After the subscriber has selected the particular digital information packet which he or she would like to

receive, the exchange 1 receives the request, notifies the publisher's computer (or modular expandable unit) that the digital information packet is to be transferred, prepares the selection for transmission, confirms that the subscriber's modular expandable unit is ready, and proceeds to transmit the selected digital information packet. The quality of this publication will depend on the quality of the publisher's recording equipment and likewise the quality of the subscription depends on the subscriber's equipment.

FIG 2 exhibits a similar system as FIG 1, but on a considerably larger scale. In this figure, several different exchanges 1 are illustrated, each with an arbitrary number of modular expandable units 13 attached to it. This figure also illustrates that a single exchange 1 can be connected to other exchanges 1, as well as to other MEUs. In this way the network can spread in a horizontal sense so as not to overburden a single exchange with too many units 13. Also, the network can spread in a vertical sense by nesting one exchange within another. Note that this configuration allows the network to incorporate and complement existing systems, such as CompuServe®, etc.

As is evident in FIG 2, a distinguishing feature of the exchange of the present invention and other exchanges or networks lies in the administrative functions the exchange performs. Each exchange has a user directory 41 and a digital information packet directory 42. Digital information packet directory 42 does not contain the actual packets themselves, but rather is a list of where the packets are located on the exchange. The user directory 41 is a list of which users are located at which addresses on the exchange. In contrast, networks not of the present invention, denoted 50 in FIG 2, need only have a user directory 41. This is because their "digital information packets" are contained within their central singular computer rather than distributed amongst

many different digital commodities 'brokers' 13.
Finally, it is important to note that user 13 is not
limited to those digital information packets located in
the directory 42 of his or her own particular exchange 1.
5 This is because a particular exchange 1 may also search
other exchanges throughout the system for a particular
requested digital information packet. This packet could
then be sent to the user in a manner completely analogous
to the transfer of a packet from a publisher to a
10 subscriber.

Although the best quality recording is stored on a
master tape originally made at the studio, exceptionally
high quality reproductions can be achieved after a
conversion to a compact disk standard format (CD). Thus,
15 it is likely that the publisher will upload the
reproduction from a compact disk. While a typical CD
player would convert the data from a digital format to an
analog format before sending it to the amplifier, in this
case the signal could be removed from the CD player at 31
20 in a digital format and could be directed to the modular
expandable unit's expansion module in that same format.
The expansion module 32 provides the necessary connectors
to interface the CD player with the modular expandable
unit through the control unit 33. The modular expandable
25 unit can then provide any necessary data compression.
The signal can then be sent over a telephone line \$ via
a modem, with the modem also providing the necessary
conversion to an analog format. If, in the alternative,
a fiberoptic cable were employed, the data could remain
30 in digital format.

The maximum amount of information to be sent can be
calculated as follows. Using a band width of 3300 Hz and
a signal-to-noise ratio of 20 dB, it is estimated that a
telephone channel can handle about 22,000 bits of data
35 per second. Standard modems today have bit rates of up
to 19,200 bits per second. Use of an ISDN standard and
digital switches would allow a rate of up to 64,000 bits

per second to be achieved. A compact disk player, handling the audio frequency range of up to 20 kHz, and taking into account the Nyquist frequency of the disk player and the need for two channels for stereo sound, would require about 80,000 bytes per second. The large data rate mismatch would require, on the publisher's side, a buffer 32, as depicted in FIG 3, to store data prior to the data being sent over the telephone line. The size of the buffer would depend on the length of the digital information packet to be sent. Once the data is buffered and sent over the telephone line, a buffer 23 on the subscriber's side would restore the data to its original rate. The data could then be stored in a variety of forms. Each buffer 23 forms part of its modular expandable unit. The expansion module 24 could be equipped with both digital and analog outputs. The digital output emerges directly from the modem. The analog output is simply the digital output after processing by a digital-to-analog converter. In the present example, the signal can then be sent into either a digital or analog input of a digital audio tape player.

In the course of buffering the data, compression techniques can be used to speed the transfer. Other techniques, such as storing the data on RAM chips, can be used to minimize the time necessary to maintain the telephone connection. Additionally, if a fiberoptic link is used to transfer the data, the wide band afforded by the fiberoptic would allow the packet to be sent even more expeditiously.

Publishers and subscribers can be connected to the exchange system over any one of a variety of transmission media 5. For example, they may choose to be connected to the exchange system over private circuits, television lines, the public switched telephone network, cellular communications, electric power lines, or even satellite communications. Depending on the type and amount of data

to be sent, some of the digital information packets could be sent over one type of medium and simultaneously another part could be sent over a different type of medium. For example, if a movie were to be transmitted to a subscriber, the audio portion of the movie contains considerably less information than the video. Thus, the telephone line, with its limited band width, is sufficient to transmit the audio portion of the movie. A higher band width transmission medium such as a fiberoptic, a cable TV line, or a power line could be used to transmit the video, thus allowing a more rapid transfer of a digital information packet. The exchange provides this versatility by being equipped with a large variety of transmitters/receivers interfaced to many types of transmission media.

The exchange system is capable of performing administrative functions with respect to the publication/subscription transactions. The exchange system interacts with publishers and subscribers via menu-driven software so that the users can easily perform the desired transactions. The exchange system can also maintain profiles of subscribers and their usage in such a way that subscribers may be kept informed of newly available digital information packets that may be of particular interest. Publishers may be kept informed of who is subscribing to their publications and any other relevant market information. To support the exchange system, transaction fees may be charged to either the publisher, the subscriber, or both. Furthermore, the exchange system can track the publications and subscriptions so that either the exchange system or the publisher can bill the subscriber for the price of the digital information packets. The exchange can provide many options regarding the commercial aspects of the digital information commodity exchange. For instance, various price mechanisms can be supported. In this way the subscriber can be charged less per packet for

ordering a higher quantity of data, or alternatively can be charged less for ordering a data reproduction of lesser quality. For example, a video for use on standard televisions would cost less than one for use on high-
5 definition televisions. Some publishers would pay to have their publications subscribed to. An example might be a car company who would issue an exchange credit for the first 1000 subscribers who receive their video of a test drive of the company's new luxury car. Similarly,
10 receiving a live lecture from a Nobel Laureate might cost more than receiving the same lecture pre-recorded.

FIG 4 schematically illustrates a modular expandable unit. A modular expandable unit can provide the interface to the exchange system for either a publisher
15 or a subscriber. A modular expandable unit includes a central processing unit and various expansion modules 24. The central processing unit includes an input, an output, a serial line for connecting the input to the output, software running on a microprocessor which may be used to
20 select which digital information is desired, and a system for entering commands. The software system can be in the form of microcode or can utilize other known techniques such as EPROM. Obviously contrary to some popular usage, the term central processing unit as used here encompasses
25 more than just a microprocessor. A base system of the modular expandable unit is used to send requests to the exchange and may include a small video screen 23, an apparatus for inputting commands 26 (e.g., a keyboard or a pointing device), and software for user interaction.
30 In addition, the MEU is capable of accepting input and output from several known techniques such as a keyboard, a CRT, a modem, etc. The software serves to configure the hardware and to control the conversion of data with the appropriate add-on communication module. The unit is
35 also capable of sending digital information packets to the exchange system, receiving digital information packets from the exchange system, reformatting data

received from the exchange system for replaying on a specific device, and playing or recording digital information packets thus received.

The modular expandable unit is capable of sending and receiving digital information packets to and from the exchange system over a selected transmission medium 5. If the transmission along a particular data link fails, it does not preclude the parties in that link from immediately re-establishing the connection in another link. The unit may also have a variety of expansion modules 24 available, some of which serve to format a particular data type and others which serve to adapt the modular expandable unit with a particular transmission medium. For example, if a publisher wants to send a digital information packet from a digital audio tape (DAT) over an ISDN connection to the exchange, the MEU would have an expansion module 24 allowing the MEU to interface to an appropriate DAT device and would have an expansion module to interface to the ISDN circuit. The data coming from the DAT device would be received by the expansion module, reformatted and buffered, as necessary, by the unit and then the modular expandable unit would send the data to the exchange system 1 over the selected transmission medium 5. Examples of appropriate expansion modules 24 for audio data are those that accommodate devices using digital audio tapes, digital compact cassettes, analog speakers, analog cassettes, 9-track tapes, and telephones, however, other expansion modules might be used. Standard interfaces also exist for other data types: NTSC video, serial/parallel PC, Group III fax, etc.

In the example noted above, the subscriber at element 13 received a digital information packet from a publisher at 11. This same subscriber may wish to send a digital information packet to the publisher for review, and perhaps future publication. Thus, the consumer at element 13 will then in turn be acting as a publisher.

If the consumer at element 13 is a relatively small publisher, the manufacturing technology of producing a compact disk may be unavailable. He or she can still, however, record a digital information packet on an analog or digital audio tape. That digital information could then be sent to the exchange system using the same technique described before. In this case, rather than a menu-driven method of locating the information, the consumer may use a known address to send the information to the recipient. The recipient of the digital information packet at element 11 may store the data in RAM or perhaps in a tape format. The consumer at element 13 does not require a DAT player; a regular analog tape player suffices. In that case, however, the modular expandable unit to which it would be connected would need to be equipped with an analog-to-digital converter which could convert the data on the tape to a form usable by the modem. As stated before, this is because the bandwidth needed for most music is about 20 kHz while the bandwidth usable by a telephone is on the order of 4 kHz.

In addition to audio data, the modular expandable unit could also interface with video data devices and computer data devices through appropriate expansion modules 24. Examples of appropriate expansion modules for video data are those that would interface with devices using VHS tapes, Beta tapes, VHS-C tapes, and 8 mm tapes. Examples of appropriate expansion modules for specialized video data are those that accommodate high-resolution video/graphics screens. Examples of appropriate expansion modules 24 for computer data are those that accommodate devices using parallel ports, serial ports, printers, magnetic disks, magnetic diskettes, magnetic tape, flash RAM, EPROM, and ramdisks. Of course, for all of the above varieties of data, if the data type is initially analog, it must be converted to one of the standard digital formats prior to being published on the exchange. This analog-to-digital

converter can be a separate module attached to the modular expandable unit and may be bidirectional.

5 The modular expandable unit 14 is capable of receiving digital information packets from the exchange system 1 over the selected transmission medium 5. After the subscriber requests a particular digital information packet, the requested digital information packet is transferred to the modular expandable unit via the selected transmission medium. The received requested
10 data could be played in real time, could be stored in temporary memory for a later one-time-only play, or could be directed through an appropriate expansion module 24 to a particular recording device, such as those named above, where it may be recorded and thereafter repeatedly
15 played.

The modular expandable unit would further be capable of recording and playing back digital information packets received from the exchange system 1. Once the digital information packet has been received by the modular
20 expandable unit 14, it is directed to an expansion module 24 which acts as an interface for a particular device which is related to the type of data received. For example, if the requested digital information packet is a computer program, the MEU 14, through the appropriate
25 expansion module 24, could store the program onto a hard disk or diskette. In this same example, if a computer program required a particular operating system with which to run, the operating system could also be downloaded as a separate digital information packet. In addition, if
30 the publisher desires, a copy-inhibit feature could be included by the publisher and would be transmitted along with a particular digital information packet to prevent software piracy.

The received data can then be sent from the MEU 14
35 to any of the devices that can use digital data and are connected to the expansion modules 24 as described above.

In the example shown in FIG. 1, a subscriber at element 14 may wish to receive a digital information packet from publisher 11. This digital information packet could, for example, be music which is to be dubbed onto a home videocassette. In this case, the transfer would be similar to that described above. The music would be replayed at element 11, buffered, sent over the phone line 5 to the exchange system 1, and then sent to the modular expandable unit 14 to be re-buffered at 21 and output as a digital information packet in the same form as it was played by the publisher. This digital information can then either be sent, in this example, to the digital audio input of a videocassette recorder, or can be first sent to a digital-to-analog converter, and then sent to the analog audio input of a videocassette recorder.

In the example shown by FIG. 1, the publisher at 15 could be a software publisher who sells software products over the DICE to subscribers. A subscriber at element 12 could use the same menu-driven process as described above to request a particular digital information packet, in this case a software product. The program might then be uploaded from the publisher to the exchange system 1 and sometime later downloaded to a requesting subscriber. This type of transfer would be considerably quicker and simpler than the above-mentioned transfer of video and audio digital information packets, because there is usually much less information contained in this type of digital information packet.

In another embodiment, two private individuals may use DICE to exchange a digital audio recording. Letters "A," "B" will denote two different subscribers at two remote locations. Assume both individuals have one MEU containing the following: a primary interface expansion module, an LCD display pad, a keypad, two POTS expansion modules, one RAM expansion module, one digital audio expansion module with a digital audio input and output,

and one flash-file expansion module. Individual A has a DAT system and two POTS telephone lines. Individual B has a home entertainment center, including a stereo and two POTS telephone lines. Subscriber A would like
5 subscriber B to hear an excerpt of his latest musical composition. Thus, A contacts B via voice phone. Subscriber A asks subscriber B if he is ready to receive and B responds affirmatively. Then, both subscribers hang up the line. At this time, subscribers A and B
10 connect their two POTS lines to each of their respective MEUs. Individual A has stored his compressed digital recording in RAM on his MEU and (selecting from a series of menus displayed in the MEU LCD) programs his MEU to transfer the recording from his MEU to the phone number
15 of B. Subscriber A sends information informing the MEU of subscriber B of what resources (e.g., phone numbers) are available. It then asks the MEU of subscriber B for similar information.

It is now the job of subscriber A to determine that
20 it can transfer data over a dedicated line to MEU B. In doing so, once this acknowledgment is made, subscriber A dials up subscriber B along one of the dedicated lines. Once a connection has been made, subscriber A allocates a percentage of data to send over each line (50% is the
25 case shown if both lines have identical characteristics). Subscriber A partitions the data, encrypts it, and queues each of the chunks to the POTS expansion modules. Subscriber A informs the MEU of subscriber B of the intended transfer over one of the dedicated lines.
30 Subscriber A further signals the POTS expansion modules to commence a simultaneous transfer over the dedicated lines. Subscriber B encrypts the data and re-integrates it from the two POTS modules into RAM. After this, subscriber B may then hang up the dedicated line as well
35 as can subscriber A. Subscriber B may see a displayed message that the transfer is done and complete and may unplug from both POTS lines. Subscriber B further may

pull the stereo line out of his MEU and the selection may be used to play the RAM resident data through his stereo output. The transfer is completed and subscriber B is able to listen to an excerpt of musical composition from subscriber A.

A virtual menuing means or system is also provided for a remote interface to information systems. Such a system has three components. First, the host device contains the complete menu. The client has a device linked to the host by an arbitrary telecommunications link, which receives discrete portions of the menu from the host, presents this to a user, and relays selection codes from the user to the host in the context of the menu.

The client implements a "menu window" over the larger host-based menu, which contains only a subset of the menu items available at the host. This window at the client can be moved dynamically over the full range of the host-based menu, providing access to all menu items. Traversal of the host-based menu need not be in contiguous increments, however. To solve the problem of making an arbitrarily long list of menu items accessible to a client, menu items are presented in a manner analogous to a voice mail type of menu, with a touchtone keypad. This specific scenario might be handled at the client. Clients which use the virtual menuing system described here would maintain the following information:

- (1) a "range" of "floating" items R representing the traditional scrolling area of a menu, and
- (2) a range of "hot key" items H that remain at a fixed location regardless of any scrolling of the floating items.

The number of menu items (M) in a host may be equal to nine (corresponding to touch tone digits 1-9). The number of "hot key" (H) items visible in the client menu may be equal to three (corresponding to the touch tone keys *, 0, and #), which are typically special function

keys in a voice menu. The value of M is arbitrary. In general practice, M is greater than or equal to the floating range number of items (R), which are the number visible at one time in the client's menu. If not, no scrolling would be necessary at the client, and only M less than R would be valid menu choices, with the balance remaining as unused and displayed as blank items. The number of hot key items actually used can be any number less than or equal to H.

5
10 The host maintains a menu as a single contiguous list of items. Each item has at least an ASCII string identifier and an index number unique to the item. Typically, such numbers would start at "1" and increase for each item but any such arrangement is possible.

15 The total number of items displayed at the client equals the number of floating items plus the number of hot key items. The sum is the number of items actually displayed on the interface of the client device. The floating and hot key items are maintained in contiguous arrays. Clients communicate their configuration with regards to the number of each type of item to the host.

20 For a given client, the host maintains a menu base indicator, representing which item in its menu list the client has displayed as the first item in the floating area. It also knows the floating range of the client. So the current main chunk seen by the client is the range of items starting from the base. Aside from the number of hot keys transmitted once for the menu, the host sends chunks of range R items. The configuration also includes information regarding the scrolling increment of the client wishes to use.

25
30 The hot keys could perform any number of functions. In the case of a 100-item menu, with a floating range of ten items, if the user was at the beginning of the menu, and used a hot key function to zoom to the end, the host could simply set its base to item 91, directly from item 35 1, and send items 91 to 100, thus saving the transmission

of the intervening 80 items. In a typical scenario, a 100 item menu might be rare, and even considered a poor design. As the market for interactive and on line content evolves, however, large menus representing catalogs of content will be quite commonplace.

In general, the system implements a two-way data stream between the host and client. The host transmits menu chunks, as well as updates to individual or small numbers of menu items, to the client, while the client sends selection codes to the host. The selection codes include tokens representing the various hot keys, as well as navigation codes such as Up, Down, In, Out, (for hierarchical menu navigation), Select, and Zoom.

The following codes are examples of those that may be sent from the client to the host in response to user actions at the client.

SelectUp

If the current menu item at the host is greater than one, it is decremented by one. If the resulting current menu item is less than the base, the base is decremented by the client's scroll increment, and the menu chunk from the base item of R items is transmitted to the client. The client displays the new menu chunk, effecting a scroll up.

SelectDown

Similar to SelectUp, except the current item is incremented if it is less than M. If the current item exceeds the item computed by adding the range R to the base, then the base is incremented by the client's scroll increment and the menu chunk is transmitted from the base item of R items to the client. The client displays the new menu chunk, effecting a scroll down.

SelectIn

If the current menu items is itself a menu, the host is initialized with the new menu information, and a menu definition is transmitted containing summary information
5 on the new menu to the client, which clears its display. The host base is set to item one. If there are items in this menu, then the menu chunk is sent starting from the base. The client displays the new menu.

10 SelectOut

If the client has navigated inside a sub-menu, that menu is unloaded recovering the previous menu, initializing the host to base one, and a new menu definition is transmitted. Further, the first menu chunk is sent to
15 the client. The client displays the menu which contained the menu it previously displayed.

SelectCurrent

This signals the host to perform some operation related
20 to the menu item currently highlighted in the client menu. This is the current menu item at the host. The action triggered is determined by the host.

SelectZoom (i: L; = i; = R)

25 This sets the current menu item at the host to correspond to the client menu item within the client's currently displayed floating range, which is indicated by the value of i. The current item is computed by adding i to the base and subtracting 1.

30

Select HotKey

Any number of predefined functions could be tied to hotkey codes. There are three types of menu transmissions from the host to the client. Each current
35 menu item is highlighted in the client display.

Menu Definition

This includes information on how many columns to display in the menu, and what the labels of such columns are (if there are multiple items per row). One row is still
5 considered one menu item. Each row may have multiple segments, with each segment applying to a column in the definition. It might also include information on hotkey items.

10 Menu Chunk

This represents a complete range of menu items. If a client was configured with a floating range of nine items, then each menu chunk would contain the data for the nine rows of the menu, including all row segments for
15 each item.

Menu Update

Data included in this message can be used to alter the display of individual menu items without redrawing a
20 complete menu range, or to change the information on hotkey functions. It would be used to immediately add a check mark to an item that was selected using SelectCurrent. Although the client might do this himself, if he waits for the host to send a Menu Update,
25 the client reflects the actual state of the host.

The present invention is well-adapted to the recent development of multimedia microprocessors. For example, AT&T's 32-bit Hobbit microprocessor has a built-in
30 communications ability, as well as a multitude of connectivity products being designed for it. These include applications allowing users to interact with multimedia in real-time over telephone lines. Such a microprocessor would well serve the needs of a digital
35 information commodities exchange and in particular the MEU. Depending on the connectivity of the products that are designed for the Hobbit microprocessor and its built-

in communications facilities, the need for elaborate buffering of data may be less necessary than envisioned above. For example, the Hobbit microprocessor's communications abilities may be used to simplify much of the transmissions requirements.

Menu-driven software on the MEU would allow users to request digital information packets. This software interacts with software running on the exchange. Communications software on the exchange and on the MEU coordinates the transmission of digital information packets between them.

The menu-driven software could first request a publisher/subscriber's identification number and password for verification. The software would then inquire whether the publisher/subscriber chooses to publish a digital information packet, subscribe to a digital information packet, or gather information about a digital information packet.

If the publisher/subscriber chooses to subscribe to a particular digital information packet, he or she would conduct a search to find that digital information packet by maneuvering through one or more menus and thereupon requests it. If a publisher/subscriber wishes to post a publication on the exchange, he/she also "logs in" but then inputs the particulars of his/her publication. The menu-driven software can be similar to that used, for example, by the Prodigy® Network where the user first views a menu with a choice of different types of news stories, such as business news, politics, sports, etc. Once the subscriber chooses a particular type of story, the subscriber is then presented with another menu with a choice of other stories, all within that same type of news. After choosing a story from this menu the user is then actually looking at the text of a news story. Alternatively, a program similar to Apple® Computer's Applesearch® program could be employed to facilitate key word searches of data. Applesearch® is also used to rank

the retrieved documents by relevance. In the present system, the user would have a menu with choices of different types of data to request. These menus would ask the user if the information requested is textual, 5 visual, aural, etc. or a combination of these. The categories would further divide into news, music, movies, educational, and other subdivisions. After several iterations of choices, the user would find the appropriate digital information packet, and request it. 10 The user further could specify to what device the digital information packet is to be sent. The exchange system, after verifying the functionality of all the appropriate ports, would arrange the transfer, from the digital information commodities exchange, of the requested 15 digital information packet to the subscriber's MEU where it would be directed to the expansion module associated with the specified attached device, and optionally would bill the subscriber accordingly.

If the publication is meant for real-time access and 20 the publisher is connected to the exchange at all times, then the information could be routed from a publisher to a subscriber at any time the subscriber chooses. If this publisher is only intermittently connected to the exchange system, then the subscriber would wait until the 25 publisher is on-line again before the data could be requested and transferred from the publisher through the exchange system 1 to the subscriber. Alternatively, if the publisher has stored his or her publication on the exchange, the digital information packet would be 30 available whenever a subscriber wishes to subscribe to it. In any case, after the subscriber specifies the digital information packet to be sent, notification of the time of sending, whether immediate or in the future, would be given to the subscriber.

35 If the publisher/subscriber chooses to publish a particular digital information packet, occasionally in response to a subscriber request, he or she could replay

the digital information packet and also describe to the exchange system what the electronic standards are for replaying the data. The publisher also specifies price and distribution information. The publisher then specifies to which subscriber the digital information packet is to be sent. The exchange system again verifies the functionality of the selected ports. The digital information packet is then sent through the exchange system to the subscriber. Billing information is again recorded.

To verify the integrity of a received digital information packet, a data flag could be put on to the end of the digital information packet. The flag would thus notify the exchange that the entire packet was received. The publisher/subscriber would then choose to publish another packet, request a packet, or disconnect the call.

The invention describes an exchange where the traded commodities are digital information packets. The digital information packets consist of a wide variety of different types of data. A relatively large number of publishers can make available a number of different data types to an equally wide variety of subscribers. The subscribers, via their modular expandable units with menu-driven software, can specify which digital information packets they would like to receive, in which format they would like to receive the data, and whichever transmission media they may prefer. Once the exchange is made aware of the subscriber's request, it sends the requested digital information packet to the subscriber. The exchange system records information about all the publication/subscription transactions and bills the publishers and subscribers accordingly.

WHAT IS CLAIMED IS:

1. A system for the exchange of digital information packets, comprising:

an exchange including a plurality of connectors for
5 interfacing said exchange to a plurality of transmission media;

a plurality of modular expandable units, each of said plurality of modular expandable units having at least one input source terminal, at least one output
10 terminal, and a central processing unit between said at least one input and said at least one output terminals; and

at least one transmission medium;

wherein said plurality of modular expandable units
15 are connected to said exchange through said transmission medium to allow the first transfer of a user-selected amount and type of digital information from a first one of said plurality of modular expandable units to a second one of said plurality of modular expandable units,

and wherein said plurality of modular expandable
20 units are connected to said exchange through said transmission medium to allow the second transfer of a user-selected amount and type of digital information from the second one of said plurality of modular expandable units to at least a third one of said plurality of
25 modular expandable units,

such that said first one of said plurality of modular expandable units is capable of transferring data to said second one of said plurality of modular
30 expandable units over two transmission media simultaneously.

2. The system for the exchange of digital information packets of claim 1, wherein said input source
35 terminal includes a module selected from plurality of expansion modules, each of which can accommodate one variety of signal input.

3. The system for the exchange of digital information packets of claim 1, wherein said output terminal include a module selected from a plurality of available expansion modules, each of which can accommodate one variety of signal output.

4. The system for the exchange of digital information packets of claim 1, wherein said central processing unit includes:

10 software running on a microprocessor suitable for selecting digital information;

a system for entering commands;

an input;

an output; and

15 a serial line;

such that said serial line connects said at least one input to said at least one output.

5. The system for the exchange of digital information packets of claim 1, wherein said central processing unit includes:

20 software suitable for selecting digital information;

a system for entering commands; and

a parallel line;

25 such that said parallel line connects said at least one input to said at least one output.

6. The system for the exchange of digital information packets of claim 1, further comprising:

30 an information buffer connected to said expandable module;

such that said information buffer allows for the asynchronous communication of digital information between said exchange and one of said two modular expandable

35 units over said transmission medium.

7. The system for the exchange of digital information packets of claim 1, further comprising:

an information buffer connected to said exchange;
such that said information buffer allows for the
5 asynchronous communication between said exchange and one
of said two modular expandable units over said
transmission medium of digital information.

8. A method for the exchange of digital information
10 packets, comprising:

(a) creating a digital information packet wherein
the packet includes:

(i) a series string of data representing
desired information;

15 (ii) a publisher address, corresponding to the
location of a publisher creating said digital information
packet;

(iii) a digital information packet directory
entry, corresponding to a publishable address which is be
20 used to locate and order said particular digital
information packet;

(b) transmitting said digital information packet
directory entry and said publisher address from a modular
expandable unit to an exchange over a transmission
25 medium;

(c) publishing said digital information packet
directory entry and said publisher address over the
exchange by filing and cataloguing, according to subject
matter and type of medium supported, said digital
30 information packet directory entry and said publisher
address;

(d) compiling a list of said digital information
packet directory entries and corresponding said publisher
addresses;

35 (e) making available said list to subscribers with
modular expandable units;

(f) locating a particular desired digital information packet by choosing one of said digital information packet directory entries from said compiled list over said exchange by using another modular expandable unit;

(g) subscribing to said digital information packet over said exchange by using one of said modular expandable units and providing information to said exchange, including:

(i) subscriber address where said digital information packet is to be sent;

(ii) the publisher address where said digital information packet is to be sent from;

(iii) the digital information packet directory entry where said digital information packet is stored;

(h) transferring said digital information packet from said publisher to said subscriber over said transmissions medium;

(i) concurrent with step (h), buffering said transfer of said digital information packet from said publisher to said subscriber such that said transfer occurs asynchronously.

9. The method of claim 8, wherein said steps of buffering of said transfer of said digital information packet is performed by both said publisher's and said subscriber's modular expandable units.

10. The method of claim 8, wherein said desired information is analog data which is then converted to digital form by an expansion module forming part of the modular expandable unit to provide said series string of data.

11. The method of claim 8 comprising the further step of:

storing said transferred digital information packet in a static semiconductor memory.

5 12. The method of claim 8 comprising the further step of:

storing said transferred digital information packet on a magnetic medium.

10 13. The method of claim 8 comprising the further step of:

playing said transferred digital information packet on a device appropriate to that data type.

15 14. The method of claim 8 comprising the further step of:

billing said subscriber for the transfer and price of said transferred digital information packet.

20 15. The method of claim 8 comprising the further step of:

billing said subscriber by said exchange for the transfer and price of said transferred digital information packet.

25 16. The method of claim 8, wherein said step of creating said digital information packet, occurs at the same time as said step of transferring of said digital information packet,

30 such that said transfer can be effected for real-time transmission of contemporaneously created data.

17. The method of claim 8, wherein data compression techniques are utilised to speed said transfer of said digital information packet.

35 18. The system for the exchange of digital information packets of claim 1, further comprising an

expansion module coupled to said input source terminal, said expansion module accommodating a particular variety of signal input.

5 19. The system for the exchange of digital information packets of claim 1, wherein said exchange may be communicably connected to another exchange.

10 20. A system for the exchange of digital information packets, comprising:

 an exchange including a plurality of connectors for interfacing said exchange to a plurality of transmission media;

15 a plurality of modular expandable units, each of said plurality of modular expandable units having at least one input source terminal, at least one output terminal, and a central processing unit between said at least one input and said at least one output terminals; and

20 at least one transmission medium;

 wherein said plurality of modular expandable units are connected to said exchange through said transmission medium to allow the first transfer of a user-selected amount and type of digital information from a first one of said plurality of modular expandable units to a second one of said plurality of modular expandable units,

25 and wherein said plurality of modular expandable units are connected to said exchange through said transmission medium to allow the second transfer of a user-selected amount and type of digital information from the second one of said plurality of modular expandable units to at least a third one of said plurality of modular expandable units,

30 such that said first one of said plurality of modular expandable units transfers data to said second one of said plurality of modular expandable units over at least two transmission media simultaneously.

21. A system for the exchange of digital information packages comprised of:

an exchange including a plurality of modular expandable units (MEUs), where each of said MEUs includes:

a subsystem of circuitry having a plurality of IC's and memory devices;

a control bus connected to and used in tandem with said subsystem;

wherein said control bus provides regulated coherent access to at least one wide bandwidth high clock speed data bus such that said data is physically and logically separated within each of said MEU devices;

a plurality of expansion module interfaces, each of said interfaces providing a connection between said control bus and said data bus;

wherein said connection is dynamically completed or broken by said subsystem in accordance with requests transmitted over said control bus;

a plurality of connectors for interfacing said MEUs to a plurality of transmission media;

wherein said MEUs are connected to said exchange through said plurality of transmission media to allow the transfer of digital information from any one of said MEUs to any other of said MEUs.

22. The system for the exchange of digital information packets of claim 21 wherein one of said plurality of expansion modules transmits and receives information by said data bus and an external interface.

23. The system for the exchange of digital information packets of claim 22, wherein said expansion module further comprises:

a microprocessor; and

a memory device;

said microprocessor, said memory device, and said external connection operating in a first condition to convert digital information received from at least one external source connected to said external interface to a format to be transmitted to said expansion module interface;

and operating in a second condition to convert digital information transmitted away from said expansion module interface to a format to be received by at least one external device.

24. The system for the exchange of digital information packets of claim 21 wherein said subsystem is used to control said microprocessor.

25. The system for the exchange of digital information packets of claim 21 wherein said transmission media is any assembly capable of transmitting digital information.

26. The central processing unit of claim 4 where said software is microcode.

27. The central processing unit of claim 4 wherein said software is stored in EPROM.

28. The system of claim 21 wherein at least one of said MEUs is connected directly to at least one other of said MEUs over one transmission medium.

29. The system of claim 28 wherein at least one of said MEU's is connected directly to at least one other of said MEU's over at least two transmission media.

30. The system of claim 1, further comprising means for virtual menuing.

41

31. The system of claim 21, further comprising means for virtual menuing.

5

10

15

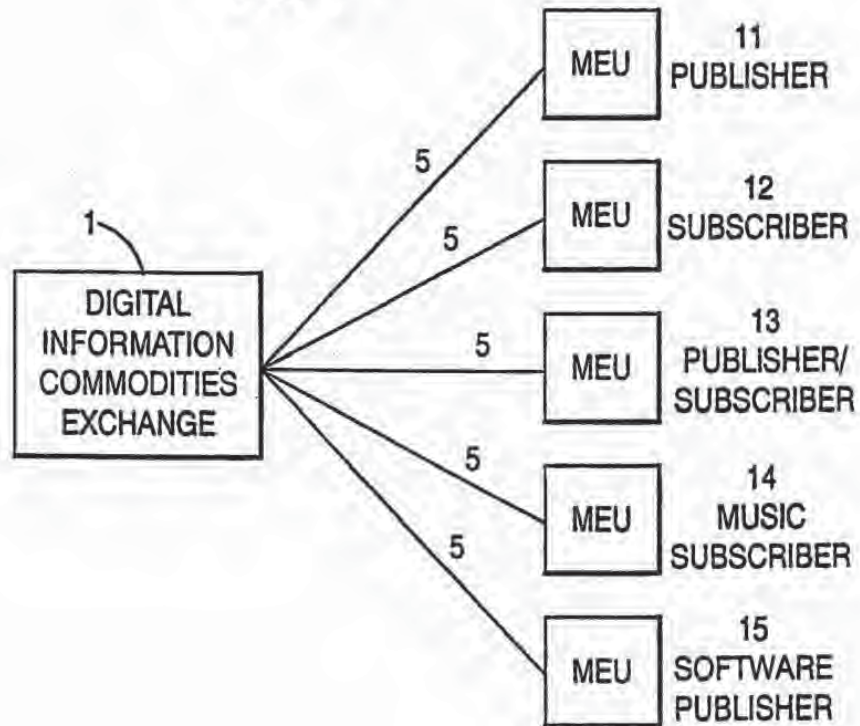
20

25

30

35

FIG. 1



SUBSTITUTE SHEET (RULE 26)

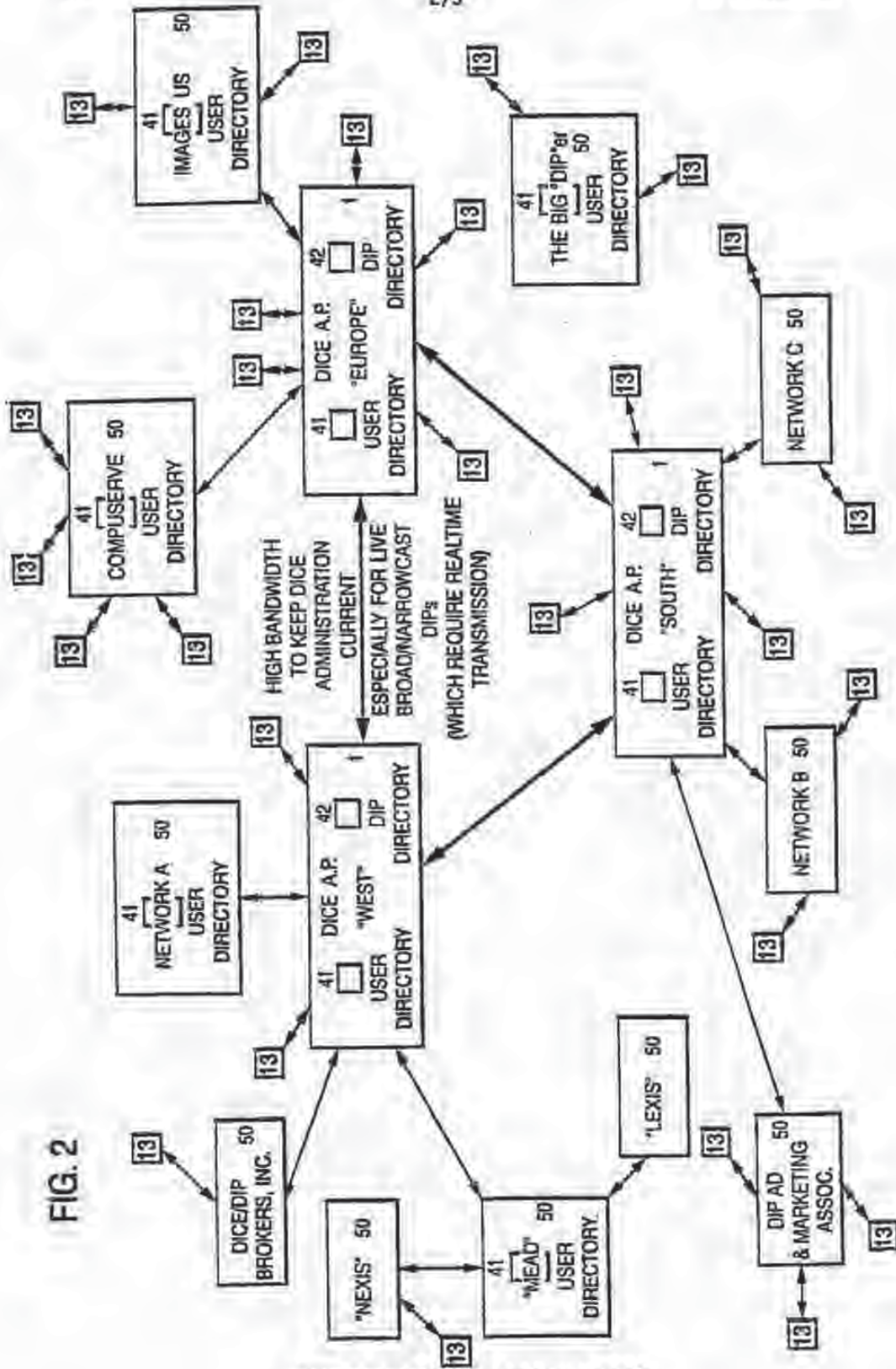


FIG. 2

SUBSTITUTE SHEET (RULE 26)

FIG. 3

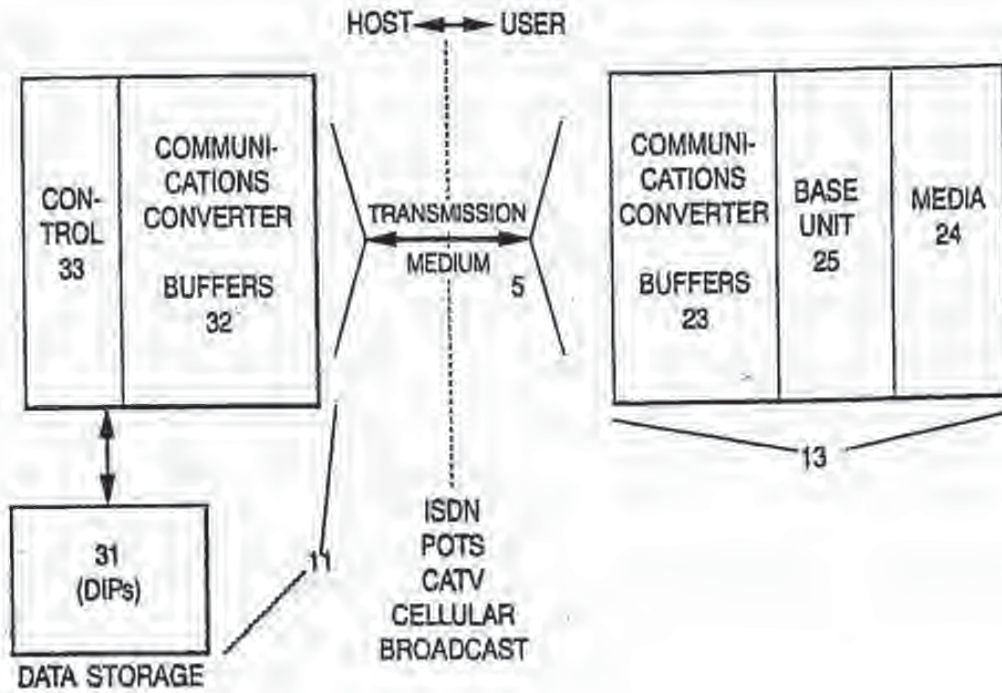
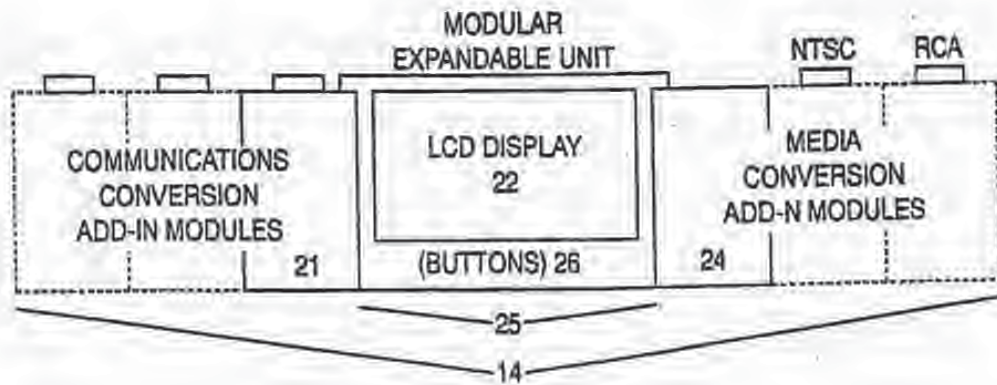


FIG. 4



SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08159

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) : H04B 13/00; H04J 3/26; H04L 12/40 US CL : 370/60, 85.11, 85.11; 375/260 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. : J70/32, 53, 54, 58.1, 58.2, 60, 60.1, 61, 62, 85.1, 85.11, 94.1; 375/257, 260, 267; 348/6, 7, 8, 10, 12, 16; 379/110, 219, 220 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)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,491,983, (PINNOW et al) 01 January 1985, col. 3, lines 22-45, col. 4, lines 16-33, col. 4, line 44 to col. 5, line 20.	1-7, 18-20, 26-27 and 30
Y	US, A, 4,958,341 (HEMMADY et al) 18 September 1990, col. 6, lines 4-59 and figure 2.	1-7, 18-20, 26-27 and 30
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: *A* documents defining the general state of the art which is not considered as to part of particular relevance *E* earlier document published on or after the international filing date *L* documents 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 *Z* document member of the same patent family		
Date of the actual completion of the international search 13 SEPTEMBER 1995		Date of mailing of the international search report 17 NOV 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3220		Authorized officer HUY D. VU <i>B. Harder for</i> Telephone No. (703) 305-6602

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08159**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Telephone Practice

- I. Claims 1-7, 18-20, 26-27 and 30, drawn to an apparatus for exchanging information packets between plurality of modules expandable units over two transmission media. (375/260)
- II. Claims 8-17, drawn to a method for publishing directory entries and publisher address. (375/260)
- III. Claims 21-25, 28-29 and 31, drawn to a bus transmission system having a data bus and a separate control bus. (370/85.11)

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04L</p>	<p>A2</p>	<p>(11) International Publication Number: WO 96/42151 (43) International Publication Date: 27 December 1996 (27.12.96)</p>
<p>(21) International Application Number: PCT/US96/10257 (22) International Filing Date: 7 June 1996 (07.06.96) (30) Priority Data: 08/489,172 9 June 1995 (09.06.95) US (71) Applicant: THE DICE COMPANY [US/US]; P.O. Box 60471, Palo Alto, CA 94306-0471 (US). (72) Inventors: COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US). MOSKOWITZ, Scott, A.; Townhouse 4, 20191 East Country Club Drive, North Miami Beach, FL 33180 (US). (74) Agents: ALTMILLER, John, C. et al; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).</p>	<p>(81) Designated States: CA, CN, FI, JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>Without international search report and to be republished upon receipt of that report.</i></p>	
<p>(54) Title: STEGANOGRAPHIC METHOD AND DEVICE</p> <p>(57) Abstract</p> <p>An apparatus and method for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

STEGANOGRAPHIC METHOD AND DEVICE

Definitions

- 5 Several terms of art appear frequently in the following. For ease of reference they are defined here as follows:

“Content” refers to multimedia content. This term encompasses the various types of information to be processed in a multimedia entertainment system. Content
10 specifically refers to digitized audio, video or still images in the context of this discussion. This information may be contained within files on a multimedia computer system, the files having a particular format specific to the modality of the content (sound, images, moving pictures) or the type of systems, computer or otherwise, used to process the content.

15 “Digitized” refers to content composed of discrete digital samples of an otherwise analog media, which approximate that media inside a computer or other digital device. For instance, the sound of music occurs naturally, and is experienced by humans as an analog (continuous) sound wave. The sound can be digitized into a
20 stream of discrete samples, or numbers, each of which represents an approximate

value of the amplitude of the real analog wave at a particular instant in time. These samples can be stored in files in a computer and then used to recreate the original sound wave to a high degree of accuracy.

In general, content entering a digital system is digitized by Analog to Digital converters (A/D) and analog media are recreated by the digital system using a Digital to Analog (D/A) converter. In the context of this discussion content is always digitized content.

"Cryptography" is a field covering numerous techniques for scrambling information conveying messages so that when the message is conveyed between the sender and receiver an unintended party who intercepts this message cannot read it, or extract useful information from it.

A "Public Key Cryptosystem" is a particular cryptographic system where all parties possess pairs of keys for encryption and decryption. Parties to this type of system freely distribute their public keys, which other may use to encrypt messages to the owner of the public key. Such messages are decrypted by the receiver with the private key. Private keys are never distributed. A message encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. A message encrypted with a private key is said to have been signed by the owner of that key. Anyone in possession of the public key may decrypt the message and know that it was encrypted, and thus signed, by the owner of the public key, since only they possess the corresponding private key.

"Steganography" is a field distinguished from cryptography, but associated with it, that covers numerous methods for hiding an informational message within some other medium, perhaps another unrelated message, in such a manner that an unintended party who intercepts the medium carrying the hidden message does not know it contains this hidden message and therefore does not obtain the information in the hidden message. In other words, steganography seeks to hide messages in plain view.

Background of the Invention

5 In the current environment of computer networks and the proliferation of digital or digitized multimedia content which may be distributed over such networks, a key issue is copyright protection. Copyright protection is the ability to prevent or deter the proliferation of unauthorized copies of copyrighted works. It provides a reasonable guarantee that the author of a copyrighted work will be paid for each copy of that work.

10 A fundamental problem in the digital world, as opposed to the world of physical media, is that a unlimited number of perfect copies may be made from any piece of digital or digitized content. A perfect copy means that if the original is comprised of a given stream of numbers, then the copy matches the original, exactly, for each number in the stream. Thus, there is no degradation of the original signal during the copy operation. In an analog copy, random noise is always introduced, degrading the copied signal.

20 The act of making unlicensed copies of some content, digital or analog, whether audio, video, software or other, is generally known as *piracy*. Piracy has been committed for the purpose of either profit from the sale of such unlicensed copies, or to procure for the "pirate" a copy of the content for personal use without having paid for it.

25 The problem of piracy has been made much worse for any type of content by the digitization of content. Once content enters the digital domain, an unlimited number of copies may be made without any degradation, if a pirate finds a way to break whatever protection scheme was established to guard against such abuses, if any. In the analog world, there is generally a degradation in the content (signal) with each successive copy, imposing a sort of natural limit on volume of piracy.

30

To date, three general types of schemes have been implemented in an attempt to protect copyrights.

- 1) Encryption
- 5 2) Copy Protection
- 3) Content Extensions

Copy Protection and Content Extensions generally apply in the digital world only, while a scheme related to Encryption, commonly known as scrambling, may be applied to an analog signal. This is typical in analog cable systems.

Encryption scrambles the content. Before the content is made ready for delivery, whether on floppy disk, or over a network, it must be encrypted, or scrambled. Once the content has been encrypted, it cannot be used until it is decrypted, or
15 unscrambled. Encrypted audio data might sound like incomprehensible screeching, while an encrypted picture or video might appear as random patterns on a screen. The principle of encryption is that you are free to make as many copies as you want, but you can't read anything that makes sense until you use a special key to decrypt, and you can only obtain the key by paying for the content.

20 Encryption has two problems, however. 1) Pirates have historically found ways to crack encryption, in effect, obtaining the key without having paid for it; and 2) Once a single legitimate copy of some content has been decrypted, a pirate is now free to make unlimited copies of the decrypted copy. In effect, in order to sell an
25 unlimited quantity of an encrypted piece of software, the pirate could simply buy one copy, which they are entitled to decrypt.

Copy Protection includes various methods by which a software engineer can write the software in a clever manner to determine if it has been copied, and if so to
30 deactivate itself. Also included are undocumented changes to the storage format of the content. Copy protection was generally abandoned by the software industry.

since pirates were generally just as clever as the software engineers and figured out ways to modify their software and deactivate the protection. The cost of developing such protection was not justified considering the level of piracy which occurred despite the copy protection.

5

Content Extension refers to any system which attaches some extra information to the original content which indicates whether or not a copy may be made. A software or hardware system must be specifically built around this scheme to recognize the additional information and interpret it in an appropriate manner. An example of such a system is the Serial Copyright Management System embedded in Digital Audio Tape (DAT) hardware. Under this system, additional information is stored on the disc immediately preceding each track of audio content which indicates whether or not it can be copied. The hardware reads this information and uses it accordingly.

15

A fundamental problem with Encryption and Content Extension is the "rogue engineer". An employee who helped design such a system or an individual with the knowledge and means to analyze such a system can modify it to ignore the copyright information altogether, and make unlicensed copies of the content. Cable piracy is quite common, aided by illicit decoder devices built by those who understand the technical details of the cable encryption system. Although the cable systems in question were actually based on analog RF signals, the same principle applies to digital systems.

20

The practical considerations of weak encryption schemes and rogue engineers have served to limit the faith which may be put in such copyright protection schemes. The invention disclosed herein serves to address these problems with conventional systems for digital distribution. It provides a way to enforce copyright online. The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended

30

parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. The message itself is encrypted which serves to further protect the message, verify the validity of the message, and redistribute the information in a random manner so that anyone attempting to locate the message without the keys cannot rely on pre-supposed knowledge of the message contents as a help in locating it.

Summary of the Invention

The invention disclosed herein combines two techniques, steganography - obscuring information that is otherwise in plain sight, and cryptography - scrambling information that must be sent over unsecured means, in a manner such that only the intended recipient may successfully unscramble it. The net effect of this system is to specifically watermark a piece of content so that if it is copied, it is possible to determine who owned the original from which the copies were made, and hence determine responsibility for the copies. It is also a feature of the system to uniquely identify the content to which it is applied.

For a comprehensive discussion of cryptography, its theory, applications and specific algorithms, see *APPLIED CRYPTOGRAPHY*, by Bruce Schneier, which is herein incorporated by reference at pages 66-68, 387-392.

Steganography is discussed briefly in *THE CODE BREAKERS* by David Kahn, which is herein incorporated by reference at pages xiii, 81-83, 522-526, and 873. An example application, Stego by Romana Machado, is also available for the Apple Macintosh. Stego can be found at the internet uniform resource locator "<http://mamex.aim.stanford.edu/info-misc/emp/stego10a2.htm>". This application demonstrates a simple

steganographic technique to encode a text message into a graphical image without significantly distorting the image.

5 The invention improves upon the prior art by providing a manner for protecting copyright in the digital domain, which neither steganography or cryptography does. It improves specifically on steganography by making use of special keys which dictate exactly where within a larger chunk of content a message is to be hidden, and makes the task of extracting such a message without the proper key the equivalent of looking for a needle in a haystack.

10 The information encoded by the Stega-Cipher process serves as a watermark which identifies individual copies of content legally licensed to specific parties. It is integral with the content. It cannot be removed by omission in a transmission. It does not add any overhead to signal transmission or storage. It does allow the content to be stored to and used with traditional offline analog and digital media, without modification or significant signal degradation. These aspects of the stega-cipher all represent improvements to the art. That is, its forces would - be pirates to damage the content in order to guarantee the disabling of the watermark.

20 The invention described herein is used for protecting and enforcing copyrights in the digital or on-line domain, where there are no physical limitations on copying copyrighted content.

25 The invention uniquely identifies every copy of multimedia content made using the invention, composed of digitized samples whether compressed or uncompressed, including but not limited to still digital images, digital audio, and digital video.

30 The invention is for use in meterware or pay-by-use systems where an online user incurs a charge each time they access a particular piece of content, or uses a software title.

8

The invention is for use as a general improvement to cryptographic techniques to increase the complexity of cryptanalysis on a given cipher.

5 It is considered that the method and steps of the present invention will be modified to account for the effects of loss compression schemes on the samples and particularly includes modification to handle MPEG compressed audio and video.

10 It is considered that statistical data spreading and recovery techniques, error coding or spread spectrum processing techniques might be applied in the invention to handle the effects of loss compression, or counter the effects of a randomization attack.

15 It is considered that the apparatus described might be further specialized and optimized in hardware by replacing general purpose data buses and CPU or DSP driven operations with hardwired circuitry, incorporated in one or more special purpose ICs.

20 It is considered that the apparatus will be modeled and implemented in software on general purpose computer platforms.

It is considered that stega-cipher hardware could be embedded in a consumer electronics device and used to not only identify content and copyright, but to enable use of that content.

25 Detailed Description

L Digital Copyright Stega-Cipher Protocol and the Decode/Encode Program

30 The purpose of the program described here is to watermark digital multimedia content for distribution to consumers through online services in such a way as to meet the following criteria

Given a unique piece of multimedia content, composed of digitized samples, it is desirable to:

- 5 1) Uniquely identify this particular piece of content from others in a manner which is secure and undeniable (e.g. to know whether a digital audio recording is "My Way" by Frank Sinatra, or "Stairway to Heaven", by Led Zeppelin), and in a manner such that this identification can be performed automatically by an electronic device or mechanism.
- 10 2) Uniquely identify the copyright owner of the content, and the terms under which it may be distributed in general, in a manner which is secure and undeniable.
- 15 3) At such time as is necessary, additionally, uniquely identify in a secure and undeniable manner the licensed publisher who received a particular copy of the content, and the terms under which they may redistribute or resell it.
- 20 4) At such time as is necessary, additionally, uniquely identify in a secure and undeniable manner, the licensed subscriber who received a particular copy of the content from the publisher described in item 3.

20 The program described in more detail below combines the techniques of cryptography and steganography to hide a securely encrypted digital copyright certificate which contains information satisfying the criteria listed above, in such a manner as to be integral with the content, like a watermark on paper, so that

25 possession of the content dictates possession of the watermark information. In addition, the watermark cannot be "found" or successfully decoded, without possession of the correct "masks" or keys, available only to those legitimately authorized, namely, those parties to a commercial transaction involving the sale of a copy of the content. Finally, the ability to distribute such watermarked content in a

30 system which implements the watermark scheme is denied without a successfully decoded watermark. Because well known and tested cryptographic techniques are

used to protect the certificate itself, these certificates are virtually impossible to forge. Finally, the watermark cannot be erased without significantly damaging the content.

- 5 The basic program represents a key part of the invention itself. This program is then used as the method by which copyright information is to be associated in an integral manner with the content. This is a concept absent from copy protection, encryption and content extension schemes. The copyright information itself can be made undeniable and unforgeable using cryptographic techniques, so that through it an
- 10 audit trail of ownership may be established for each copy of a given piece of content, thus customizing each copy to a particular owner, in a way that can be used to identify the owner.

The value of the stega-cipher is that it provides a way to watermark the content in a way that changes it slightly, but does not impact human perception significantly.

15 And, furthermore, that it is made difficult to defeat since one must know exactly where the information resides to extract it for analysis and use in forgery attempts, or to remove it without overly degrading the signal. And, to try to forge copyright information one must first be able to analyze the encrypted copyright information,

20 and in order to do that, one must be able to find it, which requires masks.

II. Example Embodiment of General Processing

Digital audio data is represented by a series of samples in 1 dimension,

25

$$\{S_1, S_2, S_3, \dots, S_n\}$$

This series is also referred to as a sample stream. The sample stream approximates an analog waveform of sound amplitude over time. Each sample represents an

30 estimate of the wave amplitude at the instant of time the sample is recorded. For monaural audio, there is one such sample stream. Stereo audio is comprised of two

sample streams, one representing the right channel, and the other representing the left. Each stream is used to drive a corresponding speaker to reproduce the stereo sound.

- 5 What is referred to as CD quality audio is characterized by 16 bit (2 byte) stereo samples, recorded at 44.1 KHz, or 44,100 samples per second in each channel. The dynamic range of sound reproduction is directly proportional to the number of bits per sample. Some lower quality recordings are done at 8 bits. A CD audio recording can be stored using any scheme for containing the 2 sample streams in
 10 their entirety. When these streams are played back at the same frequency they were recorded at, the sound recorded is reproduced to a high degree of accuracy.

The sample stream is processed in order from first sample to last. For the purpose of the invention disclosed, the stream is separated into sample windows, each of
 15 which has a fixed number of consecutive samples from the stream, and where windows do not overlap in the sample stream. Windows may be contiguous in the sample stream. In this discussion assume each window contains 128 samples, and that windows are contiguous. So, the windows within the stream look like

20
$$\{ [S_1, S_2, S_3 \dots S_{128}], [S_{129}, S_{130}, S_{131} \dots S_{256}], \dots [S_{n-128} \dots S_n] \}$$

where [...] denotes each window and any odd samples at the end of the stream which do not completely fill a window can be ignored, and simply passed through the system unmodified.

- 25 These windows will be used as input for the discrete Fast Fourier Transform (and its inverse) operation.

Briefly, Fourier Transform methods are based on the principle that a complex waveform, expressed as amplitude over time and represented by a sample stream, is
 30 really the sum of a number of simple waveforms, each of which oscillate at different frequencies.

By complex, it is meant that the value of the next sample is not easily predicted from the values of the last N samples or the time of the sample. By simple it is meant that the value of the sample is easily predictable from the values of the last N samples and/or the time of the sample.

5

The sum of multiple simple waves is equivalent to the complex wave. The discrete FFT and its inverse simply translate a limited amount of data from one side of this equivalence to the other, between the complex waveform and the sum of simple waves. The discrete FFT can be used to translate a series of samples representing amplitude over time (the complex wave, representing a digital audio recording) into the same number of samples representing total spectral energy in a given range of frequencies (the simple wave components) at a particular instant of time. This instant is the time in the middle of the original amplitude/time samples. The inverse discrete FFT translates the data in the other direction, producing the complex waveform, from its simpler parts.

10
15

Each 128 sample window will be used as an input to the discrete FFT, resulting in 128 bins representing each of 128 frequency bands, ranging from 0Hz to 22Khz (the Nyquist frequency, or $\frac{1}{2}$ the sampling rate).

20

Information can be encoded into the audio signal in the frequency domain or in the time domain. In the latter case, no FFT or inverse FFT is necessary. However, encoding in the frequency domain is recommended, since its effects are scattered over the resultant time domain samples, and not easily predicted. In addition, frequency domain encoding makes it more likely that randomization will result in noticeable artifacts in the resultant signal, and therefore makes the stega-cipher more defensible against such attacks. It is in the frequency domain that additional information will be encoded into the audio signal for the purpose of this discussion. Each frequency band in a given time slice can potentially be used to store a small portion of some additional information to be added to the signal. Since these are discrete estimates, there is some room for error which will not significantly effect

25
30

the perceived quality of the signal, reproduced after modification, by the inverse FFT operation. In effect, intentional changes, which cannot be distinguished from random variations are introduced in the frequency domain, for the purpose of storing additional information in the sample stream. These changes are minimized so as not to adversely affect the perceived quality of the reproduced audio signal, after it has been encoded with additional information in the manner described below. In addition, the location of each of these changes is made virtually impossible to predict, an innovation which distinguishes this scheme from simple steganographic techniques.

Note that this process differs from the Nagata, et al. patents, 4,979,210 and 5,073,925, which encode information by modulating an audio signal in amplitude/time domain. It also differs in that the modulations introduced in the Nagata process (which are at very low amplitude and frequency relative to the carrier wave as to remain inaudible) carry only copy/ don't copy information, which is easily found and circumvented by one skilled in the art. Also, there is no limitation in the stega-cipher process as to what type of information can be encoded into the signal, and there is more information storage capacity, since the encoding process is not bound by any particular frequency of modulation but rather by the number of samples available. The granularity of encoding in the stega-cipher is determined by the sample window size, with potentially 1 bit of space per sample or 128 bits per window (a secure implementation will halve this to 64 bits). In Nagata, et al. the granularity of encoding is fixed by the amplitude and frequency modulation limits required to maintain inaudibility. These limits are relatively low, and therefore make it impractical to encode more than simple copy/ don't copy information using the Nagata process.

III. Example Embodiment of Encoding and Decoding

5 A modification to standard steganographic technique is applied in the frequency domain described above, in order to encode additional information into the audio signal.

In a scheme adapted from cryptographic techniques, 2 keys are used in the actual encode and decode process. For the purposes of this invention the keys are referred to as masks. One mask, the primary, is applied to the frequency axis of FFT results, the other mask is applied to the time axis (this will be called the convolution mask). The number of bits comprising the primary mask are equal to the sample window size in samples (or the number of frequency bands computed by the FFT process), 128 in this discussion. The number of bits in the convolution mask are entirely arbitrary. This implementation will assume a time mask of 1024 bits. Generally the larger the key, the more difficult it is to guess.

Prior to encoding, the primary and convolution masks described above are generated by a cryptographically secure random generation process. It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in decoding, should that step become necessary.

25 Prior to encoding, some additional information to be encoded into the signal is prepared and made available to the encoder, in a bit addressable manner (so that it may be read one bit at a time). If the size of the sample stream is known and the efficiency characteristics of the stega-cipher implementation are taken into account, a known limit may be imposed on the amount of this additional information.

30 The encoder captures one sample window at a time from the sample stream, in sequential, contiguous order. The encoder tracks the sequential number of each

window it acquires. The first window is 0. When the number of windows processed reaches the number of bits in the window mask, minus one, the next value of the window counter will be reset to 0.

- 5 This counter is the convolution index or phase. In the current implementation it is used as a simple index into the convolution bitmask. In anticipated developments it will be used to perform convolution operations on the convolution mask to determine which bit to use. For instance the mask might be rotated by a number corresponding to the phase, in bits to the left and XORed with the primary mask to
- 10 produce a new mask, which is then indexed by the phase. There are many possibilities for convolution.

The encoder computes the discrete FFT of the sample window.

- 15 Starting with the lowest frequency band, the encoder proceeds through each band to the highest, visiting each of the 128 frequency bands in order. At each band value, the encoder takes the bit of the primary mask corresponding to the frequency band in question, the bit of the convolution mask corresponding to the window in question, and passes these values into a boolean function. This function is designed
- 20 so that it has a near perfectly random output distribution. It will return true for approximately 50% of its input permutations, and false for the other 50%. The value returned for a given set of inputs is fixed, however, so that it will always return the same value given the same set of inputs.
- 25 If the function returns true, the current frequency band in the current window is used in the encoding process, and represents a valid piece of the additional information encoded in the signal. If the function returns false, this cell, as the frequency band in a given window is called, is ignored in the process. In this manner it is made extremely difficult to extract the encoded information from the signal
- 30 without the use of the exact masks used in the encoding process. This is one place in which the stega-cipher process departs from traditional steganographic

implementations, which offer a trivial decode opportunity if one knows the information is present. While this increases the information storage capacity of the carrier signal, it makes decoding trivial, and further degrades the signal. Note that it is possible and desirable to modify the boolean cell flag function so that it returns true < 50% of the time. In general, the fewer cells actually used in the encode, the more difficult they will be to find and the less degradation of content will be caused, provided the function is designed correctly. There is an obvious tradeoff in storage capacity for this increased security and quality.

5
10
15
20
The encoder proceeds in this manner until a complete copy of the additional information has been encoded in the carrier signal. It will be desirable to have the encoder encode multiple copies of the additional information continuously over the duration of the carrier signal, so that a complete instance of this information may be recovered from a smaller segment of a larger signal which has been split into discontinuous pieces or otherwise edited. It is therefore desirable to minimize the size of the information to be encoded using both compact design and pre-encoding compression, thus maximizing redundant encoding, and recoverability from smaller segments. In a practical implementation of this system it is likely the information will be first compressed by a known method, and then encrypted using public-key techniques, before being encoded into the carrier signal.

25
30
The encoder will also prepare the package of additional information so that it contains an easily recognizable start of message delimiter, which can be unique to each encoding and stored along with the keys, to serve as a synchronization signal to a decoder. The detection of this delimiter in a decoding window signifies that the decoder can be reasonably sure it is aligned to the sample stream correctly and can proceed in a methodic window by window manner. These delimiters will require a number of bits which minimizes the probability that this bit sequence is not reproduced in a random occurrence, causing an accidental misalignment of the decoder. A minimum of 256 bits is recommended. In the current implementation 1024 bits representing a start of message delimiter are used. If each sample is

random, then each bit has a 50% probability of matching the delimiter and the conditional probability of a random match would be $1/2^{1024}$. In practice, the samples are probably somewhat less than random, increasing the probability of a match somewhat.

5

The decode process uses the same masks in the same manner, only in this case the information is extracted one bit at a time from the carrier signal.

The decoder is assumed to have access to the proper masks used to encode the information originally. These masks might be present in a database, which can be indexed by a value, or values computed from the original content, in a manner insensitive to the modifications to the content caused by the stega-cipher process. So, given an arbitrary piece of content, a decoder might first process the content to generate certain key values, and then retrieve the decode masks associated with the matching key values from the database. In the case where multiple matches occur, or none are found, it is conceivable that all mask sets in the database could be tried sequentially until a valid decode is achieved, or not, indicating no information is present.

10
15
20
25
In the application of this process, it is anticipated that encoding operations may be done on a given piece of content up to 3 times, each adding new information and using new masks, over a sub-segment of the content, and that decode operations will be done infrequently. It is anticipated that should it become necessary to do a search of a large number of masks to find a valid decode, that this process can be optimized using a guessing technique based on close key matching, and that it is not a time critical application, so it will be feasible to test large numbers of potential masks for validity on a given piece of content, even if such a process takes days or weeks on powerful computers to do a comprehensive search of known mask sets.

30
The decode process is slightly different in the following respect. Whereas the encoding process can start at any arbitrary point in the sample stream, the decode

process does not know where the encode process began (the exact offset in samples to the start of the first window). Even though the encode process, by convention, starts with sample 0, there is no guarantee that the sample stream has not been edited since encoding, leaving a partial window at the start of the sample stream, and thus requiring the decoder to find the first complete window to start the decode. Therefore, the decode process will start at the first sample, and shift the sample window along by 1 sample, keeping the window index at 0, until it can find a valid decode delimiter encoded in the window. At this point, the decoder knows it has synchronized to the encoder, and can then proceed to process contiguous windows in a more expedient manner.

Example Calculations based on the described implementation for adding copyright certificate information to CD quality digital audio:

- 15 In a stream of samples, every 128 samples will contain, on average 64 bits of certificate related information. Digital audio is composed of 16 bit samples, at 44.1 Khz, or 44,100 samples per second. Stereo audio provides 2 streams of information at this rate, left and right, or 88,200 samples per second. That yields approximately 689 contiguous sample windows (of 128 samples) per second in which to encode information. Assume a song is 4 minutes long, or 240 seconds. This yields $240 * 689 = 165,360$ windows, which on average (50% utilization) contain 64 bits (8 bytes) each of certificate information. This in turns gives approximately 1291Kb of information storage space per 4 minute stereo song (1.2 MB). There is ample room for redundant encoding of information continuously over the length of the content.
- 25 Encoding 8 bytes for every 256 bytes represents 3.1% of the signal information. Assuming that a copyright certificate requires at most approximately 2048 bytes (2K), we can encode the same certificate in 645 distinct locations within the recording, or approximately every 37/100ths of a second.
- 30 Now to account for delimiters and synchronization information. Assuming a sync marker of 1024 bits to avoid random matches, then we could prefix each 2K

- certificate block with this 1024 bit marker. It takes 256 windows to store 2K, and under this proposed scheme, the first 16 windows are reserved for the sync marker. A decoder could search for this marker by progressively matching each of the first 16 windows (64 bits at a time) against the corresponding portion of the sync marker. The decoder could reset the match advancing through the sample stream, as soon as one window did not conform to the sync marker, and proceed in this manner until it matches 16 consecutive windows to the marker, at which point it is synchronized.
- Under this scheme, 240 windows, or 1.92K remain for storing certificate information, which is not unreasonable.

IV. Possible Problems, Attacks and Subsequent Defenses

A. Randomization

- The attacker simply randomizes the least significant bits of each data point in the transform buffer, obliterating the synchronization signal and the watermark. While this attack can remove the watermark, in the context in which stega-cipher is to be used, the problem of piracy is kept to a minimum at least equal to that afforded by traditional media, since the system will not allow an unwatermarked piece of content to be traded for profit and watermarks cannot be forged without the proper keys, which are computationally difficult to obtain by brute-force or cryptanalysis. In addition, if the encoding is managed in such a way as to maximize the level of changes to the sample stream to be just at the threshold below human perception, and the scheme is implemented to anticipate randomization attempts, it is possible to force the randomization level to exceed the level that can be perceived and create destructive artifacts in the signal, in much the same manner as a VHS cassette can be manufactured at a minimal signal level, so that a single copy results in unwatchable static.

30

B. Low Bit-Depth Bitmaps (black & white images)

These bitmaps would be too sensitive to the steganization process, resulting in unacceptable signal degradation, and so are not good candidates for the stega-cipher process. The problem may be circumvented by inflating bit-depth, although
5 this is an inefficient use of space and bandwidth.

C. Non-Integer Transforms

The FFT is used to generate spectral energy information for a given audio signal. This information is not usually in integer format. Computers use methods of
10 approximation in these cases to represent the real numbers (whole numbers plus fractional amounts). Depending on the exact value of the number to be represented slight errors, produced by rounding off the nearest real number that can be completely specified by the computer occur. This will produce some randomization in the least significant bit or bits. In other words, the same operation on the same
15 sample window might yield slightly different transform values each time. It is possible to circumvent this problem using a modification to the simple LSB steganographic technique described later. Instead of looking at the LSB, the stega-cipher can use an energy quantization technique in place of the LSB method. Some variant of rounding the spectral energy values up or down, with a granularity
20 greater than the rounding error should work, without significantly degrading the output samples.

V. A Method and Protocol For Using the Stega-Cipher

25 The apparatus described in the claims below operates on a window by window basis over the sample stream. It has no knowledge of the nature of the specific message to be encoded. It merely indexes into a bit stream, and encodes as many of those bits as possible into a given sample window, using a map determined by the given
30 masks.

The value of encoding information into a single window in the sample stream using such an apparatus may not be inherently apparent until one examines the manner in which such information will be used. The protocol discussed in this section details how messages which exceed the encoding capacity of a single sample window (128 samples) may be assembled from smaller pieces encoded in the individual windows and used to defend copyrights in an online situation.

An average of 64 bits can be encoded into each window, which equals only 8 bytes. Messages larger than 8 bytes can be encoded by simply dividing the messages up and encoding small portions into a string of consecutive windows in the sample stream. Since the keys determine exactly how many bits will be encoded per window, and an element of randomness is desirable, as opposed to perfect predictability, one cannot be certain exactly how many bits are encoded into each window.

The start of each message is marked by a special start of message delimiter, which, as discussed above is 1024 bits, or 128 bytes. Therefore, if precisely 8 bytes are encoded per window, the first 16 windows of any useable message in the system described here are reserved for the start of message delimiter. For the encoder, this scheme presents little challenge. It simply designates the first sample window in the stream to be window 0, and proceeds to encode the message delimiter, bit-by-bit into each consecutive window. As soon as it has processed the last bit of the SOM delimiter it continues by encoding 32 bits representing the size, in bytes of the complete message to follow. Once the 32nd and final bit of the size is encoded, the message itself is encoded into each consecutive window, one bit at a time. Some windows may contain more encoded bits than others, as dictated by the masks. As the encoder processes each window in the content it increments its window counter. It uses this counter to index into the window mask. If the number of windows required to encode a complete message is greater than the size of this mask, 256 bits in this case, or 256 windows, then it simply resets the counter after window

255, and so on, until a complete message is encoded. It can then start over, or start on a new message.

The decoder has a bigger challenge to face. The decoder is given a set of masks, just like encoder. Unlike the encoder, the decoder cannot be sure that the first series of 128 samples it receives are the window 0 start of message, encoded by the decoder. The sample stream originally produced by an encoder may have been edited by clipping its ends randomly or splicing pieces together. In that case, the particular copy of the message that was clipped is unrecoverable. The decoder has the start of message delimiter used to encode the message that the decoder is looking for. In the initial state, the decoder assumes the first window it gets is window 0. It then decodes the proper number of bits dictated by the masks it was given. It compares these bits to the corresponding bits of the start of message delimiter. If they match, the decoder assumes it is still aligned, increments the window counter and continues. If the bits do not match, the decoder knows it is not aligned. In this case, it shifts one more sample onto the end of the sample buffer, discarding the first sample, and starts over. The window counter is set to 0. The decoder searches one sample at a time for an alignment lock. The decoder proceeds in this manner until it has decoded a complete match to the start of message delimiter or it exhausts the sample stream without decoding a message. If the decoder can match completely the start of message delimiter bit sequence, it switches into aligned mode. The decoder will now advance through the sample stream a full window at a time (128 samples). It proceeds until it has the 32 bits specifying the message size. This generally won't occupy more than 1 complete window. When the decoder has locked onto the start of message delimiter and decoded the message size, it can now proceed to decode as many consecutive additional windows as necessary until it has decoded a complete message. Once it has decoded a complete message, the state of the decoder can be reset to unsynchronized and the entire process can be repeated starting with the next 128 sample window. In this manner it is not absolutely necessary that encoding windows

be contiguous in the sample stream. The decoder is capable of handling random intervals between the end of one message and the start of another.

5 It is important to note that the circuit for encoding and decoding a sample window does not need to be aware of the nature of the message, or of any structure beyond the start of message delimiter and message size. It only needs to consider a single sample window, its own state (whether the decoder is misaligned, synchronizing, or synchronized) and what bits to encode/decode.

10 Given that the stega-cipher apparatus allows for the encoding and decoding of arbitrary messages in this manner, how can it be used to protect copyrights?

15 The most important aspect of the stega-cipher in this respect is that fact that it makes the message integral with the content, and difficult to remove. So it cannot be eliminated simply by removing certain information prepended or appended to the sample stream itself. In fact, removing an arbitrary chunk of samples will not generally defeat the stega-cipher either.

20 Given that some information can be thus integrated with the content itself, the question is then how best to take advantage of this arrangement in order to protect copyrights.

25 The following protocol details how the stega-cipher will be exploited to protect copyrights in the digital domain.

In a transaction involving the transfer of digitized content, there are at least 3 functions involved:

30 The Authority is a trusted arbitrator between the two other functions listed below, representing parties who actually engage in the transfer of the content. The Authority maintains a database containing information on the particular piece of

content itself and who the two parties engaged in transferring the content are. The Authority can perform stega-cipher encoding and decoding on content.

5 The Publisher, or online distributor is the entity which is sending the copyrighted content to another party. The Publisher can perform stega-cipher encoding and decoding on content.

10 The Consumer is the person or entity receiving the copyrighted content, generally in exchange for some consideration such as money. The consumer cannot generally perform stega-cipher encoding or decoding on content.

15 Each of these parties can participate in a message exchange protocol using well known public-key cryptographic techniques. For instance, a system licensing RSA public key algorithms might be used for signed and encrypted message exchange. This means that each party maintains a public key / private key pair, and that the public keys of each party are freely available to any other party. Generally, the Authority communicates via electronic links directly only to the Publisher and the Consumer communicates directly only with the publisher.

20 Below is an example of how the protocol operates from the time a piece of content enters an electronic distribution system to the time it is delivered to a Consumer.

25 A copyright holder (an independent artist, music publisher, movie studio, etc.) wishes to retail a particular title online. For instance, Sire Records Company might wish to distribute the latest single from Seal, one of their musical artists, online. Sire delivers a master copy of this single, "Prayer for the Dying", to the Authority, Ethical Inc. Ethical converts the title into a format suitable for electronic distribution. This may involve digitizing an analog recording. The title has now become content in the context of this online distribution system. The title is not yet available to anyone except Ethical Inc., and has not yet been encoded with the stega-cipher watermark. Ethical generates a Title Identification and Authentication

30

(TIA) certificate. The certificate could be in any format. In this example it is a short text file, readable with a small word-processing program, which contains information identifying

- 5 the title
- the artist
- the copyright holder
- the body to which royalties should be paid
- general terms for publishers' distribution
- 10 any other information helpful in identifying this content

Ethical then signs the TIA with its own private key, and encrypts the TIA certificate plus its signature with its own public key. Thus, the Ethical can decrypt the TIA certificate at a later time and know that it generated the message and that the
15 contents of the message have not been changed since generation.

Sire Records, which ultimately controls distribution of the content, communicates to the Ethical a specific online Publisher that is to have the right of distribution of this content. For instance, Joe's Online Emporium. The Authority, Ethical Inc. can
20 transmit a short agreement, the Distribution Agreement to the Publisher, Joe's Online Emporium which lists

- the content title
- the publisher's identification
- 25 the terms of distribution
- any consideration paid for the right to distribute the content
- a brief statement of agreement with all terms listed above

The Publisher receives this agreement, and signs it using its private key. Thus, any
30 party with access to the Joe's Online Emporium's public key could verify that the Joe's signed the agreement, and that the agreement has not been changed since

Joe's signed it. The Publisher transmits the signed Distribution Agreement to the Authority, Ethical Inc.

Ethical Inc. now combines the signed TIA certificate and the Distribution Agreement into a single message, and signs the entire message using its private key. Ethical has now created a Publisher Identification message to go into its own stega-cipher channel in the content. Ethical Inc. now generates new stega-cipher masks and encodes this message into a copy of the content using a stega-cipher encoder. The Authority saves the masks as a Receipt in a database, along with information on the details of the transfer, including the title, artist and publisher.

Ethical then transfers this watermarked copy to the Joe's Online Emporium, the Publisher. Well known encryption methods could be used to protect the transfer between the Authority and the Publisher. The Authority may now destroy its copy, which the Publisher has received. The Publisher, Joe's Online Emporium now assumes responsibility for any copies made to its version of the content, which is a Publisher Master copy.

Finally, the Consumer, John Q. Public wishes to purchase a copy of the content from Joe's Online Emporium. Joe's Emporium sends the John Q. Public a short agreement via an electronic communication link, similar to Publisher's Distribution Agreement, only this is a Purchase Agreement, which lists

the content title
consumer identification
the terms of distribution
the consideration pas for the content
a brief statement of agreement with the terms above

John Q. Public signs this agreement with his private key and returns it to the Joe's Online Emporium. The Publisher, Joe's prepares to encode its own stega-cipher

watermark onto a copy of the content by generating a set of masks for the algorithm. Joe's Online Emporium then stores these masks (a receipt) in its own database, indexed by title and consumer. Joe's Online Emporium signs the agreement received from John Q. Public with the Emporium's own private key, and
5 forwards it to the Authority, Ethical Inc., along with a copy of the masks. It is important to note that this communication should be done over a secured channel. The Authority verifies the Publisher and Consumer information and adds its own signature to the end of the message, approving the transaction, creating a Contract of Sale. The Authority adds the Publisher's receipt (mask set) to its database,
10 indexed by the title, the publisher, and the consumer identification. The Authority signs the Contract of Sale by encrypting it with their private key. So anyone with the Authority's public key (any Publisher) could decrypt the Contract of Sale and verify it, once it was extracted from the content. The Publisher then transmits the signed Contract of Sale back to the Publisher, who uses a stega-cipher device to
15 imprint this Contract as its own watermark over the content. The Publisher then transmits the newly watermarked copy to the Consumer, who is accepting responsibility for it. The Publisher destroys their version of the consumer's copy.

If this procedure is followed for all content distribution within such an online system
20 then it should be possible for the Authority to identify the owner of a piece of content which appears to be unauthorized. The Authority could simply try its database of stega-cipher keys to decode the watermark in the content in question. For instance, if a copy of Seal's latest single originally distributed with stega-cipher watermarks showed up on an Internet flip site the Authority should be able to
25 extract a TIA Certificate and Distribution Agreement or a Contract of Sale identifying the responsible party. If a Publisher sold this particular copy to a Consumer, that particular publisher should be able to extract a Contract of Sale, which places responsibility with the Consumer. This is not a time critical application, so even if it takes days or weeks, it is still worthwhile.

30

In a modification to the protocol discussed above, each Publisher might act as its own Authority. However, in the context of online services, this could open avenues of fraud committed by the collusion of certain Publishers and Consumers. Using an Authority, or one of several available Authorities to keep records of Publisher-
5 Consumer transactions and verify their details decreases the likelihood of such events.

It should also be obvious that a similar watermarking system could be used by an individual entity to watermark its own content for its own purposes, wether online
10 or in physical media. For instance, a CD manufacturer could incorporate unique stega-cipher watermarks into specific batches of its compact discs to identify the source of a pirate ring, or to identify unauthorized digital copies made from its discs. This is possible because the stega-cipher encoding works with the existing
15 formats of digital samples and does not add any new structures to the sample data that cannot be handled on electronic or mechanical systems which predate the stega-cipher.

VI. Increasing Confidence in the Stega-Cipher

20 The addition of a special pre-encoding process can make stega-cipher certificates even more secure and undeniable. Hash values may be incorporated which match exactly the content containing the watermark to the message in the watermark itself. This allows us a verification that the watermark decoded was encoded by
whomever signed it into this precise location in this specific content.

25 Suppose one wants to use a 256 bit (32 byte) hash value which is calculated with a secure one-way hash function over each sample in each sample window that will contain the message. The hash starts with a seed value, and each sample that would be processed by the encoder when encoding the message is incorporated into the
30 hash as it is processed. The result is a 256 bit number one can be highly confident is

unique, or sufficiently rare to make intentionally duplicating it with another series of samples difficult.

5 It is important that the hash function be insensitive to any changes in the samples induced by the stega-cipher itself. For instance, one might ignore the least significant bit of each sample when computing the hash function, if the stega-cipher was implemented using a least significant bit encode mode.

10 Based on the size of the non-hash message, one knows the hash-inclusive message requires 32 more bytes of space. One can now calculate the size of a signed encrypted copy of this message by signing and encrypting exactly as many random bytes as are in the message, and measuring the size of the output in bytes. One now knows the size of the message to be encoded. One can pre-process the sample stream as follows.

15 Proceed through the stega-cipher encode loop as described in the claims. Instead of encoding, however, calculate hash values for each window series which will contain the message, as each sample is processed. At the end of each instance of "encoding" take the resultant hash value and use it to create a unique copy of the message
20 which includes the hash value particular to the series of sample windows that will be used to encode the message. Sign and encrypt this copy of the message, and save it for encoding in the same place in the sample stream.

25 A memory efficient version of this scheme could keep on hand the un-hashed message, and as it creates each new copy, back up in the sample stream to the first window in the series and actually encode each message, disposing of it afterwards

The important result is evident on decoding. The decoding party can calculate the same hash used to encode the message for themselves, but on the encoded samples.
30 If the value calculated by the decoding party does not match the value contained in the signed message, the decoder is alerted to the fact that this watermark was

transplanted from somewhere else. This is possible only with a hash function which ignores the changes made by the stega-cipher after the hash in the watermark was generated.

- 5 This scheme makes it impossible to transplant watermarks, even with the keys to the stega-cipher.

Appendix - Psuedo-code

```

const int WINDOW_RESET = 256;
const int WINDOW_SIZE = 128;
const int MARKER_BITS = 1024;
const int CHUNK_BITS = 2048 * 8;

int window_offset;
int msg_bit_offset;
int frequency_offset;
Boolean useCell;

/* 8 bits per byte, 1 byte per char */
unsigned char frequency_mask[WINDOW_SIZE/8];
unsigned char window_mask[WINDOW_RESET/8];
unsigned char msg_start_marker[MARKER_BITS/8];
unsigned char msg_end_marker[MARKER_BITS/8];
Int16 amplitude_sample_buffer[WINDOW_SIZE];
float power_frequency_buffer[WINDOW_SIZE];
unsigned char message_buffer[CHUNK_BITS/8];

void doFFT(Int16 *amp_sample_buffer, float *power_freq_buffer,int size);
void doInverseFFT(Int16 *amp_sample_buffer, float *power_freq_buffer,int size);
void initialize();
Bit getBit(unsigned char *buffer,int bitOffset);
Boolean map(Bit window_bit, Bit band_bit, int window, int frequency);
Boolean getSamples(Int16 *amplitude_sample_buffer,int samples);
void encode()

void initialize()
{
    /* message to be encoded is generated */
    /* message is prefixed with 1024 bit msg_start_marker */
    /* message is suffixed with 1024 bit msg_end_marker */
    /* remaining space at end of message buffer padded with random bits */
    window_offset = 0;
    msg_bit_offset = 0;
    frequency_offset = 0;
    frequency_mask loaded
    window_mask loaded
    zeroAmpSampleBuffer();
}

```

```

Boolean getSamples(Int16 *buffer,int samples)
{
    /* get samples number of samples and shift them contiguously into the sample
    buffer from right to left*/
    if(samples < samples available)
        return false;
    else
        return true;
}

void doFFT(Int16 *sample_buffer, float *spectrum_buffer, int size)
{
    calculate FFT on sample_buffer, for size samples
    store result in spectrum buffer
}

void doInverseFFT(Int16 *sample_buffer,float *spectrum_buffer,int size)
{
    calculate inverse FFT on spectrum_buffer
    store result in sampe_buffer
}

Bit getBit(unsigned char *buffer,in bitOffset)
{
    returns value of specified bit in specified buffer
    either 0 or 1, could use Boolean (true/false) values for bit set of bit off
}

Boolean map(Bit window_bit,Bit band_bit,int window, int frequency_
{
    /* this is the function that makes the information difficult to find */
    /* the inputs window_bit and band_bit depend only on the mask values
    used for encoding the information, they are 1) random, 2) secret */
    /* window and frequency values are used add time and frequency band dependent
    complexity to this function */
    /* this function is equivalent to a Boolean truth table with window * frequency * 4
    possible input combinations and 2 possible output */
    /* for any input combination, the output is either true or false */
    /* window ranges from 0 to WINDOW_RESET -1 */
    /* frequency ranges from 0 to WINDOW_SIZE - 1 */
    return calculated truth value
}

```

```

void encodeBit(float *spectrum_buffer,int freq_offset,Bit theBit)
{
    /* modifies the value of the cell in spectrum_buffer, indexed by freq_offset
       in a manner that distinguishes each of the 2 possible values of theBit,
       1 or 0
    */
    /* suggested method of setting the Least Significant bit of the cell == theBit */
    /* alternative method of rounding the value of the cell upward or downward to
       certain fractional values proposed
       i.e. <= .5 fractional remainder signifies 0, > .5 fraction remainder
          signifies 1
    */
}

void encode()
{
    initialize();

    do {

        if(getSamples(amplitude_sample_buffer) == false)
            return;

        doFFT(amplitude_sample_buffer,power_frequency_buffer,WINDOW_SIZE);

        for (frequency_offset = 0; frequency_offset < WINDOW_SIZE;
            frequency_offset++){

            useCell = map(getBit(window_mask,window_offset),
                getBit(frequency_mask,frequency_offset),
                window_offset, frequency_offset);

            if(useCell == true){
                encodeBit(power_frequency_buffer,frequency_offset,
                    getBit(message_buffer,msg_bit_offset));
                message_bit_offset ++;
                if(msg_bit_offset == MESSAGEBITS){
                    initialize();
                    break; /* exit frequency loop */
                }
            }
        }
    }
}

```

```

doInverseFFT(amplitude_sample_buffer,power_frequency_buffer,
             WINDOW_SIZE);

outputSamples(amplitude_sample_buffer);

window_offset++;
if(window_offset == WINDOW_RESET){
    window_offset = 0;
}

} while(true);
}

```

The encode() procedure processes an input sample stream using the specified frequency and window masks as well as a pre-formatted message to encode.

encode() processes the sample stream in windows of WINDOW_SIZE samples, contiguously distributed in the sample stream, so it advances WINDOW_SIZE samples at a time.

For each sample window, encode() first compute the FFT of the window, yielding its Power Spectrum Estimation. For each of these window PSEs, encode() then uses the map() function to determine where in each PSE to encode the bits of the message, which it reads from the message buffer, one bit at a time. Each time map() returns true, encode() consumes another sample from the message.

After each window is encoded, encode() computes the inverse FFT on the PSE to generate a modified sample window, which is then output as the modified signal. It is important the sample windows NOT overlap in the sample stream, since this would potentially damage the preceding encoding windows in the stream.

Once the message is entirely encoded, including its special end of message marker bit stream, encode() resets its internal variables to begin encoding the message once more in the next window. encode() proceeds in this manner until the input sample stream is exhausted.

```

enum {
    Synchronizing,
    Locked
}; /* decode states */

```

```

unsigned char message_end_buffer[MARKER_BITS];

Bit decodeBit(float *spectrum_buffer,int freq_offset)
{
    /* reads the value of the cell in spectrum_buffer, indexed by freq_offset
       in a manner that distinguishes each of the 2 possible values of an
       encoded bit, 1 or 0
    */
    /* suggested method of testing the Least Significant bit of the cell */
    /* alternative method of checking the value of the cell versus certain fractional
       remainders proposed.
       i.e. <= .5 fractional remainder signifies 0, > .5 fraction remainder
       signifies 1
    */
    return either 1 or 0 as appropriate
}

Boolean decode()
{
    /* Initialization */
    state = Synchronizing;
    window_offset = 0;
    set frequency mask
    set window mask
    clear sample buffer
    int nextSamples = 1;
    int msg_start_offset = 0;
    clear message_end_buffer
    Bit aBit;
    Boolean bitsEqual;

    do {

        if(state == Synchronizing){
            nextSamples = 1;
            window_offset = 0;
        }
        else
            nextSamples = WINDOW_SIZE;

        if(getSamples(amplitude_sample_buffer) == false)
            return false;
    }
}

```

```

doFFT(amplitude_sample_buffer,power_frequency_buffer,
      WINDOW_SIZE); /* 2 */

for (frequency_offset = 0; frequency_offset < WINDOW_SIZE;
     frequency_offset++){

    useCell = map(getBit(window_mask,window_offset),
                 getBit(frequency_mask,frequency_offset),
                 window_offset, frequency_offset);

    if(useCell == true){
        aBit = decodeBit(power_frequency_buffer,
                        frequency_offset);
        setBit(message_buffer,message_bit_offset,aBit);
        message_bit_offset++;
    }
    else
        continue;
    if(state == Synchronizing){
        bitsEqual =
        compareBits(message_start_marker,message_buffer,
                    message_bit_offset);
        if(!bitsEqual){
            message_bit_offset = 0;
            misaligned = true;
            break; /* exit frequency loop */
        }
        else if (message_bit_offset == MARKER_BITS)
            state == Locked;
    }
    else {
        /* locked onto encoded stream */
        shift aBit into right side of message_end_buffer
        bitsEqual = compareBits(message_end_buffer,
                                msg_end_marker,MARKER_BITS);
        if(bitsEqual)
            return true;
    }
}
} while (true);
}

```

The `decode()` procedure scans an input sample stream using specified window and frequency masks, until it either decodes a valid message block, storing it in a message buffer, or exhausts the sample stream.

The `decode()` procedure starts in state *Synchronizing*, in which it does not know where in the sample stream the encoding windows are aligned. The procedure advances the sample window through the sample stream one sample at a time, performing the FFT calculation on each window, and attempting to decode valid message bits from the window. As it extracts each bit using the `map()` function, the `decode()` procedure compares these bits against the start of message marker. As soon as a mismatch is detected, the `decode()` procedure knows it is not yet properly aligned to an encoding window, and immediately ceases decoding bits from the current window and moves to the next window, offset by 1 sample. The `decode()` procedure continues in this manner until it matches successfully the complete bitstream of a start of message marker. At this point the `decode()` procedure assumes it is aligned to an encoded message and can then decode bits to the message buffer quickly, advancing the sample window fully at each iterations. It is now in *Locked* mode. For each bit it stores in the message buffer when in *Locked* mode, the `decode()` procedure also shifts the same bit value into the least significant bit of the `message_end_buffer`. After each bit is decoded in *Locked* mode, the `decode()` procedure checks compares the `message_end_buffer` with the `msg_end_marker` in a bit by bit manner. When a complete match is found, `decode()` is finished and returns true. If the sample stream is exhausted before this occurs, `decode()` returns false. If `decode()` returns true, a valid message is stored in the message buffer, including the start and end of message markers.

Claims

1. A steganographic method comprising the steps of:
using random keys in combination with steganography to encode additional
information into digitized samples such that a signal generated from the modified
sample stream is not significantly degraded and such that the additional information
cannot be extracted without the keys and such that the signal generated from the
modified sample stream will be degraded by attempts to erase, scramble, or
otherwise obliterate the encoded additional information.
2. An apparatus for encoding or decoding a message, represented as
series of data bits into or out of a series of digitized samples, comprising:
- a) a sample buffer for holding and accessing and transforming
digitized samples;
 - b) a digital signal processor capable of performing fast fourier
transforms;
 - c) a memory to contain information representing
 - 1) primary mask,
 - 2) convolutional mask,
 - 3) start to message delimiter,
 - 4) a mask calculation buffer,
 - 5) a message buffer,
 - 6) an integer representing a message bit index,
 - 7) a position integer M representing message size,
 - 8) an integer representing an index into said primary
mask,
 - 9) an integer representing an index into said convolution
mask,
 - 10) an integer representing the state of a decode process,
 - 11) a table representing a map function;
 - 12) a flag indicating a complete message has been
decoded or encoded,

- 13) a positive integer S representing a number of samples to read into said sample buffer, and
- 14) a flag indicating the size of a message which has been decoded;
- 5 d) an input to acquire digital samples;
e) an output to output modified digital samples;
f) an input for inputting the values of (c1) - (c5) and (c11) and (c13);
- g) an output to output the message stored in (c5) as the result of a decode process and the value of (c10) to an attached digital circuit;
- 10 h) at least one data bus to transfer information from (d) to (a), (a) to (b), (b) to (a), (a) to (e), (f) to (c), and (c) to (e); and
- 15 i) a clock which generates a clock signal to drive (b) and control the operation of the apparatus.
- 20

3. A method of encoding information into a sample stream of data, said method comprising the steps of:

- 25 A) generating a mask set to be used for encoding, said set including:
a random or pseudo-random primary mask,
a random or pseudo-random convolution mask,
a random or pseudo-random start of message
delimiter, wherein said mask set can be concatenated and manipulated as a single bit
30 stream;
- B) obtaining a message to be encoded;

- 5 C) generating a message bit stream to be encoded such that the stream includes
- 1) a start of message delimiter, and
 - 2) an integer representing the number of message bytes to follow the message;
- D) loading the message bit stream, a map table, the primary mask, the convolution mask, and the start of message delimiter into a memory;
- 10 E) resetting a primary mask index, a convolution mask and message bit index, and setting the message size integer equal to the total number of bits in the message bit stream;
- F) clearing a message encoded flag;
- G) reading a window of samples from a sample input device and storing them sequentially in a sample buffer;
- 15 H) resetting the primary mask index and looping through the sample buffer from a first sample to a last sample incrementing the primary mask index each time a sample is visited, such that for each sample position, a value of the mapping function is computed, which is either true or false, by using a bit of the primary mask representing a current sample and a bit of the convolution mask
- 20 indicated by the convolution index to calculate an offset in the map table;
- I) obtaining the bit value stored in the map table and encoding the bit of the message indicated by the message bit index into the current sample if the bit value obtained from the map table is a certain value and incrementing the message bit index, determining whether the message bit index equals the number of message bits, and if it does re-performing step A), setting the message encoded flag, and exiting the loop;
- 25 J) outputting the modified samples in the sample buffer, and if the message encoded flag is set jumping back to said step E);
- K) incrementing the convolution index, wherein if the
- 30 convolution index equals the length of the convolution mask in bits then set the convolution index to 0; and

L) jumping back to step G).

4. A method of encoding information into a sample stream of data, comprising the steps of:

- 5 A) generating a mask set to be used for encoding, including:
 a random or pseudo-random primary mask,
 a random or pseudo-random convolution mask, and
 a random or pseudo-random start of message
 delimiter, wherein said mask set can be concatenated and manipulated as a single bit
10 stream;
- B) inputting a message to be encoded;
- C) generating a message bit stream to be encoded including
 a start of message delimiter, and
 an integer representing of number of message bytes to
15 follow the message;
- D) loading the message bit stream, a map table, and the mask set
 into a memory;
- E) resetting a primary mask index, a convolution mask and
 message bit index, setting the message size index equal to the number of bits in the
20 message bitstream, and clearing a message encoded flag;
- F) reading a window of samples of the inputted message and
 storing the samples sequentially in a sample buffer;
- G) computing a spectral transform of the samples in the buffer;
- H) obtaining the bit value stored in the map table, wherein if the
25 bit value is true, then encoding the bit of the message indicated by the message bit
 index into the current sample and incrementing the message bit index, where the
 message bit index equals the number of message bits, and then reperforming step
 A), setting the message encoded flag, and exiting the loop;
- 30 I) computing the inverse spectral of the spectral values stored
 in the sample buffer;

J) outputting the values in the sample buffer, and if the sample encoded flag is set, then clear the flag and jump back to step E);

K) incrementing the convolution index and when the convolution index equals the length of the convolution mask in bits resetting the convolution index; and

L) jumping back to step F).

5. The method of claim 3 wherein the encoding of the message bit into the sample in step I includes encoding a single bit of the sample to match the message bit.

6. The method of claim 4 wherein the encoding of the message bit into the sample in step H includes altering the sample value such that said sample value falls within a prespecified range of values relative to its original value.

7. A method of decoding information from a sample stream of data, comprising the steps of:

A) obtaining a mask set including:

- (1) a random or pseudo-random primary mask,
- (2) a random or pseudo-random convolution mask, and
- (3) a random or pseudo-random start of message delimiter;

B) loading a map table, and the mask set into a memory;

C) resetting a primary mask index and convolution mask index and setting a message size integer equal to 0;

D) clearing a message decoded flag;

E) setting a state of the decode process to SYNCHRONIZED;

F) checking the state of the decode process and if the decode state is UNSYNCHRONIZED, setting a number of samples to equal 1 and resetting the convolution index to 0; otherwise, setting the number of samples to equal S ($S \geq 1$);

G) reading the number of samples specified in step F) into a sample buffer,

H) resetting the primary mask index, and looping through the sample buffer from the first sample to the last sample, incrementing the primary mask index each time, and for each sample position, computing the value of a mapping function to calculate an offset into the map table;

I) obtaining the bit value in the map table, and if the value is true, decoding the bit of the message indicated by the message bit index, storing the bit into the message buffer at the message bit index, and incrementing the message bit index;

J) comparing the decoded bits in the message buffer to the start of message delimiter, and if the number of bits in the message buffer is less than or equal to the number of bits in the start of message delimiter and the bits match, then setting the state of the decode process to SYNCHRONIZED; otherwise setting the state of the decode process to UNSYNCHRONIZED;

K) if the state of the decode process is SYNCHRONIZED and the number of bits in the message buffer is greater than or equal to the sum of the number of bits of the start of delimiter and the message size, then setting the state of the decode process to SYNC-AND-SIZE and copying certain bits from the message buffer to a message size integer container;

L) if the state of the decode process is SYNC-AND-SIZE and the number of bits in the message buffer divided by $\#$ is greater than or equal to the message size, then setting the message decoded flag, outputting the message and the message decoded flag and ending the method;

M) incrementing the convolution index, and if the convolution index equals the number of bits in the convolution mask resetting the convolution index, and

N) jumping to step F).

8. A method of decoding information from sampled data, comprising the steps of:

- 5 delimiter,
- A) Obtaining a mask set including
- (1) a random or pseudo-random primary mask,
 - (2) a random or pseudo-random convolution mask, and
 - (3) a random or pseudo-random start of message
- B) loading a map table, and the mask set into a memory;
- C) resetting a primary mask index and convolution mask index and setting a message size integer equal to 0;
- D) clearing a message decoded flag;
- 10 E) setting a state of the decode process to SYNCHRONIZED;
- F) checking the state of the decode process and if the decode state is UNSYNCHRONIZED, setting a number of samples to equal 1 and resetting the convolution index to 0; otherwise, setting the number of samples to equal S ($S > 1$);
- 15 G) reading the number of samples specified in step F) into a sample buffer;
- H) computing a spectral transform of the samples stored in the sample buffer;
- I) resetting the primary mask index and looping through the
- 20 sample buffer from the first sample to the last sample, incrementing the primary mask index each time, and for each sample position, computing the value of a mapping function by using the bit of the primary mask corresponding to the primary mask index and the bit of the convolution masks indicated by the convolution phase to calculate an offset into the map table representing the mapping function;
- 25 J) obtaining a bit value stored in the map, and if the value is true, decoding the bit of the message indicated by the message bit index from the current sample, storing the bit into the message buffer at the message bit index, and incrementing the message bit index;
- K) comparing the decoded bits in the message buffer to the start
- 30 of message delimiter, and if the number of bits in the message buffer is less than or equal to the number of bits in the start of message delimiter and the bits match, then

setting the state of the decode process to SYNCHRONIZED; otherwise, setting the state of the decode process UNSYNCHRONIZED;

5 L) if the state of the decode process is SYNCHRONIZED, and the number of bits in the message buffer is greater than or equal to the sum of the number of bits of the start of delimiter and the message size, then setting the state
of the decode process to SYNC-AND-SIZE and copying certain bits from the message buffer to a message size integer container;

10 M) if the state of the decode process is SYNC-AND-SIZE and the number of bits in the message buffer divided by 8 is greater than or equal to the message size, then setting the message decoded flag, outputting the message and the message decoded flag and ending the method;

N) incrementing the convolution index, wherein if the convolution index equals the number of bits in the convolution mask, then resetting the convolution index; and

15 O) jumping to step F).

9. The method of claim 7 wherein the decoding of the message bit from the sample in step I includes reading a single bit of the sample.

20 10. The method of claim 7 wherein the decoding of the message bit from the sample in step I includes mapping a range of sample values onto a particular message bit value.

25 11. The method of claim 4 wherein the map table is defined such that any index of the map table directs the process to encode information.

12. The method of claim 1 wherein the samples are obtained from a sample stream representing digitized sound or music.

13. The method of claim 12 wherein the identical encode process is performed on two sample streams representing channel A and channel B of digitized stereo sound.
- 5 14. The method of claim 12 wherein the sample streams represent channel A and channel B of digitized stereo sound and are interleaved before being input as a single sample stream and are separated into two channels upon output.
- 10 15. The method of claim 1 wherein the samples are obtained from a sample stream representing digitized video.
16. The method of claim 1 wherein the samples are obtained from a sample stream representing a digitized image.
- 15 17. The apparatus of claim 2, further comprising a tamper-resistant packaging, enclosing said apparatus wherein circuitry and information stored therein are destroyed if said packaging is opened.
- 20 18. The method of claim 3, further comprising a pre-encoding step which customizes the message to be encoded including: calculating over which windows in the samples stream a message will be encoded, computing a secure one way hash function of the samples in those windows, and placing the resulting hash values in the message before the message is encoded;
- 25 wherein the hash calculating step includes: calculating the size of the original message plus the size of an added hash value, and pre-processing the sample stream for the purpose of calculating hash values of each series of windows that will be used to encode the message and creating a modified copy of the message containing the hash value such that each message containing a hash value matches each window series uniquely.
- 30

19. The method of claim 1, wherein an authority for on line distribution of content encodes at least one of the following items into a sample stream ;
- the title,
 - the artist,
 - 5 the copyright holder,
 - the body to which royalties should be paid, and
 - general terms for publisher distribution.
20. The method of claim 19, wherein the authority combines at least one item with a secure private key signed message from a publisher containing at least one of the following pieces of information:
- the title,
 - the publisher's identification,
 - the terms of distribution,
 - 15 any consideration paid for the right to distribute the content,
 - a brief statement of agreement, and
- the publisher signs and encrypts the combined message using a public key cryptosystem and encodes the signed and encrypted message into the sample stream.
21. The method of claim 20, wherein a publisher obtains the encoded sample stream and additionally obtains information from the authority and combines this with a message received from a consumer, which has been signed using a public key cryptosystem and wherein the signed message contains at least one of the following
- 25 data
- the content title,
 - consumer identification,
 - the terms of distribution,
 - the consideration paid for the content,
 - 30 a brief statement of agreement, and

the publisher uses a public key cryptosystem to sign the combined information and finally encodes the signed information.

- 5 22. The method of claim 1, wherein the sample stream is obtained from at least one audio track contained within a digitized movie, video game software, or other software.
- 10 23. The method of claim 1, wherein the sample stream is obtained from at least one digitized movie or still image contained within a video game or other software.
24. The method of claim 1, wherein encoded information is contained in the differences or relationship between samples or groups of samples.
- 15 25. The method of claim 4, wherein the encoding of the message bit into the sample in step H includes encoding a single bit of the sample to match the message bit.
- 20 26. The method of claim 3, wherein the encoding of the message bit into the sample in step I includes altering the sample value such that said sample value falls within a prespecified range of values relative to its original value.
27. The method of claim 8, wherein the decoding of the message bit in step J includes reading a single bit of the sample.
- 25 28. The method of claim 8, wherein the decoding of the message bit in step J includes mapping a range of sample values onto a particular message bit value.
- 30 29. The method of claim 3, wherein the map table is defined such that any index of the map table directs the process to encode information.

30. The method of claim 7, wherein the map table is defined such that any index of the map table directs the process to encode information.

31. The method of claim 8, wherein the map table is defined such that any index
5 of the map table directs the process to encode information.

32. The method of claim 4, further comprising a pre-encoding step which
customizes the message to be encoded including: calculating over which windows
in the samples stream a message will be encoded, computing a secure one way hash
10 function of the samples in those windows, and placing the resulting hash values in
the message before the message is encoded;

wherein the hash calculating step includes: calculating the size of the
original message plus the size of an added hash value, and pre-processing the
sample stream for the purpose of calculating hash values of each series of windows
15 that will be used to encode the message and creating a modified copy of the
message containing the hash value such that each message containing a hash value
matches each window series uniquely.--

20

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04L 9/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 97/26732 (43) International Publication Date: 24 July 1997 (24.07.97)</p>
<p>(21) International Application Number: PCT/US97/00651 (22) International Filing Date: 16 January 1997 (16.01.97) (30) Priority Data: 08/587,943 17 January 1996 (17.01.96) US (71) Applicant: THE DICE COMPANY [US/US]; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US). (72) Inventors: MOSKOWITZ, Scott, A.; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US). COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US). (74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).</p>		<p>(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>
<p>(54) Title: METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE</p> <p>(57) Abstract</p> <p>A method for protecting computer code copyrights by encoding the code into a data resource with a digital watermark. The digital watermark contains licensing information interwoven with essential code resources encoded into data resources. The result is that while an application program can be copied in an uninhibited manner, only the licensed user having the license code can access essential code resources to operate the program and any descendant copies bear the required license code.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LJ	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODEFIELD OF INVENTION

With the advent of computer networks and digital
5 multimedia, protection of intellectual property has
become a prime concern for creators and publishers of
digitized copies of copyrightable works, such as musical
recordings, movies, video games, and computer software.
One method of protecting copyrights in the digital
10 domain is to use "digital watermarks."

The prior art includes copy protection systems
attempted at many stages in the development of the
software industry. These may be various methods by
which a software engineer can write the software in a
15 clever manner to determine if it has been copied, and if
so to deactivate itself. Also included are undocumented
changes to the storage format of the content. Copy
protection was generally abandoned by the software
industry, since pirates were generally just as clever as
20 the software engineers and figured out ways to modify
the software and deactivate the protection. The cost of
developing such protection was not justified considering
the level of piracy which occurred despite the copy
protection.

25 Other methods for protection of computer software
include the requirement of entering certain numbers or
facts that may be included in a packaged software's
manual, when prompted at start-up. These may be

overcome if copies of the manual are distributed to unintended users, or by patching the code to bypass these measures. Other methods include requiring a user to contact the software vendor and to receive "keys" for
5 unlocking software after registration attached to some payment scheme, such as credit card authorization. Further methods include network-based searches of a user's hard drive and comparisons between what is registered to that user and what is actually installed
10 on the user's general computing device. Other proposals, by such parties as AT&T's Bell Laboratories, use "kerning" or actual distance in pixels, in the rendering of text documents, rather than a varied number of ASCII characters. However, this approach can often
15 be defeated by graphics processing analogous to sound processing, which randomizes that information. All of these methods require outside determination and verification of the validity of the software license.

Digital watermarks can be used to mark each
20 individual copy of a digitized work with information identifying the title, copyright holder, and even the licensed owner of a particular copy. When marked with licensing and ownership information, responsibility is created for individual copies where before there was
25 none. Computer application programs can be watermarked by watermarking digital content resources used in conjunction with images or audio data. Digital watermarks can be encoded with random or pseudo random keys, which act as secret maps for locating the
30 watermarks. These keys make it impossible for a party to find the watermark without having the key. In addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark. Digital
35 watermarks are described in "Steganographic Method and Device" - The DICE Company, Serial No. 08/489,172, the disclosure of which is hereby incorporated by reference.

Other information is disclosed in "Technology: Digital Commerce", Denise Caruso, New York Times, August 7, 1995; and "Copyrighting in the Information Age", Harley Ungar, ONLINE MARKETPLACE, September 1995, Jupiter

5 Communications.

Additionally, other methods for hiding information signals in content signals, are disclosed in U.S. Patent No. 5,319,735 - Preuss et al. and U.S. Patent No. 5,379,345 - Greenberg.

10 It is desirable to use a "stega-cipher" or watermarking process to hide the necessary parts or resources of the executable object code in the digitized sample resources. It is also desirable to further modify the underlying structure of an executable
15 computer application such that it is more resistant to attempts at patching and analysis by memory capture. A computer application seeks to provide a user with certain utilities or tools, that is, users interact with a computer or similar device to accomplish various tasks
20 and applications provide the relevant interface. Thus, a level of authentication can also be introduced into software, or "digital products," that include digital content, such as audio, video, pictures or multimedia, with digital watermarks. Security is maximized because
25 erasing this code watermark without a key results in the destruction of one or more essential parts of the underlying application, rendering the "program" useless to the unintended user who lacks the appropriate key. Further, if the key is linked to a license code by means
30 of a mathematical function, a mechanism for identifying the licensed owner of an application is created.

It is also desirable to randomly reorganize program memory structure intermittently during program run time, to prevent attempts at memory capture or object code
35 analysis aimed at eliminating licensing or ownership information, or otherwise modifying, in an unintended manner, the functioning of the application.

In this way, attempts to capture memory to determine underlying functionality or provide a "patch" to facilitate unauthorized use of the "application," or computer program, without destroying the functionality and thus usefulness of a copyrightable computer program can be made difficult or impossible.

It is thus the goal of the present invention to provide a higher level of copyright security to object code on par with methods described in digital watermarking systems for digitized media content such as pictures, audio, video and multimedia content in its multifarious forms, as described in previous disclosures, "Steganographic Method and Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System", filed on even date herewith, the disclosure of which is hereby incorporated by reference.

It is a further goal of the present invention to establish methods of copyright protection that can be combined with such schemes as software metering, network distribution of code and specialized protection of software that is designed to work over a network, such as that proposed by Sun Microsystems in their HotJava browser and Java programming language, and manipulation of application code in proposed distribution of documents that can be exchanged with resources or the look and feel of the document being preserved over a network. Such systems are currently being offered by companies including Adobe, with their Acrobat software. This latter goal is accomplished primarily by means of the watermarking of font, or typeface, resources included in applications or documents, which determine how a bitmap representation of the document is ultimately drawn on a presentation device.

The present invention includes an application of the technology of "digital watermarks." As described in previous disclosures, "Steganographic Method and

Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System," watermarks are particularly suitable to the identification, metering, distributing and authenticating digitized content such as pictures, audio, video and derivatives thereof under the description of "multimedia content." Methods have been described for combining both cryptographic methods, and steganography, or hiding something in plain view. Discussions of these technologies can be found in Applied Cryptography by Bruce Schneier and The Code Breakers by David Kahn. For more information on prior art public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig.

Computer code, or machine language instructions, which are not digitized and have zero tolerance for error, must be protected by derivative or alternative methods, such as those disclosed in this invention, which focuses on watermarking with "keys" derived from license codes or other ownership identification information, and using the watermarks encoded with such keys to hide an essential subset of the application code resources.

SUMMARY OF THE INVENTION

It is thus a goal of the present invention, to provide a level of security for executable code on similar grounds as that which can be provided for digitized samples. Furthermore, the present invention differs from the prior art in that it does not attempt to stop copying, but rather, determines responsibility for a copy by ensuring that licensing information must be preserved in descendant copies from an original. Without the correct license information, the copy cannot function.

An improvement over the art is disclosed in the present invention, in that the software itself is a set of commands, compiled by software engineer, which can be

configured in such a manner as to tie underlying
functionality to the license or authorisation of the
copy in possession by the user. Without such
verification, the functions sought out by the user in
5 the form of software cease to properly work. Attempts
to tamper or "patch" substitute code resources can be
made highly difficult by randomizing the location of
said resources in memory on an intermittent basis to
resist most attacks at disabling the system.

10

DETAILED DESCRIPTION

An executable computer program is variously
referred to as an application, from the point of view of
a user, or executable object code from the point of view
15 of the engineer. A collection of smaller, atomic (or
indivisible) chunks of object code typically comprise
the complete executable object code or application which
may also require the presence of certain data resources.
These indivisible portions of object code correspond
20 with the programmers' function or procedure
implementations in higher level languages, such as C or
Pascal. In creating an application, a programmer writes
"code" in a higher level language, which is then
compiled down into "machine language," or, the
25 executable object code, which can actually be run by a
computer, general purpose or otherwise. Each function,
or procedure, written in the programming language,
represents a self-contained portion of the larger
program, and implements, typically, a very small piece
30 of its functionality. The order in which the programmer
types the code for the various functions or procedures,
and the distribution of and arrangement of these
implementations in various files which hold them is
unimportant. Within a function or procedure, however,
35 the order of individual language constructs, which
correspond to particular machine instructions is
important, and so functions or procedures are considered

indivisible for purposes of this discussion. That is, once a function or procedure is compiled, the order of the machine instructions which comprise the executable object code of the function is important and their order

5 in the computer memory is of vital importance. Note that many "compilers" perform "optimizations" within functions or procedures, which determine, on a limited scale, if there is a better arrangement for executable instructions which is more efficient than that

10 constructed by the programmer, but does not change the result of the function or procedure. Once these optimizations are performed, however, making random changes to the order of instructions is very likely to "break" the function. When a program is compiled, then,

15 it consists of a collection of these sub-objects, whose exact order or arrangement in memory is not important, so long as any sub-object which uses another sub-object knows where in memory it can be found.

The memory address of the first instruction in one

20 of these sub-objects is called the "entry point" of the function or procedure. The rest of the instructions comprising that sub-object immediately follow from the entry point. Some systems may prefix information to the entry point which describes calling and return

25 conventions for the code which follows, an example is the Apple Macintosh Operating System (MacOS). These sub-objects can be packaged into what are referred to in certain systems as "code resources," which may be stored separately from the application, or shared with other

30 applications, although not necessarily. Within an application there are also data objects, which consist of some data to be operated on by the executable code. These data objects are not executable. That is, they do not consist of executable instructions. The data

35 objects can be referred to in certain systems as "resources."

When a user purchases or acquires a computer program, she seeks a computer program that "functions" in a desired manner. Simply, computer software is overwhelmingly purchased for its underlying

5 functionality. In contrast, persons who copy multimedia content, such as pictures, audio and video, do so for the entertainment or commercial value of the content. The difference between the two types of products is that multimedia content is not generally interactive, but is

10 instead passive, and its commercial value relates more on passive not interactive or utility features, such as those required in packaged software, set-top boxes, cellular phones, VCRs, PDAs, and the like. Interactive digital products which include computer code may be

15 mostly interactive but can also contain content to add to the interactive experience of the user or make the underlying utility of the software more aesthetically pleasing. It is a common concern of both of these creators, both of interactive and passive multimedia

20 products, that "digital products" can be easily and perfectly copied and made into unpaid or unauthorized copies. This concern is especially heightened when the underlying product is copyright protected and intended for commercial use.

25 The first method of the present invention described involves hiding necessary "parts" or code "resources" in digitized sample resources using a "digital watermarking" process, such as that described in the "Steganographic Method and Device" patent application.

30 The basic premise for this scheme is that there are a certain sub-set of executable code resources, that comprise an application and that are "essential" to the proper function of the application. In general, any code resource can be considered "essential" in that if

35 the program proceeds to a point where it must "call" the code resource and the code resource is not present in memory, or cannot be loaded, then the program fails.

However, the present invention uses a definition of "essential" which is more narrow. This is because, those skilled in the art or those with programming experience, may create a derivative program, not unlike
5 the utility provided by the original program, by writing additional or substituted code to work around unavailable resources. This is particularly true with programs that incorporate an optional "plug-in architecture," where several code resources may be made
10 optionally available at run-time. The present invention is also concerned with concentrated efforts by technically skilled people who can analyze executable object code and "patch" it to ignore or bypass certain code resources. Thus, for the present embodiment's
15 purposes, "essential" means that the function which distinguishes this application from any other application depends upon the presence and use of the code resource in question. The best candidates for this type of code resources are NOT optional, or plug-in
20 types, unless special care is taken to prevent work-arounds.

Given that there are one or more of these essential resources, what is needed to realize the present invention is the presence of certain data resources of a
25 type which are amenable to the "stega-cipher" process described in the "Steganographic Method and Device" patent application. Data which consists of image or audio samples is particularly useful. Because this data consists of digital samples, digital watermarks can be
30 introduced into the samples. What is further meant is that certain applications include image and audio samples which are important to the look and feel of the program or are essential to the processing of the application's functionality when used by the user.
35 These computer programs are familiar to users of computers but also less obvious to users of other devices that run applications that are equivalent in

some measure of functionality to general purpose computers including, but not limited to, set-top boxes, cellular phones, "smart televisions," PDAs and the like. However, programs still comprise the underlying
5 "operating systems" of these devices and are becoming more complex with increases in functionality.

One method of the present invention is now discussed. When code and data resources are compiled and assembled into a precursor of an executable program
10 the next step is to use a utility application for final assembly of the executable application. The programmer marks several essential code resources in a list displayed by the utility. The utility will choose one or several essential code resources, and encode them
15 into one or several data resources using the steganographic process. The end result will be that these essential code resources are not stored in their own partition, but rather stored as encoded information in data resources. They are not accessible at run-time
20 without the key. Basically, the essential code resources that provide functionality in the final end-product, an executable application or computer program, are no longer easily and recognizably available for manipulation by those seeking to remove the underlying
25 copyright or license, or its equivalent information, or those with skill to substitute alternative code resources to "force" the application program to run as an unauthorized copy. For the encoding of the essential code resources, a "key" is needed. Such a key is
30 similar to those described in the "Steganographic Method and Device." The purpose of this scheme is to make a particular licensed copy of an application distinguishable from any other. It is not necessary to distinguish every instance of an application, merely
35 every instance of a license. A licensed user may then wish to install multiple copies of an application, legally or with authorization. This method, then, is to

choose the key so that it corresponds, is equal to, or is a function of, a license code or license descriptive information, not just a text file, audio clip or identifying piece of information as desired in digital watermarking schemes extant and typically useful to stand-alone, digitally sampled content. The key is necessary to access the underlying code, i.e., what the user understands to be the application program.

The assembly utility can be supplied with a key generated from a license code generated for the license in question. Alternatively, the key, possibly random, can be stored as a data resource and encrypted with a derivative of the license code. Given the key, it encodes one or several essential resources into one or several data resources. Exactly which code resources are encoded into which data resources may be determined in a random or pseudo random manner. Note further that the application contains a code resource which performs the function of decoding an encoded code resource from a data resource. The application must also contain a data resource which specifies in which data resource a particular code resource is encoded. This data resource is created and added at assembly time by the assembly utility. The application can then operate as follows:

- 1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;
- 2) it stores this information in a personalization data resource;
- 3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources.

Note that the application can be copied in an uninhibited manner, but must contain the license code issued to the licensed owner, to access its essential code resources. The goal of the invention, copyright

protection of computer code and establishment of responsibility for copies, is thus accomplished

This invention represents a significant improvement over prior art because of the inherent difference in use
5 of purely informational watermarks versus watermarks which contain executable object code. If the executable object code in a watermark is essential to an application which accesses the data which contains the watermark, this creates an all-or-none situation.
10 Either the user must have the extracted watermark, or the application cannot be used, and hence the user cannot gain full access to the presentation of the information in the watermark bearing data. In order to extract a digital watermark, the user must have a key.
15 The key, in turn, is a function of the license information for the copy of the software in question. The key is fixed prior to final assembly of the application files, and so cannot be changed at the option of the user. That, in turn, means the license
20 information in the software copy must remain fixed, so that the correct key is available to the software. The key and the license information are, in fact, interchangeable. One is merely more readable than the other. In the earlier developed "Steganographic Method and Device," the possibility of randomization erasure
25 attacks on digital watermarks was discussed. Simply, it is always possible to erase a digital watermark, depending on how much damage you are willing to do to the watermark-bearing content stream. The present
30 invention has the significant advantage that you must have the watermark to be able to use the code it contains. If you erase the watermark you have lost a key piece of the functionality of the application, or even the means to access the data which bear the
35 watermark.

A preferred embodiment would be implemented in an embedded system, with a minimal operating system and

memory. No media playing "applets," or smaller sized applications as proposed in new operating environments envisioned by Sun Microsystems and the advent of Sun's Java operating system, would be permanently stored in the system, only the bare necessities to operate the device; download information, decode watermarks and execute the applets contained in them. When an applet is finished executing, it is erased from memory. Such a system would guarantee that content which did not contain readable watermarks could not be used. This is a powerful control mechanism for ensuring that content to be distributed through such a system contains valid watermarks. Thus, in such networks as the Internet or set-top box controlled cable systems, distribution and exchange of content would be made more secure from unauthorized copying to the benefit of copyright holders and other related parties. The system would be enabled to invalidate, by default, any content which has had its watermark(s) erased, since the watermark conveys, in addition to copyright information, the means to fully access, play, record or otherwise manipulate, the content.

A second method according to the present invention is to randomly re-organize program memory structure to prevent attempts at memory capture or object code analysis. The object of this method is to make it extremely difficult to perform memory capture-based analysis of an executable computer program. This analysis is the basis for a method of attack to defeat the system envisioned by the present invention.

Once the code resources of a program are loaded into memory, they typically remain in a fixed position, unless the computer operating system finds it necessary to rearrange certain portions of memory during "system time," when the operating system code, not application code, is running. Typically, this is done in low memory systems, to maintain optimal memory utilization. The

MacOS for example, uses Handles, which are double-indirect pointers to memory locations, in order to allow the operating system to rearrange memory transparently, underneath a running program. If a computer program

5 contains countermeasures against unlicensed copying, a skilled technician can often take a snapshot of the code in memory, analyze it, determine which instructions comprise the countermeasures, and disable them in the stored application file, by means of a "patch." Other

10 applications for designing code that moves to prevent scanning-tunnelling microscopes, and similar high sensitive hardware for analysis of electronic structure of microchips running code, have been proposed by such parties as Wave Systems. Designs of Wave Systems'

15 microchip are intended for preventing attempts by hackers to "photograph" or otherwise determine "burn in" to microchips for attempts at reverse engineering. The present invention seeks to prevent attempts at understanding the code and its organization for the

20 purpose of patching it. Unlike systems such as Wave Systems', the present invention seeks to move code around in such a manner as to complicate attempts by software engineers to reengineer a means to disable the methods for creating licensed copies on any device that

25 lacks "trusted hardware." Moreover, the present invention concerns itself with any application software that may be used in general computing devices, not chipsets that are used in addition to an underlying computer to perform encryption. Wave Systems' approach

30 to security of software, if interpreted similarly to the present invention, would dictate separate microchip sets for each piece of application software that would be tamperproof. This is not consistent with the economics of software and its distribution.

35 Under the present invention, the application contains a special code resource which knows about all the other code resources in memory. During execution

time, this special code resource, called a "memory scheduler," can be called periodically, or at random or pseudo random intervals, at which time it intentionally shuffles the other code resources randomly in memory, so that someone trying to analyze snapshots of memory at various intervals cannot be sure if they are looking at the same code or organization from one "break" to the next. This adds significant complexity to their job. The scheduler also randomly relocates itself when it is finished. In order to do this, the scheduler would have to first copy itself to a new location, and then specifically modify the program counter and stack frame, so that it could then jump into the new copy of the scheduler, but return to the correct calling frame. Finally, the scheduler would need to maintain a list of all memory addresses which contain the address of the scheduler, and change them to reflect its new location.

The methods described above accomplish the purposes of the invention - to make it hard to analyze captured memory containing application executable code in order to create an identifiable computer program or application that is different from other copies and is less susceptible to unauthorized use by those attempting to disable the underlying copyright protection system. Simply, each copy has particular identifying information making that copy different from all other copies.

What is Claimed Is:

1 i. A method of associating executable object code with
2 a digital sample stream by means of a digital watermark
3 wherein the digital watermark contains executable object
4 code and is encoded into the digital sample stream.

1 2. The method of claim 1 wherein a key to access the
2 digital watermark is a function of a collection of
3 license information pertaining to the software which is
4 accessing the watermark
5 where license information consists of one or more
6 of the following items:

7 Owning Organization name;
8 Personal Owner name;
9 Owner Address;
10 License code;
11 Software serialization number;
12 Distribution parameters;
13 Appropriate executable general computing
14 device architecture;
15 Pricing; and
16 Software Metering details.

1 3. The method of claim 1 further comprising the step
2 of transmitting the digital sample stream, via a
3 transmission means, from a publisher to a subscriber
4 wherein transmission means can selected from the
5 group of

6 soft sector magnetic disk media;
7 hard sector magnetic disk media;
8 magnetic tape media;
9 optical disc media;
10 Digital Video Disk media;
11 magneto-optical disk media;
12 memory cartridge;
13 telephone lines;

14 SCSI;
15 Ethernet or Token Ring Network;
16 ISDN;
17 ATM network;
18 TCP/IP network;
19 analog cellular network;
20 digital cellular network;
21 wireless network;
22 digital satellite;
23 cable network;
24 fiber optic network; and
25 electric powerline network.

1 4. The method of claim 1 where the object code to be
2 encoded is comprised of series of executable machine
3 instructions which perform the function of
4 processing a digital sample stream for the purpose
5 of modifying it or playing the digital sample stream.

1 5. The method of claim 3 further comprising the steps
2 of:
3 decoding said digital watermark and extracting
4 object code;
5 loading object code into computer memory for the
6 purpose of execution;
7 executing said object code in order to process said
8 digital sample stream for the purpose of playback.

1 6. A method of assembling an application to be
2 protected by watermark encoding of essential resources
3 comprising the steps of:
4 assembling a list of identifiers of essential
5 code resources of an application where identifiers allow
6 the code resource to be accessed and loaded into memory;
7 providing license information on the
8 licensee who is to receive an individualized copy of the
9 application;

10 storing license information in a
11 personalization resource which is added to the list of
12 application data resources;
13 generating a digital watermark key from
14 the license information; using the key as a pseudo-
15 random number string to select a list of suitable
16 digital sample data resources, the list of essential
17 code resources, and a mapping of which essential code
18 resources are to be watermarked into which data
19 resources;
20 storing the map, which is a list of
21 paired code and data resource identifiers, as a data
22 resource, which is added to the application;
23 adding a digital watermark decoder code
24 resource to the application, to provide a means for
25 extracting essential code resource from data resources,
26 according to the map;
27 processing the map list and encoding
28 essential code resources into digital sample data
29 resources with a digital watermark encoder;
30 removing self-contained copies of the
31 essential code resources which have been watermarked
32 into data resources; and
33 combining all remaining code and data
34 resources into a single application or installer.

1 7. A method of intermittently relocating application
2 code resources in computer memory, in order to prevent,
3 discourage, or complicate attempts at memory capture
4 based code analysis.

1 8. The method of claim 7 additionally comprising the
2 step of
3 assembling a list of identifiers of code resources
4 of an application where identifiers allow the code
5 resource to be accessed and loaded into memory.

1 9. The method of claim 8 additionally comprising the
2 step of modifying application program structure to make
3 all code resource calls indirectly, through the memory
4 scheduler, which looks up code resources in its list and
5 dispatches calls.

1 10. The method of claim 9 additionally comprising the
2 step of intermittently rescheduling or shuffling all
3 code resources prior to or following the dispatch of a
4 code resource call through the memory scheduler.

1 11. The method of claim 10 additionally comprised of
2 the step of the memory scheduler copying itself to a new
3 location in memory.

1 12. The method of claim 11 additionally comprising the
2 step of modifying the stack frame, program counter, and
3 memory registers of the CPU to cause the scheduler to
4 jump to the next instruction comprising the scheduler,
5 in the copy, to erase the previous memory instance of
6 the scheduler, and changing all memory references to the
7 scheduler to reflect its new location, and to return
8 from the copy of the scheduler to the frame which called
9 the previous copy of the scheduler.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00651

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) : H04L 9/00 US CL : 380/54 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. : 380/54, 2, 4, 9, 21, 23, 25, 28, 49, 50, 59; 283/73, 113, 17 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)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,349,655 A (MANN) 20 September 1994, see Abstract.	1
X	US 4,262,329 A (BRIGHT et al) 14 April 1981, see Abstract.	7
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:		
A document defining the general state of the art which is not considered to be of particular relevance	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	
B earlier document published on or after the international filing date	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	
L document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	
O document referring to an oral disclosure, use, exhibition or other means	*Z* document member of the same patent family	
P document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 04 APRIL 1997	Date of mailing of the international search report 29 APR 1997	
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 <i>Bernarr Earl Gregory</i> BERNARR EARL GREGORY Telephone No. (703) 206-4153	



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/00	A1	(11) International Publication Number: WO 97/26733 (43) International Publication Date: 24 July 1997 (24.07.97)
<p>(21) International Application Number: PCT/US97/00652</p> <p>(22) International Filing Date: 17 January 1997 (17.01.97)</p> <p>(30) Priority Data: 08/567,944 17 January 1996 (17.01.96) US</p> <p>(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).</p> <p>(72) Inventors: COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US). MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).</p> <p>(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).</p>	<p>(81) Designated States: AL, AU, BA, BE, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	
<p>(54) Title: METHOD FOR AN ENCRYPTED DIGITAL WATERMARK</p> <p>(57) Abstract</p> <p>A method for the human-assisted generation and application of pseudo-random keys for the purpose of encoding and decoding digital watermarks to and from a digitized data stream. A pseudo-random key and key application "envelope" are generated and stored using guideline parameters input by a human engineer interacting with a graphical representation of the digitized data stream. Key "envelope" information is permanently associated with the pseudo-random binary string comprising the key. Key and "envelope" information are then applied in a digital watermark system to the encoding and decoding of digital watermarks.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

METHOD FOR AN ENCRYPTED DIGITAL WATERMARKFIELD OF INVENTION

5 With the advent of computer networks and digital
multimedia, protection of intellectual property has
become a prime concern for creators and publishers of
digitized copies of copyrightable works, such as musical
recordings, movies, and video games. One method of
10 protecting copyrights in the digital domain is to use
"digital watermarks". Digital watermarks can be used to
mark each individual copy of a digitized work with
information identifying the title, copyright holder, and
even the licensed owner of a particular copy. The
15 watermarks can also serve to allow for secured metering
and support of other distribution systems of given media
content and relevant information associated with them,
including addresses, protocols, billing, pricing or
distribution path parameters, among the many things that
20 could constitute a "watermark." For further discussion
of systems that are oriented around content-based
addresses and directories, see U.S. Patent No. 5,428,606
Moskowitz. When marked with licensing and ownership
information, responsibility is created for individual
25 copies where before there was none. More information on
digital watermarks is set forth in "Steganographic
Method and Device" - The DICE Company, U.S. application
Serial No. 08/489,172, the disclosure of which is hereby
incorporated by reference. Also, "Technology: Digital

Commerce", Denise Caruso, New York Times, August 7, 1995
"Copyrighting in the Information Age", Harley Ungar,
ONLINE MARKETPLACE, September 1995, Jupiter
Communications further describe digital watermarks.

- 5 Additional information on other methods for hiding
information signals in content signals, is disclosed in
U.S. Patent No. 5,319,735 - Preuss et al. and U.S.
Patent No. 5,379,345 - Greenberg.

Digital watermarks can be encoded with random or
10 pseudo random keys, which act as secret maps for
locating the watermarks. These keys make it impossible
for a party without the key to find the watermark - in
addition, the encoding method can be enhanced to force a
party to cause damage to a watermarked data stream when
15 trying to erase a random-key watermark.

It is desirable to be able to specify limitations
on the application of such random or pseudo random keys
in encoding a watermark to minimize artifacts in the
content signal while maximizing encoding level. This
20 preserves the quality of the content, while maximizing
the security of the watermark. Security is maximized
because erasing a watermark without a key results in the
greatest amount of perceptible artifacts in the digital
content. It is also desirable to separate the
25 functionality of the decoder side of the process to
provide fuller recognition and substantiation of the
protection of goods that are essentially digitized bits,
while ensuring the security of the encoder and the
encoded content. It is also desirable that the separate
30 decoder be incorporated into an agent, virus, search
engine, or other autonomously operating or search
function software. This would make it possible for
parties possessing a decoder to verify the presence of
valid watermarks in a data stream, without accessing the
35 contents of the watermark. It would also be possible to
scan or search archives for files containing watermarked

content, and to verify the validity of the presence of such files in an archive, by means of the information contained in the watermarks. This scenario has particular application in screening large archives of files kept by on-line services and internet archives. It is further a goal of such processes to bring as much control of copyrights and content, including its pricing, billing, and distribution, to the parties that are responsible for creating and administering that content. It is another goal of the invention to provide a method for encoding multiple watermarks into a digital work, where each watermark can be accessed by use of a separate key. This ability can be used to provide access to watermark information to various parties with different levels of access. It is another goal of the invention to provide a mechanism which allows for accommodation of alternative methods encoding and decoding watermarks from within the same software or hardware infrastructure. This ability can be used to provide upgrades to the watermark system, without breaking support for decoding watermarks created by previous versions of the system. It is another goal of the invention to provide a mechanism for the certification and authentication, via a trusted third party, and public forums, of the information placed in a digital watermark. This provides additional corroboration of the information contained in a decoded digital watermark for the purpose of its use in prosecution of copyright infringement cases. It also has use in any situation in which a trusted third party verification is useful. It is another goal of this invention to provide an additional method for the synchronization of watermark decoding software to an embedded watermark signal that is more robust than previously disclosed methods.

SUMMARY OF THE INVENTION

The invention described herein is a human-assisted random key generation and application system for use in a digital watermark system. The invention allows an engineer or other individual, with specialized knowledge regarding processing and perception of a particular content type, such as digital audio or video, to observe a graphical representation of a subject digital recording or data stream, in conjunction with its presentation (listening or viewing) and to provide input to the key generation system that establishes a key generation "envelope", which determines how the key is used to apply a digital watermark to the digital data stream. The envelope limits the parameters of either or both the key generation system and the watermark application system, providing a rough guide within which a random or pseudo random key may be automatically generated and applied. This can provide a good fit to the content, such that the key may be used to encode a digital watermark into the content in such a manner as to minimize or limit the perceptible artifacts produced in the watermarked copy, while maximizing the signal encoding level. The invention further provides for variations in creating, retrieving, monitoring and manipulating watermarks to create better and more flexible approaches to working with copyrights in the digital domain.

Such a system is described herein and provides the user with a graphical representation of the content signal over time. In addition, it provides a way for the user to input constraints on the application of the digital watermark key, and provides a way to store this information with a random or pseudo random key sequence which is also generated to apply to a content signal. Such a system would also be more readily adaptable by current techniques to master content with personal

computers and authoring/editing software. It would also enable individuals to monitor their copyrights with decoders to authenticate individual purchases, filter possible problematic and unpaid copyrightable materials in archives, and provide for a more generally distributed approach to the monitoring and protection of copyrights in the digital domain.

DETAILED DESCRIPTION

10 Digital watermarks are created by encoding an information signal into a larger content signal. The information stream is integral with the content stream, creating a composite stream. The effectiveness and value of such watermarks are highest when the

15 informational signal is difficult to remove, in the absence of the key, without causing perceptible artifacts in the content signal. The watermarked content signal itself should contain minimal or no perceptible artifacts of the information signal. To

20 make a watermark virtually impossible to find without permissive use of the key, its encoding is dependent upon a randomly generated sequence of binary 1s and 0s, which act as the authorization key. Whoever possesses this key can access the watermark. In effect, the key

25 is a map describing where in the content signal the information signal is hidden. This represents an improvement over existing efforts to protect copyrightable material through hardware-based solutions always existing outside the actual content.

30 "Antipiracy" devices are used in present applications like VCRs, cable television boxes, and digital audio tape (DAT) recorders, but are quite often disabled by those who have some knowledge of the location of the device or choose not to purchase hardware with these

35 "additional security features." With digital watermarks, the "protection," or more accurately, the

deterrent, is hidden entirely in the signal, rather than a particular chip in the hardware.

Given a completely random key, which is uniformly applied over a content signal, resulting artifacts in the watermarked content signal are unpredictable, and depend on the interaction of the key and the content signal itself. One way to ensure minimization of artifacts is to use a low information signal level. However, this makes the watermark easier to erase, without causing audible artifacts in the content signal. This is a weakness. If the information signal level is boosted, there is the risk of generating audible artifacts.

The nature of the content signal generally varies significantly over time. During some segments, the signal may lend itself to masking artifacts that would otherwise be caused by high level encoding. At other times, any encoding is likely to cause artifacts. In addition, it might be worthwhile to encode low signal level information in a particular frequency range which corresponds to important frequency components of the content signal in a given segment of the content signal. This would make it difficult to perform bandpass filtering on the content signal to remove watermarks.

Given the benefits of such modifications to the application of the random key sequence in encoding a digital watermark, what is needed is a system which allows human-assisted key generation and application for digital watermarks. The term "human-assisted key generation" is used because in practice, the information describing how the random or pseudo random sequence key is to be applied must be stored with the key sequence. It is, in essence, part of the key itself, since the random or pseudo random sequence alone is not enough to encode, or possibly decode the watermark.

Encoding of digital watermarks into a content signal can be done in the time domain, by modifying content samples on a sample by sample basis, or in the frequency domain, by first performing a mathematical
5 transform on a series of content samples in order to convert them into frequency domain information, subsequently modifying the frequency domain information with the watermark, and reverse transforming it back into time-based samples. The conversion between time
10 and frequency domains can be accomplished by means of any of a class of mathematical transforms, known in general as "Fourier Transforms." There are various algorithmic implementations and optimizations in computer source code to enable computers to perform such
15 transform calculations. The frequency domain method can be used to perform "spread spectrum" encoding implementations. Spread spectrum techniques are described in the prior art patents disclosed. Some of the shortcomings evident in these techniques relate to
20 the fixed parameters for signal insertion in a sub audible level of the frequency-based domain, e.g., U.S. Patent No. 5,319,735 Preuss et al. A straightforward randomization attack may be engaged to remove the signal by simply over-encoding random information continuously
25 in all sub-bands of the spread spectrum signal band, which is fixed and well defined. Since the Preuss patent relies on masking effects to render the watermark signal, which is encoded at -15 dB relative to the carrier signal, inaudible, such a randomization attack
30 will not result in audible artifacts in the carrier signal, or degradation of the content. More worrisome, the signal is not the original but a composite of an actual frequency in a known domain combined with another signal to create a "facsimile" or approximation, said to
35 be imperceptible to a human observer, of the original copy. What results is the forced maintenance of one

original to compare against subsequent "suspect" copies for examination. Human-assisted watermarking would provide an improvement over the art by providing flexibility as to where information signals would be inserted into content while giving the content creator the ability to check all subsequent copies without the requirement of a single original or master copy for comparison. Thus the present invention provides for a system where all necessary information is contained within the watermark itself.

Among other improvements over the art, generation of keys and encoding with human assistance would allow for a better match of a given informational signal (be it an ISRC code, an audio or voice file, serial number, or other "file" format) to the underlying content given differences in the make-up of the multitudes of forms of content (classical music, CD-ROM versions of the popular game DOOM, personal HTML Web pages, virtual reality simulations, etc.) and the ultimate wishes of the content creator or his agents. This translates into a better ability to maximize the watermark signal level, so as to force maximal damage to the content signal when there is an attempt to erase a watermark without the key. For instance, an engineer could select only the sections of a digital audio recording where there were high levels of distortion present in the original recording, while omitting those sections with relatively "pure" components from the watermark process. This then allows the engineer to encode the watermark at a relatively higher signal level in the selected sections without causing audible artifacts in the signal, since the changes to the signal caused by the watermark encoding will be masked by the distortion. A party wanting to erase the watermark has no idea, however, where or at what level a watermark is encoded, and so must choose to "exase" at the maximum level across the

entire data stream, to be sure they have obliterated every instance of a watermark.

In the present invention, the input provided by the engineer is directly and immediately reflected in a graphical representation of content of that input, in a manner such that it is overlaid on a representation of the recorded signal. The key generation "envelope" described by the engineer can be dictated to vary dynamically over time, as the engineer chooses. The graphical representation of the content is typically rendered on a two dimensional computer screen, with a segment of the signal over time proceeding horizontally across the screen. The vertical axis is used to distinguish various frequency bands in the signal, while the cells described by the intersection of vertical and horizontal unit lines can signify relative amplitude values by either a brightness or a color value on the display.

Another possible configuration and operation of the system would use a display mapping time on the horizontal axis versus signal amplitude on the vertical axis. This is particularly useful for digital audio signals. In this case, an engineer could indicate certain time segments, perhaps those containing a highly distorted signal, to be used for watermark encoding, while other segments, which contain relatively pure signals, concentrated in a few bandwidths, may be exempt from watermarking. The engineer using a time vs. amplitude assisted key generation configuration would generally not input frequency limiting information.

In practice, the system might be used by an engineer or other user as follows:

The engineer loads a file containing the digitized content stream to be watermarked onto a computer. The engineer runs the key generation application and opens the file to be watermarked. The application opens a

window which contains a graphical representation of the digitized samples. Typically, for digital audio, the engineer would see a rectangular area with time on the horizontal axis, frequency bands on the vertical axis, and varying color or brightness signifying signal power at a particular time and frequency band. Each vertical slice of the rectangle represents the frequency components, and their respective amplitude, at a particular instant ("small increment") of time.

Typically, the display also provides means for scrolling from one end of the stream to the other if it is too long to fit on the screen, and for zooming in or out magnification in time or frequency. For the engineer, this rectangular area acts as a canvas. Using a mouse and/or keyboard, the engineer can scroll through the signal slowly marking out time segments or frequency band minima and maxima which dictate where, at what frequencies, and at what encoding signal level a watermark signal is to be encoded into the content, given a random or pseudo random key sequence. The engineer may limit these marks to all, none or any of the types of information discussed above. When the engineer is finished annotating the content signal, he or she selects a key generation function. At this point, all the annotated information is saved in a record and a random or pseudo random key sequence is generated associated with other information. At some later point, this combined key record can be used to encode and/or decode a watermark into this signal, or additional instances of it.

A suitable pseudo-random binary sequence for use as a key may be generated by: collecting some random timing information based on user keystrokes input to a keyboard device attached to the computer, performing a secure one way hash operation on this random timing data, using the results of the hash to seed a block cipher algorithm

loop, and then cycling the block cipher and collecting a sequence of 1s and 0s from the cipher's output, until a pseudo-random sequence of 1s and 0s of desired length is obtained.

5 The key and its application information can then be saved together in a single database record within a database established for the purpose of archiving such information, and sorting and accessing it by particular criteria. This database should be encrypted with a
10 passphrase to prevent the theft of its contents from the storage medium.

 Another improvement in the invention is support for alternate encoding algorithm support. This can be accomplished for any function which relates to the
15 encoding of the digital watermark by associating with the pseudo-random string of 1s and 0s comprising the pseudo-random key, a list of references to the appropriate functions for accomplishing the encoding. For a given function, these references can indicate a
20 particular version of the function to use, or an entirely new one. The references can take the form of integer indexes which reference chunks of computer code, of alphanumeric strings which name such "code resources," or the memory address of the entry point of
25 a piece of code already resident in computer memory. Such references are not, however, limited to the above examples. In the implementation of software, based on this and previous filings, each key contains associated references to functions identified as CODEC - basic
30 encode/decode algorithm which encodes and decodes bits of information directly to and from the content signal, MAP - a function which relates the bits of the key to the content stream, FILTER - a function which describes how to pre-filter the content signal, prior to encoding
35 or decoding, CIPHER - a function which provides encryption and decryption services for information

contained in the watermark, and ERRCODE - a function which further encodes/decodes watermark information so that errors introduced into a watermark may be corrected after extraction from the content signal.

5 Additionally, a new method of synchronizing decoder software to an embedded watermark is described. In a previous disclosure, a method whereby a marker sequence of N random bits was generated, and used to signal the start of an encoded watermark was described. When the
10 decoder recognizes the N bit sequence, it knows it is synchronized. In that system the chance of a false positive synchronization was estimated at $1/(N^2)$ ("one over (N to the power of 2)"). While that method is fairly reliable, it depends on the marker being encoded
15 as part of the steganographic process, into the content stream. While errors in the encoded bits may be partially offset by error coding techniques, error coding the marker will require more computation and complexity in the system. It also does not completely
20 eliminate the possibility that a randomization attack can succeed in destroying the marker. A new method is implemented in which the encoder pre-processes the digital sample stream, calculating where watermark information will be encoded. As it is doing this, it
25 notes the starting position of each complete watermark, and records to a file, a sequence of N-bits representing sample information corresponding to the start of the watermark, for instance, the 3rd most significant bit of the 256 samples immediately preceding the start of a
30 watermark. This would be a 256 bit marker. The order in which these markers are encountered is preserved, as it is important. The decoder then searches for matches to these markers. It processes the markers from first to last, discarding each as it is found, or possibly not
35 found within a certain scanning distance, and proceeding with the remaining markers. This method does not modify

the original signal with marker information and has the added benefit that high-significance sequences can be used, requiring that an attack based on randomizing markers do very obvious damage to the content stream.

5 With multichannel encoding, both private and public keys, similar in use to those from public-key cryptosystems, could be provided for authentication by concerned third party vendors and consumers, as well as contribute to better management and protection of
10 copyrights for the digital world that already exist in the physical world. For more information on public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig. In addition, any number of key "designations"
15 between "public" and "private" could be established, to provide various access privileges to different groups. Multi-channel watermarks are effected by encoding separate watermark certificates with separate keys by either interleaving windows in the time domain or by
20 using separate frequency bands in the frequency domain. For instance, 3 separate watermarks could be encoded by using every third sample window processed to encode a corresponding certificate. Alternatively, complete watermarks could be interleaved. Similarly, the
25 frequency range of an audio recording might be partitioned into 3 sub-ranges for such a purpose. Use of multi-channel watermarks would allow groups with varying access privileges to access watermark information in a given content signal. The methods of
30 multichannel encoding would further provide for more holographic and inexpensive maintenance of copyrights by parties that have differing levels of access priority as decided by the ultimate owner or publisher of the underlying content. Some watermarks could even play
35 significant roles in adhering to given filtering (for example, content that is not intended for all

observers), distribution, and even pricing schemes for given pieces of content. Further, on-the-fly watermarking could enhance identification of pieces of content that are traded between a number of parties or
5 in a number of levels of distribution. Previously discussed patents by Preuss et al. and Greenberg and other similar systems lack this feature.

Further improvements over the prior art include the general capacity and robustness of the given piece of
10 information that can be inserted into media content with digital watermarks, described in *Steganographic Method and Device* and further modified here, versus "spread spectrum-only" methods. First, the spread spectrum technique described in US. Patent No. 5,319,735 Preuss
15 et al. is limited to an encoding rate of 4.3 8-bit symbols per second within a digital audio signal. This is because of the nature of reliability requirements for spread spectrum systems. The methods described in this invention and those of the previous application,
20 "Steganographic Method and Device," do not particularly adhere to the use of such spread spectrum techniques, thus removing such limitation. In the steganographic derived implementation the inventors have developed based on these filings, watermarks of approximately
25 1,000 bytes (or 1000x 8 bits) were encoded at a rate of more than 2 complete watermarks per second into the carrier signal. The carrier signal was a two channel (stereo) 16-bit, 44.1 KHz recording. The cited encoding rate is per channel. This has been successfully tested
30 in a number of audio signals. While this capacity is likely to decrease by 50% or more as a result of future improvements to the security of the system, it should still far exceed the 4.3 symbols per second envisioned by Preuss et al. Second, the ability exists to recover
35 the watermarked information with a sample of the overall piece of digitized content (that is, for instance, being

able to recover a watermark from just 10 seconds of a 3 minute song, depending on the robustness or size of the data in a given watermark) instead of a full original. Third, the encoding process described in *Steganographic Method and Device* and further modified in this invention explicitly seeks to encode the information signal in such a way with the underlying content signal as to make destruction of the watermark cause destruction of the underlying signal. The prior art describes methods that confuse the outright destruction of the underlying content with "the level of difficulty" of removing or altering information signals that may destroy underlying content. This invention anticipates efforts that can be undertaken with software, such as Digidesign's Sound Designer II or Passport Design's Alchemy, which gives audio engineers (similar authoring software for video also exists, for instance, that sold by Avid Technology, and others as well as the large library of picture authoring tools) very precise control of digital signals, "embedded" or otherwise, that can be purely manipulated in the frequency domain. Such software provides for bandpass filtering and noise elimination options that may be directed at specific ranges of the frequency domain, a ripe method for attack in order to hamper recovery of watermark information encoded in specific frequency ranges.

Separating the decoder from the encoder can limit the ability to reverse the encoding process while providing a reliable method for third parties to be able to make attempts to screen their archives for watermarked content without being able to tamper with all of the actual watermarks. This can be further facilitated by placing separate signals in the content using the encoder, which signal the presence of a valid watermark, e.g. by providing a "public key accessible" watermark channel which contains information comprised

of a digitally signed digital notary registration of the watermark in the private channel, along with a checksum verifying the content stream. The checksum reflects the unique nature of the actual samples which contain the watermark in question, and therefore would provide a means to detect an attempt to graft a watermark lifted from one recording and placed into another recording in an attempt to deceive decoding software of the nature of the recording in question. During encoding, the encoder can leave room within the watermark for the checksum, and analyze the portion of the content stream which will contain the watermark in order to generate the checksum before the watermark is encoded. Once the checksum is computed, the complete watermark certificate, which now contains the checksum, is signed and/or encrypted, which prevents modification of any portion of the certificate, including the checksum, and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders. Once the decoder functions are separate from the encoder, watermark decoding functionality could be embedded in several types of software including search agents, viruses, and automated archive scanners. Such software could then be used to screen files or search out files from archive which contain specific watermark information, types of watermarks, or lack watermarks. For instance, an online service could, as policy, refuse to archive any digital audio file which does not contain a valid watermark notarized by a trusted digital notary. It could then run automated software to continuously scan its archive for digital audio files which lack such watermarks, and erase them.

Watermarks can be generated to contain information to be used in effecting software or content metering services. In order to accomplish this, the watermark

would include various fields selected from the following information:

- title identification;
- unit measure;
- 5 unit price;
- percentage transfer threshold at which liability is incurred to purchaser;
- percent of content transferred;
- authorized purchaser identification;
- 10 seller account identification;
- payment means identification;
- digitally signed information from sender indicating percent of content transferred; and
- digitally signed information from receiver
- 15 indicating percent of content received.

These "metering" watermarks could be dependent on a near continuous exchange of information between the transmitter and receiver of the metered information in question. The idea is that both sides must agree to what

20 the watermark says, by digitally signing it. The sender agrees they have sent a certain amount of a certain title, for instance, and the receiver agrees they have received it, possibly incurring a liability to pay for the information once a certain threshold is passed. If

25 the parties disagree, the transaction can be discontinued before such time. In addition, metering watermarks could contain account information or other payment information which would facilitate the transaction.

30 Watermarks can also be made to contain information pertaining to geographical or electronic distribution restrictions, or which contain information on where to locate other copies of this content, or similar content. For instance, a watermark might stipulate that a

35 recording is for sale only in the United States, or that it is to be sold only to persons connecting to an online

distribution site from a certain set of internet domain names, like ".us" for United States, or ".ny" for New York. Further a watermark might contain one or more URLs describing online sites where similar content that the
5 buyer of a piece of content might be interested in can be found.

A digital notary could also be used in a more general way to register, time stamp and authenticate the information inside a watermark, which is referred to as
10 the certificate. A digital notary processes a document which contains information and assigns to it a unique identification number which is a mathematical function of the contents of the document. The notary also generally includes a time stamp in the document along
15 with the notary's own digital signature to verify the date and time it received and "notarized" the document. After being so notarized, the document cannot be altered in any way without voiding its mathematically computed signature. To further enhance trust in such a system,
20 the notary may publish in a public forum, such as a newspaper, which bears a verifiable date, the notarization signatures of all documents notarized on a given date. This process would significantly enhance the trust placed in a digital watermark extracted for
25 the purpose of use in settling legal disputes over copyright ownership and infringement.

Other "spread spectrum" techniques described in the art have predefined time stamps to serve the purpose of verifying the actual time a particular piece of content
30 is being played by a broadcaster, e.g., U.S. Patent No. 5,379,345 Greenberg, not the insertion and control of a copyright or similar information (such as distribution path, billing, metering) by the owner or publisher of the content. The Greenberg patent focuses almost
35 exclusively on concerns of broadcasters, not content creators who deal with digitized media content when

distributing their copyrightable materials to unknown parties. The methods described are specific to spread spectrum insertion of signals as "segment timing marks" to make comparisons against a specific master of the underlying broadcast material-- again with the intention of specifying if the broadcast was made according to agreed terms with the advertisers. No provisions are made for stamping given audio signals or other digital signals with "purchaser" or publisher information to stamp the individual piece of content in a manner similar to the sales of physical media products (CDs, CD-ROMs, etc.) or other products in general (pizza delivery, direct mail purchases, etc.). In other words, "interval-defining signals," as described in the Greenberg patent, are important for verification of broadcasts of a time-based commodity like time and date-specific, reserved broadcast time, but have little use for individuals trying to specify distribution paths, pricing, or protect copyrights relating to given content which may be used repeatedly by consumers for many years. It would also lack any provisions for the "serialization" and identification of individual copies of media content as it can be distributed or exchanged on the Internet or in other on-line systems (via telephones, cables, or any other electronic transmission media). Finally, the Greenberg patent ties itself specifically to broadcast infrastructure, with the described encoding occurring just before transmission of the content signal via analog or digital broadcast, and decoding occurring upon reception.

While the discussion above has described the invention and its use within specific embodiments, it should be clear to those skilled in the art that numerous modifications may be made to the above without departing from the spirit of the invention, and that the

scope of the above invention is to be limited only by
the claims appended hereto.

What is Claimed:

1 1. A method for using a computer to generate a
2 random or pseudo random key for a digital watermark
3 system wherein said random key includes:
4 a random or pseudo random sequence of binary
5 1s and 0s
6 information describing the application of the
7 random sequence to a stream of digitized samples wherein
8 said information includes:
9 at least one list of time delimiters
10 describing segments of the stream;
11 at least one list of frequency delimiters
12 describing frequency bands to be included in watermark
13 computations; and
14 a signal encoding level;
15 wherein the method comprises the
16 step of receiving human interactive input information
17 used to describe limits on where, at what level, and at
18 what frequencies the random binary information of the
19 random key is to be applied to the stream of digitized
20 samples in encoding the digital watermark;
21 wherein said human interactive input
22 information comprises at least one of the following
23 datum:
24 a list of time delimiters;
25 a list of frequency delimiters; and
26 a signal encoding level.

1 2. The method of claim 1 further comprising the
2 step of selecting said stream of digitized samples from
3 a list provided by a computer system.

1 3. The method of claim 2 further comprising the
2 step of creating and displaying a graphical
3 representation on the display device of the computer

4 system, wherein said graphical representation includes a
5 time axis and a signal frequency axis,

1 4. The method of claim 2 further comprising the
2 step of creating and displaying a graphical
3 representation on the display device of the computer
4 system, wherein said graphical representation includes a
5 time axis and a signal amplitude axis,

1 5. The method of claim 3 or 4, further comprising
2 the step of updating the graphical display to reflect
3 receipt of new human interactive input information.

1 6. The method of claim 5 further comprising the
2 step of generating a random or pseudo random sequence of
3 1s and 0s.

1 7. The method of claim 6 further comprising the
2 step of storing input information in association with
3 the random sequence of 1s and 0s as a single record in a
4 database of such records.

1 8. The method of claim 7 wherein the record is
2 encrypted using a pass phrase.

1 9. The method of claim 1 where the stream of
2 digitized samples contains a digital audio recording.

1 10. The method of claim 1 where the stream of
2 digitized samples to be watermarked contains a digital
3 video recording.

1 11. The method of claim 6 wherein the process of
2 generating the random sequence comprises the steps of:

- 3 (a) collecting a series of random bits
4 derived from keyboard latency intervals in random
5 typing;
- 6 (b) processing the initial series of random
7 bits through a secure one-way hash function;
- 8 (c) using the results of one-way hash
9 function to seed a block encryption cipher loop;
- 10 (d) cycling through the block encryption
11 loop, and extracting the least significant bit of each
12 result after cycle; and
- 13 (e) concatenating the block encryption output
14 bits into the random key sequence

1 12. A method of encoding and decoding a digital
2 watermark where the encoder and decoder are separate
3 software applications or hardware devices.

1 13. The method of claim 12 wherein the decoder
2 functionality is embedded in a software search engine,
3 word-wide web-crawler file scanning engine, intelligent
4 agent, or a virus.

1 14. The method of claim 12 wherein the decoder can
2 access only a limited number of watermark channels,
3 corresponding to public watermark keys, or any keys
4 otherwise made available to said decoder.

1 15. The method of claim 12 wherein the decoder is
2 capable of detecting the presence of a valid watermark
3 but not of accessing the information in the watermark.

1 16. The method of claim 12 wherein the encoder
2 places a separate signal, which does not interfere with
3 the watermark, into a content stream, where said
4 separate signal can indicate

5 watermark synchronization information, which helps
6 locate watermarks in the content; and
7 the presence of a valid watermark in the content.

1 17. A method of using digital watermarks to convey
2 information which is to be used for a content metering
3 service, wherein said watermarks contain at least one of
4 the following pieces of information:

5 title identification;
6 unit measure;
7 unit price;
8 percentage transfer threshold at which liability is
9 incurred to purchaser;
10 percent of content transferred;
11 authorized purchaser identification;
12 seller account identification;
13 payment means identification;
14 digitally signed information from sender indicating
15 percent of content transferred; and
16 digitally signed information from receiver
17 indicating percent of content received.

1 18. A method of encoding digital watermarks which
2 contain information pertaining to distribution
3 restrictions and a location of an addressable directory
4 containing related content, where said watermarks
5 contain at least one of the following pieces of
6 information:

7 geographical constraints on distribution (state,
8 country, etc);
9 logical constraints on distribution;
10 Universal Resource Locator (URL);
11 telephone number;
12 Internet Protocol address;
13 Internet domain name;
14 email address; and

15 file name.

1 19. A method of encoding multiple digital
2 watermarks into a single content stream wherein each
3 watermark is encoded with a separate key.

1 20. The method of claim 18 wherein watermark
2 information from each watermark is interleaved in the
3 time domain.

1 21. A method of claim 18 wherein watermark
2 information from each watermark is placed into specific
3 frequency bands, or interleaved in the frequency domain.

1 22. A method of associating with a pseudo-random
2 key, a list of component function references, which
3 dictate what component functions are applied to the
4 encoding and decoding of a digital watermark using the
5 key in question.

1 23. A method of providing synchronization of a
2 decoder to watermark which consists of the following
3 steps:
4 a) recording a feature of sample stream, or a
5 marker extracted from the sample stream immediately
6 preceding the start of an encoded watermark;
7 b) recording the order in which a list of markers
8 was encountered in the sample stream;
9 c) storing a list of such markers and the order of
10 their appearance in a file for use by the decoder;
11 d) optionally, associating the stored information
12 of step c) with a watermark key or watermark receipt or
13 content title;
14 e) in the decoder, selecting a marker from the file
15 in step c) such that the selected marker is not previous

16 in order to any other marker previously selected in
17 decoding the sample stream in question;
18 f) attempting to find a feature or marker in the
19 portion of the sample stream currently under processing;
20 g) at such time as the currently selected marker is
21 deemed unlikely to be found, discarding it and
22 proceeding to step e);
23 h) at such time as marker is found, decoding the
24 watermark, then proceeding to step e) unless the sample
25 stream is exhausted.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00632

<p>A. CLASSIFICATION OF SUBJECT MATTER</p> <p>IPC(6) : H04L 9/00 US CL : 380/20</p> <p>According to International Patent Classification (IPC) or to both national classification and IPC</p>																										
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols)</p> <p>U.S. : 380/20, 54</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)</p>																										
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>Y, P</td> <td>US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.</td> <td>1-11, 22</td> </tr> <tr> <td>.</td> <td>..</td> <td>.</td> </tr> <tr> <td>.</td> <td>.</td> <td>.</td> </tr> <tr> <td>.</td> <td>..</td> <td>.</td> </tr> <tr> <td>.</td> <td>.</td> <td>.</td> </tr> <tr> <td>.</td> <td>..</td> <td>.</td> </tr> <tr> <td>.</td> <td>.</td> <td>.</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	Y, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																								
Y, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22																								
.	..	.																								
.	.	.																								
.	..	.																								
.	.	.																								
.	..	.																								
.	.	.																								
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.</p>																										
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td>*A* document defining the general state of the art which is not considered to be of particular relevance</td> <td>*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</td> </tr> <tr> <td>*E* earlier document published on or after the international filing date</td> <td>*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</td> </tr> <tr> <td>*L* documents 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)</td> <td>*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</td> </tr> <tr> <td>*O* document referring to an oral disclosure, use, exhibition or other means</td> <td>*Z* document member of the same patent family</td> </tr> <tr> <td>*F* document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table>			*A* document defining the general state of the art which is not considered to be of particular relevance	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	*E* earlier document published on or after the international filing date	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	*L* documents which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	*O* document referring to an oral disclosure, use, exhibition or other means	*Z* document member of the same patent family	*F* document published prior to the international filing date but later than the priority date claimed															
A document defining the general state of the art which is not considered to be of particular relevance	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention																									
E earlier document published on or after the international filing date	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone																									
L documents which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art																									
O document referring to an oral disclosure, use, exhibition or other means	*Z* document member of the same patent family																									
F document published prior to the international filing date but later than the priority date claimed																										
<p>Date of the actual completion of the international search</p> <p>06 MAY 1997</p>		<p>Date of mailing of the international search report</p> <p>09 JUN 1997</p>																								
<p>Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231</p> <p>Facsimile No. (703) 305-3230</p>		<p>Authorized officer</p> <p><i>Salvatore Cangialosi</i> SALVATORE CANGIALOSI</p> <p>Telephone No. (703) 305-1837</p>																								

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-11 and 22

- Remark on Protest**
- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING

This ISA found multiple inventions as follows:

Group I, Claims 1-11, 22, drawn to an method of generating an encrypted digital watermark.

Group II, Claims 12-21 and 23 method of making and using a digital watermark.

The inventions listed as Groups I-II do not relate to a single inventive concept under PCT Rule 13.1 because under PCT Rule 13.2, they lack the same or corresponding technical features for the following Reasons: The invention of Group I lack the separate software, hardware devices or content monitoring. The invention of Group II lack the pseudo-Random key.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification⁶ : G09C 5/00, H04L 9/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 98/02864 (43) International Publication Date: 22 January 1998 (22.01.98)</p>
<p>(21) International Application Number: PCT/US97/11455 (22) International Filing Date: 2 July 1997 (02.07.97) (30) Priority Data: 08/677,435 2 July 1996 (02.07.96) US (71) Applicant: THE DICE COMPANY (US/US); Townhouse 4, 20191 E. Country Club Drive, Avventura, FL 33180 (US). (72) Inventors: MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Avventura, FL 33180 (US); COOPER- MAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US). (74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).</p>	<p>(81) Designated States: AU, BR, CN, JP, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	
<p>(54) Title: OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA</p>		
<p>(57) Abstract</p> <p>The implementations of digital watermarks can be optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video and other multimedia works. Watermark application parameters can be adapted to the individual characteristics of a given digital sample stream. Watermark information can be either carried in individual samples or in relationships between multiple samples, such as in a waveform shape. More optimal models may be obtained to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with different frequency and time components. The highest quality of a given content signal may be maintained as it is mastered, with the watermark suitably hidden, taking into account usage of digital filters and error correction. The quality of the underlying content signals can be used to identify and highlight advantageous locations for the insertion of digital watermarks. The watermark is integrated as closely as possible to the content signal, at a maximum level to force degradation of the content signal when attempts are made to remove the watermarks.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

**OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION
AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA**

RELATED APPLICATIONS

This application is related to patent applications entitled
"Steganographic Method and Device", Serial No. 08/489,172 filed on June
7, 1995; "Method for Human-Assisted Random Key Generation and
5 Application for Digital Watermark System", Serial No. 08/587,944 filed on
January 17, 1996; "Method for Stega-Cipher Protection of Computer Code",
Serial No. 08/587,943 filed on January 17, 1996; "Digital Information
Commodities Exchange", Serial No. 08/365,454 filed on December 28,
1994, which is a continuation of Serial No. 08/083,593 filed on June 30,
10 1993; and "Exchange Mechanisms for Digital Information Packages with
Bandwidth Securitization, Multichannel Digital Watermarks, and Key
Management", Serial No. 08/674,726 filed on July 2, 1996. These related
applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606,
15 "Digital Information Commodities Exchange", issued on June 27, 1995,
which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to digital watermarks.
20 Digital watermarks exist at a convergence point where creators and
publishers of digitized multimedia content demand localized, secured

identification and authentication of that content. Because existence of piracy is clearly a disincentive to the digital distribution of copyrighted works, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality degradation will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data to the content in such a manner that the content must undergo damage, and therefore a reduction in value, with subsequent, unauthorized distribution of the content, whether it be commercial or otherwise.

Legal recognition and attitude shifts, which recognize the importance of digital watermarks as a necessary component of commercially distributed content (audio, video, game, etc.), will further the development of acceptable parameters for the exchange of such content by the various parties engaged in the commercial distribution of digital content. These parties may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for various forms of delivery, on-line retailers, individuals and parties that participate in the transfer of funds to arbitrate the actual delivery of content to intended parties.

Since the characteristics of digital recordings vary widely, it is a worthwhile goal to provide tools to describe an optimized envelope of parameters for inserting, protecting and detecting digital watermarks in a given digitized sample (audio, video, virtual reality, etc.) stream. The optimization techniques described hereinafter make unauthorized removal of digital watermarks containing these parameters a significantly costly operation in terms of the absolute given projected economic gain from undetected commercial distribution. The optimization techniques, at the least, require significant damage to the content signal, as to make the

unauthorized copy commercially worthless, if the digital watermark is removed, absent the use of extremely expensive tools.

Presumably, the commercial value of some works will dictate some level of piracy not detectable in practice and deemed "reasonable" by rights holders given the overall economic return. For example, there will always be fake \$100 bills, LEVI jeans, and GUCCI bags, given the sizes of the overall markets and potential economic returns for pirates in these markets-- as there also will be unauthorized copies of works of music, operating systems (Windows95, etc.), video and future multimedia goods.

However, what differentiates the "digital marketplace" from the physical marketplace is the absence of any scheme that establishes responsibility and trust in the authenticity of goods. For physical products, corporations and governments mark the goods and monitor manufacturing capacity and sales to estimate loss from piracy. There also exist reinforcing mechanisms, including legal, electronic, and informational campaigns to better educate consumers.

SUMMARY OF THE INVENTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape. The present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with

pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

The present invention additionally relates to a method for obtaining more optimal models to design watermark systems that are tamper-resistant
5 given the number and breadth of existent digitized-sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its
10 watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

The present invention additionally preserves quality of underlying content signals, while using methods for quantifying this quality to identify
15 and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

The present invention relates to a method for amplitude independent encoding of digital watermark information in a signal including steps of
20 determining in the signal a sample window having a minimum and a maximum, determining a quantization interval of the sample window, normalizing the sample window, normalizing the sample window to provide
25 normalized samples, analyzing the normalized samples, comparing the normalized samples to message bits, adjusting the quantization level of the sample window to correspond to the message bit when a bit conflicts with the quantization level and de-normalizing the analyzed samples.

The present invention also relates to a method for amplitude
30 independent decoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a

maximum, determining a quantization interval of the sample window, normalizing the sample window to provide samples, and analyzing the quantization level of the samples to determine a message bit value.

The present invention additionally relates to a method of encoding
5 and decoding watermarks in a signal where, rather than individual samples, insertion and detection of abstract signal features to carry watermark information in the signal is done.

The present invention also relates to a method for pre-analyzing a digital signal for encoding digital watermarks using an optimal digital filter in
10 which it is determined what noise elements in the digital signal will be removed by the optimal digital filter based on response characteristics of the filter.

The present invention also relates to a method of error coding watermark message certificates using cross-interleaved codes which use
15 error codes of high redundancy, including codes with Hamming distances of greater than or equal to "n", wherein "n" is a number of bits in a message block.

The present invention additionally relates to a method of pre-processing a watermark message certificate including a step of determining
20 an absolute bit length of the watermark message as it will be encoded.

The present invention additionally relates to a method of generating watermark pseudo-random key bits using a non-linear (chaotic) generator or
25 to a method of mapping pseudo-random key and processing state information to affect an encode/decode map using a non-linear (chaotic) generator.

The present invention additionally relates to a method of guaranteeing watermark certificate uniqueness including a step of attaching
a time stamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

30 The present invention also relates to a method of generating and quantizing a local noise signal to contain watermark information where the

noise signal is a function of at least one variable which depends on key and processing state information.

The present invention also relates to a method of dithering watermark quantizations such that the dither changes an absolute quantization value,
5 but does not change a quantization level or information carried in the quantization.

The present invention further relates to a method of encoding watermarks including inverting at least one watermark bit stream and encoding a watermark including the inverted watermark bit stream.

10 The present invention also relates to a method of decoding watermarks by considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks, and decoding based on those considerations.

The present invention also relates to a method of encoding and
15 decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and randomized over both frequency and time.

The present invention additionally relates to a method of analyzing composite digitized signals for watermarks including obtaining a composite
20 signal, obtaining an unwatermarked sample signal, time aligning the unwatermarked sample signal to the composite signal, gain adjusting the time aligned unwatermarked sample signal to the composite signal, estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal, estimating a watermarked sample
25 signal by subtracting the estimated pre-composite signal for the composite signal, and scanning the estimated watermark sample signal for watermarks.

The present invention additionally relates to a method for varying watermark encode/decode algorithms automatically during the encoding or
30 decoding of a watermark including steps of (a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use

of particular CODECs, (b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and f) receiving the output samples from step (e).

The present invention also relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark, including steps of (a) assigning a list of desired CODECs to a list of index values which correspond to values computed to values computed as a function of the pseudo-random watermark key and the state of the processing framework, (b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and (f) receiving the output samples from step (e).

20

DETAILED DESCRIPTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally sampled audio, video, and other multimedia works.

25

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape.

30

For example, in the same manner a US \$100 bill has copy protection features including ink type, paper stock, fiber, angles of artwork that distort in photocopier machines, inserted magnetic strips, and composite art, the present invention envisions natural extensions for digital watermarks that
5 may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

There are a number of hardware and software approaches in the
10 prior art that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copy protection in the hands of the content creator as the content is created, nor provides an economically feasible model for
15 exchanging the content to be exchanged with identification data embedded within the content.

Yet, given the existence of over 100 million personal computers and many more non-copy-protected consumer electronic goods, copy protection seems to belong within the signals. After all, the playing (i.e., using) of the
20 content establishes its commercial value.

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data (i.e., a means of securing the delivery of copyrighted material from one location to another by using
25 variations of public key cryptography or other more centralized cryptosystems).

Cryptolopes are suited specifically for copyrighted text that is time-sensitive, such as newspapers, where intellectual property rights and origin data are made a permanent part of the file. For information on public-key
30 cryptosystems see U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Rivest et al.,

and U.S. Patent No. 4,424,414 to Hellman et al. Systems are proposed by IBM and Electronic Publishing Resources to accomplish cryptographic container security.

Digitally-sampled copyrighted material, that is binary data on a fundamental level, is a special case because of its long term value coupled with the ease and perfectness of copying and transmission by general purpose computing and telecommunications devices. In particular, in digitally-sampled material, there is no loss of quality in copies and no identifiable differences between one copy and any other subsequent copy. For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised absent the use of digital watermarks to establish responsibility for specific copies and unauthorized copying. Absent digital watermarks, the unlikely instance of a market of trusted parties who report any distribution or exchange of unauthorized copies of the protected work must be relied upon for enforcement. Simply, content creators still cannot independently verify watermarks should they choose to do so.

For a discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 to Moskowitz

In combining steganographic methods for insertion of information identifying the title, copyright holder, pricing, distribution path, licensed owner of a particular copy, or a myriad of other related information, with pseudo-random keys (which map insertion location of the information) similar to those used in cryptographic applications, randomly placed signals (digital watermarks) can be encoded as random noise in a content signal. Optimal planning of digital watermark insertion can be based on the inversion of optimal digital filters to establish or map areas comprising a given content signal insertion envelope. Taken further, planning operations will vary for different digitized content: audio, video, multimedia, virtual reality, etc. Optimization techniques for processes are described in the

depending related applications entitled "Steganographic Method and Device" and "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

Optimization processes must take into consideration the general art of digitization systems where sampling and quantizing are fundamental physical parameters. For instance, discrete time sampling has a natural limit if packets of time are used, estimated at 1×10^{-12} second. This provides a natural limit to the sampling operation. Also, since noise is preferable to distortion, quantizing will vary given different storage mediums (magnetic, optical, etc.) or transmission mediums (copper, fiber optic, satellite, etc.) for given digitized samples (audio, video, etc.). Reducing random bit error, quantization error, burst error, and the like is done for the singular goal of preserving quality in a given digitized sample. Theoretical perfect error correction is not efficient, given the requirement of a huge allocation of redundant data to detect and correct errors. In the absence of such overhead, all error correction is still based on data redundancy and requires the following operations: error detection to check data validity, error correction to replace erroneous data, and error concealment to hide large errors or substitute data for insufficient data correction. Even with perfect error correction, the goal of a workable digital watermark system for the protection of copyrights would be to distribute copies that are less than perfect but not perceptibly different from the original. Ironically, in the present distribution of multimedia, this is the approach taken by content creators when faced with such distribution mechanisms as the INTERNET. As an example, for audio clips commercially exchanged on the World Wide Web (WWW), a part of the INTERNET, 8 bit sampled audio or audio downsampled from 44.1 kHz (CD-quality), to 22 kHz and lower. Digital filters, however, are not ideal because of trade-offs between attenuation and time-domain response, but provide the engineer or similarly-trained individual with a set of decisions to make about maximizing content quality with minimum data overhead and consideration of the ultimate delivery

mechanism for the content (CDs, cable television, satellite, audio tape, stereo amplifier, etc.)

For audio signals and more generally for other frequency-based content, such as video, one method of using digital filters is to include the use of an input filter to prevent frequency aliasing higher than the so-called Nyquist frequencies. The Nyquist theorem specifies that the sampling frequency must be at least twice the highest signal frequency of the sampled information (e.g., for the case of audio, human perception of audio frequencies is in a range between 20 Hz and 20 kHz). Without an input filter, aliases can still occur leaving an aliased signal in the original bandwidth that cannot be removed.

Even with anti-aliasing filters, quantization error can still cause low level aliasing which may be removed with a dither technique. Dither is a method of adding random noise to the signal, and is used to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed, but at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Thus, dither is done at low signal levels, effecting only the least significant bits of the samples. Conversely, digital watermarks, which are essentially randomly-mapped noise, are intended to be inserted into samples of digitized content in a manner such as to maximize encoding levels while minimizing any perceivable artifacts that would indicate their presence or allow for removal by filters, and without destroying the content signal. Further, digital watermarks should be inserted with processes that necessitate random searching in the content signal for watermarks if an attacker lacks the keys. Attempts to over-encode noise into known watermarked signal locations to eliminate the information signal can be made difficult or impossible without damaging the content signal by relying on temporal encoding and randomization in the generation of keys during digital watermark insertion. As a result, although the

watermark occupies only a small percentage of the signal, an attacker is forced to over-encode the entire signal at the highest encoding level, which creates audible artifacts.

The present invention relates to methods for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

Additionally, where a watermark location is determined in a random or pseudo-random operation dependent on the creation of a pseudo-random key, as described in copending related application entitled "Steganographic Method and Device" assigned to the present assignee, and unlike other forms of manipulating digitized sample streams to improve quality or encode known frequency ranges, an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion. Robustness is improved through highly redundant error correction codes and interleaving, including codes known generally as q-ary Bose-Chaudhuri-Hocquenghem (BCH) codes, a subset of Hamming coding operations, and codes combining error correction and interleaving, such as the Cross-Interleave Reed-Solomon Code. Using such codes to store watermark information in the signal increases the number of changes required to obliterate a given watermark. Preprocessing the certificate by considering error correction and the introduction of random data to make watermark discovery more difficult, prior to watermarking, will help determine sufficient key size. More generally, absolute key size can be

determined through preprocessing the message and the actual digital watermark (a file including information regarding the copyright owner, publisher, or some other party in the chain of exchange of the content) to compute the absolute encoded bit stream and limiting or adjusting the key size parameter to optimize the usage of key bits. The number of bits in the primary key should match or exceed the number of bits in the watermark message, to prevent redundant usage of key bits. Optimally, the number of bits in the primary key should exactly match the watermark size, since any extra bits are wasted computation.

5
10
15
Insertion of informational signals into content signals and ranges from applications that originate in spread spectrum techniques have been contemplated. More detailed discussions are included in copending related applications entitled "Steganographic Method and Device" and entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The following discussion illustrates some previously disclosed systems and their weaknesses.

Typically, previously disclosed systems lack emphasis or implementation of any pseudo-random operations to determine the insertion location, or map, of information signals relating to the watermarks. Instead, previous implementations provide "copy protect" flags in obvious, apparent and easily removable locations. Further, previous implementations do not emphasize the alteration of the content signal upon removal of the copy protection.

25
30
Standards for digital audio tape (DAT) prescribe insertion of data such as ISRC (Industry Standard Recording Codes) codes, title, and time in sub-code according to the Serial Copy Management System (SCMS) to prevent multiple copying of the content. One time copying is permitted, however, and systems with AES3 connectors, which essentially override copy protection in the sub-code as implemented by SCMS, actually have no copy limitations. The present invention provides improvement over this

Implementation with regard to the ability of unscrupulous users to load digital data into unprotected systems, such general computing devices, that may store the audio clip in a generalized file format to be distributed over an on-line system for further duplication. The security of SCMS (Serial Copy Management System) can only exist as far as the support of similarly-oriented hardware and the lack of attempts by those skilled in the art to simply remove the subcode data in question.

Previous methods seek to protect content, but shortcomings are apparent. U.S. Patent No. 5,319,735 to Preuss et al. discusses a spread spectrum method that would allow for over-encoding of the described, thus known, frequency range and is severely limited in the amount of data that can be encoded— 4.3 8-bit symbols per second. However, with the Preuss et al. method, randomization attacks will not result in audible artifacts in the carrier signal, or degradation of the content as the information signal is in the subaudible range. It is important to note the difference in application between spread spectrum in military field use for protection of real-time radio signals, and encoding information into static audio files. In the protection of real-time communications, spread spectrum has anti-jam features, since information is sent over several channels at once. Therefore, in order to jam the signal, one has to jam all channels, including their own. In a static audio file, however, an attacker has practically unlimited time and processing power to randomize each sub-channel in the signaling band without penalty to themselves, so the anti-jam advantages of spread spectrum do not extend to this domain.

In a completely different implementation, U.S. Patent No. 5,379,345 to Greenberg seeks enforcement of broadcast contracts using a spread spectrum modulator to insert signals that are then confirmed by a spread spectrum-capable receiver to establish the timing and length that a given, marked advertisement is played. This information is measured against a specific master of the underlying broadcast material. The Greenberg patent does not ensure that real-time downloads of copyrighted content can be

marked with identification information unless all download access points (PCs, modems, etc.), and upload points for that matter, have spread spectrum devices for monitoring.

Other methods include techniques similar to those disclosed in
5 related copending patent applications mentioned above by the present assignee, but lack the pseudo-random dimension of those patent applications for securing the location of the signals inserted into the content. One implementation conducted by Michael Gerzon and Peter Craven, and described by Ken Pohlmann in the 3rd edition of Principles of Digital Audio,
10 illustrates a technology called "buried data technique," but does not address the importance of randomness in establishing the insertion locations of the informational signals in a given content signal, as no pseudo-random methods are used as a basis for insertion. The overriding concern of the "buried data techniques" appears to be to provide for a "known channel" to
15 be inserted in such a manner as to leave little or no perceivable artifacts in the content signal while prescribing the exact location of the information (i.e., replacing the least significant bits (LSB) in a given information signal). In Gerzon and Craven's example, a 20-bit signal gives way to 4-bits of LSBs for adding about 27 dB of noise to the music. Per channel data insertion
20 reached 176.4 kilobits per second per channel, or 352.8 kbps with stereo channels. Similarly attempted data insertion by the present inventors using random data insertion yielded similar rates. The described techniques may be invaluable to manufacturers seeking to support improvements in audio, video and multimedia quality improvements. These include multiple audio
25 channel support, surround sound, compressed information on dynamic range, or any combination of these and similar data to improve quality. Unfortunately, this does little or nothing to protect the interests of copyright holders from unscrupulous pirates, as they attempt to create unmarked, perfect copies of copyrighted works.

30 The present invention also relates to copending patent applications

entitled "Steganographic Method and Device"; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System"; and "Method for Stega-Cipher Protection of Computer Code" as mentioned above, specifically addressing the weakness of inserting

5 informational signals or digital watermarks into known locations or known frequency ranges, which are sub-audible. The present invention seeks to improve on the methods disclosed in these patent applications and other methods by describing specific optimization techniques at the disposal of those skilled in the art. These techniques provide an a la carte method for

10 rethinking error correction, interleaving, digital and analog filters, noise shaping, nonlinear random location mapping in digitized samples, hashing, or making unique individual watermarks, localized noise signal mimic encoding to defeat noise filtering over the entire sample stream, super audible spread spectrum techniques, watermark inversion, preanalyzing

15 watermark key noise signatures, and derivative analysis of suspect samples against original masters to evaluate the existence of watermarks with statistical techniques.

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave few or no artifacts in the

20 underlying content signal, while maximizing its encoding level and location sensitivity in the signal to force damage to the content signal when removal is attempted. The present invention establishes methods for estimating and utilizing parameters, given principles of the digitization of multimedia content (audio, video, virtual reality, etc.), to create an optimized "envelope"

25 for insertion of watermarks, and thus establish secured responsibility for digitally sampled content. The pseudo-random key that is generated is the only map to access the information signal while not compromising the quality of the content. A digital watermark naturally resists attempts at removal because it exists as purely random or pseudo-random noise in a

30 given digitized sample. At the same time, inversion techniques and mimicking operations, as well as encoding signal features instead of given

samples, can make the removal of each and every unique encoded watermark in a given content signal economically infeasible (given the potential commercial returns of the life of a given copyright) or impossible without significantly degrading the quality of the underlying, "protected" signal. Lacking this aesthetic quality, the marketability or commercial value of the copy is correspondingly reduced.

The present invention preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

10 The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

General methods for watermarking digitized content, as well as
15 computer code, are described in copending related patent applications entitled "Steganographic Method and Device" and entitled "Method for Stega-Cipher Protection of Computer Code", both assigned to the present assignee. Recognizing the importance of perceptual encoding of watermarks by the authors and engineers who actually create content is
20 addressed in copending related application entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The present invention describes methods of random noise creation given the necessary consequence of improving signal quality with
25 digitization techniques. Additionally, methods are described for optimizing projections of data redundancy and overhead in error correction methods to better define and generate parameters by which a watermarking system can successfully create random keys and watermark messages that
subsequently cannot be located and erased without possession of the key
30 that acts as the map for finding each encoded watermark. This description will provide the backdrop for establishing truly optimized watermark

insertion including: use of nonlinear (chaotic) generators; error correction and data redundancy analysis to establish a system for optimizing key and watermark message length; and more general issues regarding desired quality relating to the importance of subjecting watermarked content to

5 different models when the content may be distributed or sold in a number of prerecorded media formats or transmitted via different electronic transmission systems; this includes the use of perceptual coding; particularized methods such as noise shaping; evaluating watermark noise signatures for predictability; localized noise function mimic encoding;

10 encoding signal features; randomizing time to sample encoding of watermarks; and, finally, a statistical method for analyzing composite watermarked content against a master sample content to allow watermark recovery. All of these features can be incorporated into specialized digital signal processing microprocessors to apply watermarks to nongeneralized

15 computing devices, such as set-top boxes, video recorders that require time stamping or authentication, digital video disc (DVD) machines and a multitude of other mechanisms that play or record copyrighted content.

The sampling theorem, known specifically as the Nyquist Theorem, proves that bandlimited signals can be sampled, stored, processed,

20 transmitted, reconstructed, desampled or processed as discrete values. In order for the theorem to hold true, the sampling must be done at a frequency that is at least twice the frequency of the highest signal frequency to be captured and reproduced. Aliasing will occur as a form of signal fold over, if the signal contains components above the Nyquist frequency. To

25 establish the highest possible quality in a digital signal, aliasing is prevented by low-pass filtering the input signal to a given digitization system by a low-pass or anti-aliasing filter. Any residue aliasing which may result in signal distortion, relates to another area of signal quality control, namely, quantization error removal.

30 Quantization is required in a digitization system. Because of the continuous nature of an analog signal (amplitude vs. time), a quantized

sample of the signal is an imperfect estimate of the signal sample used to encode it as a series of discrete integers. These numbers are merely estimates of the true value of the signal amplitude. The difference between the true analog value at a discrete time and the quantization value is the
 5 quantization error. The more bits allowed per sample, the greater the accuracy of estimation; however, errors still always will occur. It is the recurrent nature of quantization errors that provides an analogy with the location of digital watermarks.

Thus, methods for removal of quantization errors have relevance in
 10 methods for determining the most secure locations for placement of watermarks to prevent the removal of such watermarks.

The highest fidelity in digital reproduction of a signal occurs at points where the analog signal converges with a given quantization interval. Where there is no such convergence, in varying degrees, the quantization
 15 error will be represented by the following range:

+Q/2 and -Q/2, where Q is the quantization interval.

Indeed, describing maximization of the quantization error and its ratio with the maximum signal amplitude, as measured, will yield a signal-to-error ratio (S/E) which is closely related to the analog signal-to-noise ratio (S/N). To
 20 establish more precise boundaries for determining the S/E, with root mean square (rms) quantization error E_{rms} , and assuming a uniform probability density function 1/Q (amplitude), the following describes the error:

$$E_{rms} = Q/(12)^{1/2}$$

Signal to quantization error is expressed as:

25
$$S/E = (S_{rms}/E_{rms})^2 = 3/2(2^{2n})$$

Finally, in decibels (dB) and comparing 16-bit and 15-bit quantization:

30
$$\begin{aligned} S/E(\text{dB}) &= 10\log[3/2(2^{2n})] = 10\log 3/2 + 2^n \log 2 \\ &(\text{or } = 20\log [(3/2)^{1/2} (2^n)]^2) \\ &= 6.02n + 1.76 \end{aligned}$$

This explains the S/E ratio of 98 dB for 16-bit and 92 dB for 15-bit quantization. The 1.76 factor is established statistically as a result of peak-to-rms ratio of a sinusoidal waveform, but the factor will differ if the signal waveform differs. In complex audio signals, any distortion will exist as white noise across the audible range. Low amplitude signals may alternatively suffer from distortion.

Quantization distortion is directly related with the original signal and is thus contained in the output signal, it is not simply an error. This being the case, implementation of so-called quality control of the signal must use dither. As discussed above, dither is a method of adding random noise to the signal to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Dither, done at low signal levels, effects only the least significant bits of the samples.

Use of linear and nonlinear quantization can effect the trade-off in the output signal and must be considered for a system of watermarks designed to determine acceptable quantization distortion to contain the digital watermark. For audio systems, block linear quantization implementations have been chosen. However, block floating point and floating point systems, nonuniform companding, adaptive delta modulation, adaptive differential pulse-code modulation, and perceptual coding schemes (which are oriented around the design of filters that closely match the actual perception of humans) appear to provide alternative method implementations that would cause higher perceptible noise artifacts if filtering for watermarks was undertaken by pirates. The choice of method is related to the information overhead desired.

According to one aspect of the present invention, the envelope described in the quantization equations above is suitable for preanalysis of a digitized sample to evaluate optimal locations for watermarks. The

present example is for audio, but corresponding applications for digitization of video would be apparent in the quantization of color frequencies.

The matter of dither complicates preanalysis of a sample evaluated for digital watermarks. Therefore, the present invention also defines the optimal envelope more closely given the three types of dither (this example is for audio, others exist for video): triangular probability density function (pdf), Gaussian pdf, and rectangular pdf. Again, to establish better boundaries for the random or pseudo-random insertion of a watermark to exist in a region of a content signal that would represent an area for hiding watermarks in a manner most likely to cause damage to the content signal if unauthorized searches or removal are undertaken. Dither makes removal of quantization error more economical through lower data overhead in a system by shifting the signal range to decorrelate errors from the underlying signal. When dither is used, the dither noise and signal are quantized together to randomize the error. Dither which is subtractive requires removing the dither signal after requantization and creates total error statistical independence. It would also provide further parameters for digital watermark insertion given the ultimate removal of the dither signal before finalizing the production of the content signal. With nonsubtractive dither, the dither signal is permanently left in the content signal. Errors would not be independent between samples. For this reason, further analysis with the three types of dither should reveal an acceptable dither signal without materially affecting the signal quality.

Some proposed systems for implementing copyright protection into digitally-sampled content, such as that proposed by Digimarc Corporation, predicate the natural occurrence of artifacts that cannot be removed. Methods for creating a digital signature in the minimized error that is evident, as demonstrated by explanations of dither, point out another significant improvement over the art in the system described in the present invention and its antecedents. Every attempt is made to raise the error level of error from LSBs to a level at which erasure necessarily leads to the

degradation of the "protected" content signal. Furthermore, with such a system, pirates are forced to make guesses, and then changes, at a high enough encoding level over a maximum amount of the content signal so as to cause signal degradation, because guessing naturally introduces error.

- 5 Thus, dither affects the present invention's envelope by establishing a minimum encoding level. Any encoding done below the dither level might be erased by the dither.

One embodiment of the present invention may be viewed as the provision of a random-super-level non-subtractive dither which contains
10 information (the digital watermark).

To facilitate understanding of how this does not cause audible artifacts, consider the meaning of such encoding in terms of the S/E ratio. In a normal 16-bit signal, there is a 98 dB S/E according to the equation $S/E = 6.02n + 1.76$. Consider that the encoding of watermark information looks
15 like any other error, except it moves beyond the quantization level, out of the LSBs. If the error is of a magnitude expressed in, say, 8 bits, then at that moment, the signal effectively drops to 8 bits (16-8). This corresponds to a momentary drop in S/E, referred to herein as the momentary S/E. Yet, these errors are relatively few and far between and therefore, since the
20 signal is otherwise comprised of higher-bit samples, a "Perceived S/E" may be derived which is simply the weighted average of the samples using the "Pure S/E" (the samples without watermark information) and those with the Momentary S/E. As a direct consequence, it may be observed that the more sparse the watermark map, the fewer errors introduced in a given range,
25 and the higher the perceived S/E. It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive. In general, it is observed that as long as introduced errors leave resulting samples within an envelope in the sample window described by minimum and maximum values, before error introduction, and the map is sufficiently
30 sparse, the effects are not perceived.

In addition, it is possible to obtain an even higher Perceived S/E by allowing the range of introduced errors to vary between a minimum and maximum amount. This makes the weighted average S/E higher by reducing the average introduced error level. Yet, someone trying to erase a
5 watermark, assuming they knew the maximum level, would have to erase at that level throughout the data, since they would not know how the introduced level varies randomly, and would want to erase all watermarks.

A watermarking cipher could perform this operation and may also introduce the further step of local dither (or other noise) significantly above
10 the quantization amplitude on a window by window basis randomly, to restrict total correlation between the watermark signal and the probability that it remains independent between samples, as with subtractive dither implementations that are mostly concerned with the ultimate removal of the dither signal with requantization. This ability could be used to accomplish
15 signal doping, which adds a degree of random errors that do not contain watermark information so as to prevent differential analysis of multiple watermarked copies. Alternatively, it could be used to mimic a specific noise function in a segment of the signal in order to defeat attempts to filter a particular type of noise over the entire signal. By varying this function
20 between watermarks, it may be guaranteed that any particular filter is of no use over the whole signal. By applying several filters in series, it seems intuitive that the net results would be significantly different from the original signal.

The discussion may be more appropriately introduced with perceptual
25 coding techniques, but a watermarking system could also defeat some detection and correction with dither by inserting watermarks into signal features, instead of signal samples. This would be equivalent to looking for signal characteristics, independent of the overall sample as it exists as a composite of a number of signals. Basically, instead of encoding on a bit
30 per sample basis, one might spread bits over several samples. The point of doing this is that filtering and convolution operations, like "flanging", which

definitely change individual samples on a large scale, might leave intact enough of a recognizable overall signal structure (the relationship between multiple samples) to preserve the watermark information. This may be done by measuring, generalizing, and altering features determined by the relationships between samples or frequency bands. Because quantization is strictly an art of approximation, signal-to-error ratios, and thus the dynamic range of a given system are determined.

The choice of eliminating quantization distortion at the expense of leaving artifacts (not perceptible) is a permanent trade-off evident in all digitization systems which are necessarily based on approximation (the design goal of the present invention in preanalyzing a signal to mask the digital watermarks make imperceptibility possible). The high fidelity of duplication and thus subsequent ability to digitally or electronically transmit the finished content (signal) is favored by consumers and artists alike. Moreover, where there continues to be a question of approximating in quantization— digital watermark systems will have a natural partner in seeking optimized envelopes in the multitude and variety of created digitized content.

Another aspect of optimizing the insertion of digital watermarks regards error correction. Highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. A detailed description follows from the nature of a digitization system— binary data can be corrected or concealed when errors exist. Random bit errors and burst errors differ in their occurrence:

Random bit errors are error bits occurring in a random manner, whereas burst errors may exist over large sequences of the binary data comprising a digitized signal. Outside the scope of the present invention are errors caused by physical objects, such as dust and fingerprints, that contribute to the creation of dropouts are different from the errors addressed herein.

Measuring error with bit-error ratio (BER), block error ratio (BLER) and burst-error length (BERL), however, provides the basis of error correction. Redundancy of data is a focus of the present invention. This data necessarily relies on existing data, the underlying content. To

5 efficiently describe optimal parameters for generating a cryptographic key and the digital watermark message discussion of error correction and error concealment techniques is important.

Forms of error detection include one-bit parity, relying on the mathematical ability to cast out numbers, for binary systems including

10 digitization systems, such as 2. Remainders given odd or even results (parity) that are probabilistically determined to be errors in the data. For more appropriate error detection algorithms, such as Cyclic Redundancy Check Code (CRCC), which are suited for the detection of commonly occurring burst error. Pohlmann (Principles of Digital Audio) notes the high

15 accuracy of CRCC (99.99%) and the truth of the following statements given a k-bit data word with m bits of CRCC, a code word of n bits is formed ($m=n-k$):

- burst errors less than or equal to m bits are always predictable.
- 20 - the detection probability of burst errors of m+1 bits = $1-2^{-(m+1)}$
- the detection probability of burst errors longer than m+1 bits = $1-2^{-m}$
- random errors up to 3 consecutive bits long can be detected.

The medium of content delivery, however, provides the ultimate floor for

25 CRCC design and the remainder of the error correction system.

Error correction techniques can be broken into three categories: methods for algebraic block codes, probabilistic methods for convolutional codes, and cross-interleave code where block codes are used in a convolution structure. As previously discussed, the general class of codes

30 that assist in pointing out the location of error are known generally as Hamming codes, versus CRCC which is a linear block code.

What is important for establishing parameters for determining optimized error coding in systems such as digital audio are more specifically known as Reed-Solomon Codes which are effective methods for correcting burst errors. Certain embodiments of the present invention presuppose the necessity of highly redundant error codes and interleaving, such as that done in Cross Interleave Reed-Solomon Code, to counter burst errors typically resulting from randomization attacks. More generally, certain embodiments of the present invention include the use of Hamming Codes of (n,n) to provide $n-1$ bit error detection and $n-2$ bit error correction. Further, a Hamming distance of n (or greater than n) is significant because of the nature of randomization attacks. Such an attack seeks to randomize the bits of the watermark message. A bit can be either 0 or 1, so any random change has a 50% chance of actually changing a bit from what it was (50% is indicative of perfect randomness). Therefore, one must assume that a good attack will change approximately half the bits (50%). A Hamming distance of n or greater, affords redundancy on a close par with such randomization. In other words, even if half the bits are changed, it would still be possible to recover the message.

Because interleaving and parity makes data robust for error avoidance, certain embodiments of the present invention seek to perform time interleaving to randomly boost momentary S/E ratio and give a better estimate of not removing keys and watermarks that may be subsequently determined to be "errors."

Given a particular digital content signal, parity, interleaving, delay, and cross-interleaving, used for error correction, should be taken into account when preprocessing information to compute absolute size requirements of the encoded bit stream and limiting or adjusting key size parameters to optimize and perhaps further randomize usage of key bits. In addition, these techniques minimize the impact of errors and are thus valuable in creating robust watermarks.

Uncorrected errors can be concealed in digital systems.

Concealment offers a different dynamic to establish insertion parameters for the present invention. Error concealment techniques exist because it is generally more economical to hide some errors instead of requiring overly
5 expensive encoders and decoders and huge information overheads in digitization systems. Muting, interpolation, and methods for signal restoration (removal of noise) relate to methods suggested by the present invention to invert some percentage or number of watermarks so as to ensure that at least some or as many as half of the watermarks must still
10 remain in the content signal to effectively eliminate the other half. Given that a recording contains noise, whether due to watermarks or not, a restoration which "removes" such noise is likely to result in the changing of some bit of the watermark message. Therefore, by inverting every other watermark, it is possible to insure that the very act of such corrections
15 inverts enough watermark bits to create an inverse watermark. This inversion presupposes that the optimized watermark insertion is not truly optimal, given the will of a determined pirate to remove watermarks from particularly valuable content. Ultimately, the inability to resell or openly trade unwatermarked content will help enforce, as well as dictate, the
20 necessity of watermarked content for legal transactions.

The mechanisms discussed above reach physical limits as the intent of signal filtering and error correction are ultimately determined to be effective by humans— decidedly analog creatures. All output devices are thus also analog for playback.

25 The present invention allows for a preprocessed and preanalyzed signal stream and watermark data to be computed to describe an optimized envelope for the insertion of digital watermarks and creation of a pseudo-random key, for a given digitized sample stream. Randomizing the time variable in evaluating discrete sample frames of the content signal to
30 introduce another aspect of randomization could further the successful insertion of a watermark. More importantly, aspects of perceptual coding

are suitable for methods of digital watermarks or super-audible spread spectrum techniques that improve on the art described by the Preuss et al patent described above.

5 The basis for a perceptual coding system, for audio, is psychoacoustics and the analysis of only what the human ear is able to perceive. Similar analysis is conducted for video systems, and some may argue abused, with such approaches as "subliminal seduction" in advertising campaigns. Using the human for design goals is vastly different
10 than describing mathematical or theoretical parameters for watermarks. On some level of digital watermark technology, the two approaches may actually complement each other and provide for a truly optimized model.

 The following example applies to audio applications. However, this example and other examples provided herein are relevant to video systems
15 as well as audio systems. Where a human ear can discern between energy inside and outside the "critical band," (described by Harvey Fletcher) masking can be achieved. This is particularly important as quantization noise can be made imperceptible with perceptual coders given the maintenance of a sampling frequency, decreased word length (data) based
20 on signaling conditions. This is contrasted with the necessary decrease of 6 dB/bit with decreases in the sampling frequency as described above in the explanation of the Nyquist Theorem. Indeed, data quantity can be reduced by 75%. This is an extremely important variable to feed into the preprocessor that evaluates the signal in advance of "imprinting" the digital
25 watermark.

 In multichannel systems, such as MPEG-1, AC-3 and other compression schemes, the data requirement (bits) is proportional to the square root of the number of channels. What is accomplished is masking that is nonexistent perceptually, only acoustically.

30 Taken to another level for digital watermarking, which is necessary for content that may be compressed and decompressed, forward adaptive

allocation of bits and backward adaptive allocation provide for encoding signals into content signals in a manner such that information can be conveyed in the transmission of a given content signal that is subsequently decoded to convey the relatively same audible signal to a signal that carries all of its bits— e.g., no perceptual differences between two signals that differ in bit size. This coding technique must also be preanalyzed to determine the most likely sample bits, or signal components, that will exist in the smaller sized signal. This is also clearly a means to remove digital watermarks placed into LSBs, especially when they do not contribute theoretically perceptible value to the analyzed signal. Further methods for data reduction coding are similarly important for preanalyzing a given content signal prior to watermarking. Frequency domain coders such as subband and transform bands can achieve data reduction of ratios between 4:1 and 12:1. The coders adaptively quantize samples in each subband based on the masking threshold in that subband (See Pohlmann, Principles of Digital Audio). Transform coders, however, convert time domain samples into the frequency domain for accomplishing lossless compression. Hybrid coders combine both subband and transform coding, again with the ultimate goal of reducing the overall amount of data in a given content signal without loss of perceptible quality.

With digital watermarks, descriptive analysis of an information signal is important to preanalyze a given watermark's noise signature. Analysis of this signature versus the preanalysis of the target content signal for optimized insertion location and key/message length, are potentially important components to the overall implementation of a secure watermark. It is important that the noise signature of a digital watermark be unpredictable without the pseudo-random key used to encode it. Noise shaping, thus, has important applications in the implementation of the present invention. In fact, adaptive dither signals can be designed to correlate with a signal so as to mask the additional noise— in this case a digital watermark. This relates to the above discussion of buried data

techniques and becomes independently important for digital watermark systems. Each instance of a watermark, where many are added to a given content signal given the size of the content and the size of the watermark message, can be "noise shaped" and the binary description of the

- 5 watermark signature may be made unique by "hashing" the data that comprises the watermark. Generally, hashing the watermark certificate prior to insertion is recommended to establish differences between the data in each and every watermark "file."

10 Additionally, the present invention provides a framework in which to analyze a composite content signal that is suspected to contain a watermarked sample of a copyrighted work, against an unwatermarked original master of the same sample to determine if the composite content actually contains a copy of a previously watermarked content signal. Such an analysis may be accomplished in the following scenario:

- 15 - Assume the composite signal contains a watermark from the sample.

20 - Assume the provision of the suspect composite signal $C_w(t)$ (w subscript denotes a possible watermark) and the unwatermarked original sample $S_w(t)$. These are the only two recordings the analyzer is likely to have access to.

Now, it is necessary to recover a watermarked sample $S_w(t)$.

25 The methods of digital signal processing allow for the computation of an optimal estimate of a signal. The signal to be estimated is the composite minus the watermarked sample, or $C''_w(t) = C_w(t) - S_w(t)$. The analyzer, however, cannot determine a value of $S_w(t)$, since it does not know which of the many possible $S_w(t)$ signals was used in the composite. However, a close estimate may be obtained by using $S_{wm}(t)$, since watermarking makes relatively minor changes to a signal.

So, $C''_w(t)$ (an estimate of $C'_w(t)$ given $C_w(t)$ and $S_{wm}(t)$) may be obtained.

- 30 Once $C''_w(t)$ is calculated, it is simply subtracted from $C_w(t)$. This yields $S'_w(t) = C_w(t) - C''_w(t)$. If the watermark is robust enough, and the estimate good enough,

then $S'_w(t)$, which is approximately equal to $S_w(t)$, can be processed to extract the watermark. It is simply a matter of attempting watermark decoding against a set of likely encoding key candidates.

Note that although a watermark is initially suspected to be present in the composite, and the process as if it is, the specifics of the watermark are not known, and a watermark is never introduced into the calculations, so a watermark is extracted, it is valid, since it was not introduced by the signal processing operations.

The usefulness of this type of operation is demonstrated in the following scenario:

People are interested in simply proving that their copyrighted sample was dubbed into another recording, not the specifics of ownership of the sample used in the dubbing. So, this implies that only a single, or limited number of watermark keys would be used to mark samples, and hence, the decode key candidates are limited, since the same key would be used to encode simple copyright information which never varies from copy to copy.

There are some problems to solve to accomplish this sort of processing. The sample in question is generally of shorter duration than the composite, and its amplitude may be different from the original. Analysis techniques could use a combination of human-assisted alignment in the time domain, where graphical frequency analysis can indicate the temporal location of a signal which closely matches that of the original sample. In addition, automatic time warping algorithms which time align separate signals, on the assumption they are similar could also be used to solve temporal problems. Finally, once temporal alignment is accomplished, automatic amplitude adjustment could be performed on the original sample to provide an optimal match between the composite section containing the sample and the original sample.

It may be desirable to dynamically vary the encoding/decoding algorithm during the course of encoding/decoding a signal stream with a given watermark. There are two reasons for dynamically varying the encoding/decoding algorithm.

The first reason for dynamically varying the encoding/decoding algorithm is that the characteristics of the signal stream may change between one locality in the stream and another locality in the stream in a way that significantly changes the effects that a given encoding algorithm may have on the
5 perception of that section of the stream on playback. In other words, one may want the encoding algorithm, and by implication, the decoding algorithm, to adapt to changes in the signal stream characteristics that cause relative changes in the effects of the encoding algorithm, so that the encoding process as a whole causes fewer artifacts, while maintaining a certain level of security
10 or encoding a given amount of information.

The second reason for dynamically varying the encoding/decoding algorithm is simply to make more difficult attempts at decoding watermarks without keys. It is obviously a more difficult job to attempt such attacks if the encoding algorithm has been varied. This would require the attacker to guess
15 the correct order in which to use various decoding algorithms.

In addition, other reasons for varying the encoding/decoding algorithms may arise in the future.

Two methods for varying of the encoding/decoding algorithms according to embodiments of the present invention are described herein. The first method
20 corresponded to adaptation to changing signal characteristics. This method requires a continuous analysis of the sample windows comprising the signal stream as passed to the framework. Based on these characteristics, which are mathematically well-defined functions of the sample stream (such as RMS energy, RMS/peak ratio, RMS difference between samples - which could reflect
25 a measure of distortion), a new CODEC module, from among a list of pre-defined CODECs, and the algorithms implemented in them, can be applied to the window in question. For the purpose of this discussion, windows are assumed to be equivalent to frames. And, in a frame-based system, this is a straightforward application of the architecture to provide automated variance of
30 algorithms to encode and decode a single watermark.

The second method for varying of the encoding/decoding algorithms corresponds to increased security. This method is easier, since it does not require the relatively computationally-expensive process of further analyzing the samples in a frame passed to the Framework. In this method, the

5 Framework selects a new CODEC, from among a list of pre-defined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark. Again, this is a straightforward application of framework architecture which provides automated variance of algorithms to encode and decode a single watermark versus limitations evident

10 in the analysis of a single random noise signal inserted over the entire content signal as proposed by Digimarc, NEC, Thom EMI and IBM under the general guise of spread spectrum, embedded signalling schemes.

It is important to note that the modular framework architecture, in which various modules including CODECs are linked to keys, provides a basic method

15 by which the user can manually accomplish such algorithmic variations for independent watermarks. The main difference detailed above is that an automated method to accomplish this can be used within single watermarks.

Automated analysis of composited copyrighted material offers obvious advantages over subjective "human listening" and "human viewing" methods

20 currently used in copyright infringement cases pursued in the courts.

What Is Claimed Is:

1 1. A method for amplitude independent encoding of digital watermark
2 information in a signal, comprising steps of:
3 determining in said signal a sample window having a minimum and a
4 maximum;
5 determining a quantization interval of said sample window, where said
6 quantization interval can be used to quantize normalized window samples;
7 normalizing the sample window to provide normalized samples, where
8 normalized samples conform to a limited range of values, proportional to real
9 sample values, and comprise a representation of the real sample values with a
10 resolution higher than the real range of values, and where the normalized
11 values can be divided by the quantization interval into distinct quantization
12 levels;
13 analyzing the normalized samples to determine quantization levels;
14 comparing the message bits to the corresponding quantization level
15 information from the analyzing step;
16 when a bit conflicts with the quantization level, adjusting the quantization
17 level of said sample window to correspond to the message bit; and
18 de-normalizing the analyzed normalized samples.

1 2. The method according to claim 1, wherein watermark signal
2 characteristics or a watermark certificate can be compressed.

1 3. A method for amplitude independent decoding of digital watermark
2 information in a signal comprising steps of:
3 determining in said signal a sample window having a minimum and a
4 maximum;
5 determining a quantization interval of said sample window, where said
6 quantization interval can be used to quantize normalized window samples;

1 normalizing the sample window to provide samples, where normalized
2 samples conform to a limited range of values, proportional to real sample
3 values, and comprise a representation of the real sample values with a
4 resolution higher than the real range of values, and where the normalized
5 values can be divided by the quantization interval into distinct quantization
6 levels; and
7 analyzing the quantization level of said samples to determine a message
8 bit value.

1 4. The method according to claim 3, wherein watermark signal
2 characteristics or a watermark certificate can be compressed.

1 5. A method of encoding and decoding watermarks in a signal,
2 comprising insertion and detection of abstract signal features in said signal to
3 carry watermark information, wherein said abstract signal features are
4 mathematical functions of the input sample window, and by extension, adjacent
5 sample windows.

1 6. A method of pre-analyzing a digital signal for encoding digital
2 watermarks using a digital filter comprising determining what changes in the
3 digital signal will be affected by the digital filter.

1 7. The method according to claim 6, further comprising a step of
2 encoding watermarks so as to either avoid frequency or time delimited areas of
3 the signal which will be changed by the digital filter, or ensure that the
4 watermark will survive the changes introduced by the digital filter.

1 8. A method of error coding watermark message certificates using
2 cross interleaved codes which use error codes of high redundancy, including
3 codes with Hamming distances of greater than or equal to n , wherein n is a
4 number of bits in a message block.

1 9 A method of pre-processing a watermark message certificate
2 comprising determining an exact length of the watermark message as it will be
3 encoded.

1 10. The method according to claim 9, further comprising a step of
2 generating a watermark key which will provide at least one unique bit for each
3 bit comprising the watermark message.

1 11. A method of generating watermark pseudo-random key bits using
2 a non-linear generator.

1 12. A method of generating watermark pseudo-random key bits using
2 a chaotic generator.

1 13. A method of mapping pseudo-random key and processing state
2 information to effect an encode / decode map using a non-linear generator.

1 14. A method of mapping pseudo-random key and processing state
2 information to effect an encode / decode map using a chaotic generator.

1 15. A method of guaranteeing watermark certificate uniqueness
2 comprising attaching a timestamp or user identification dependent hash or
3 message digest of watermark certificate data to the certificate.

1 16. A method of generating and modulating a local noise signal to
2 contain watermark information, wherein the noise signal is a function of at
3 least one variable which depends on key and processing state information.

1 17. A method of dithering watermark quantizations such that the
2 dither changes an absolute quantization value, but does not change a
3 quantization level or information carried in the quantization.

1 18. A method of encoding watermarks comprising steps of:
2 inverting at least one instance of the watermark bit stream; and
3 encoding at least one instance of the watermark using said inverted
4 instance of the watermark bit stream.

1 19. A method of decoding watermarks comprising steps of:
2 considering an original watermark synchronization marker, an inverted
3 watermark synchronization marker, and inverted watermarks; and
4 decoding based on the considering step.

1 20. A method of encoding and decoding watermarks in a signal
2 using a spread spectrum technique to encode or decode where information is
3 encoded or decoded at audible levels and the encoding and decoding
4 methods are pseudo-random over frequency.

1 21. A method of encoding and decoding watermarks in a signal
2 using a spread spectrum technique to encode or decode where information is
3 encoded or decoded at audible levels and the encoding and decoding
4 methods are pseudo-random over time.

1 22. The method of claim 21, wherein the information is encoded or
2 decoded at audible levels and the encoding and decoding methods are
3 pseudo-random, over both frequency and time.

1 23. A method of analyzing composite digitized signals for
2 watermarks comprising steps of:

3 obtaining a composite signal;
4 obtaining an unwatermarked sample signal;
5 time aligning the unwatermarked sample signal to the
6 composite signal;
7 gain adjusting the time aligned unwatermarked sample signal to
8 a corresponding segment of the composite signal, determined in the
9 time aligning step;
10 estimating a pre-composite signal using the composite signal
11 and the gain adjusted unwatermarked sample signal;
12 estimating a watermarked sample signal by subtracting the
13 estimated pre-composite signal from the composite signal; and
14 scanning the estimated watermarked sample signal for
15 watermarks.

1 24. A method for varying watermark encode/decode algorithms
2 automatically during the encoding or decoding of a watermark comprising
3 steps of:
4 a) assigning a list of desired CODECs to a list of corresponding
5 signal characteristics which indicate use of particular CODECs;
6 b) during encoding/decoding, analyzing characteristics of the
7 current sample frame in the signal stream, prior to delivering the frame to a
8 CODEC;
9 c) looking up the corresponding CODEC from the list of CODECs
10 in step (a) which matches the observed signal characteristics from step (b);
11 d) loading and/or preparing the desired CODEC;
12 e) passing the sample frame to the CODEC selected in step (c);
13 and
14 f) receiving the output samples from step (e).

1 25. The method according to claim 24, wherein watermark signal
2 characteristics or a watermark certificate can be compressed.

- 1 26. A method for varying watermark encode/decode algorithms
2 automatically during the encoding or decoding of a watermark comprising
3 steps of:
- 4 a) assigning a list of desired CODECs to a list of index values
5 which correspond to values computed as a function of the pseudo-random
6 watermark key and the state of the processing framework;
 - 7 b) during encoding/decoding, computing the pseudo-random key
8 index value for the current sample frame in the signal stream, prior to
9 delivering the frame to a CODEC;
 - 10 c) looking up the corresponding CODEC from the list of CODECs
11 in step (a) which matches the index value from step (b);
 - 12 d) loading and/or preparing the desired CODEC;
 - 13 e) passing the sample frame to the CODEC selected in step (c);
 - 14 and
 - 15 f) receiving the output samples from step (e).
- 1 27. The method according to claim 26, wherein watermark signal
2 characteristics or a watermark certificate can be compressed.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/1455

A. CLASSIFICATION OF SUBJECT MATTER		
IPC(6) : G09C 5/00 H04L 9/00 IIS CL. : 380/54, 3, 4, 23, 55, 283/73, 113, 17 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. : 380/54, 3, 4, 23, 55, 49, 51, 59, 283/73, 113, 17		
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)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 5,664,018 A (LEIGHTON) 02 SEPTEMBER 1997	1-27
A, P	US, 5,636,292 A (RHOADS) 03 JUNE 1997	1-27
A, P	US 5,617,119 A (BRIGGS ET AL.) 01 APRIL 1997	1-27
A, P	US 5,568,570 A (RABBANI) 22 OCTOBER 1996	1-27
A, P	US 5,530,759 A (BRAUDAWAY, ET AL.) 25 JUNE 1996	1-27
A	US 5,493,677 A (BALOGH, ET AL.) 20 FEBRUARY 1996	1-27
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:	*Y*	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
A document defining the general state of the art which is not considered to be of particular relevance	*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
B earlier document published on or after the international filing date	*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
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)	*A*	document member of the same patent family
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		
Date of the actual completion of the international search	Date of mailing of the international search report	
23 OCTOBER 1997	23 DEC 1997	
Name and mailing address of the IEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer <i>David Cain</i> DAVID CAIN Telephone No. (703) 305-1836	

Form PCT/ISA/210 (second sheet)(July 1992)*



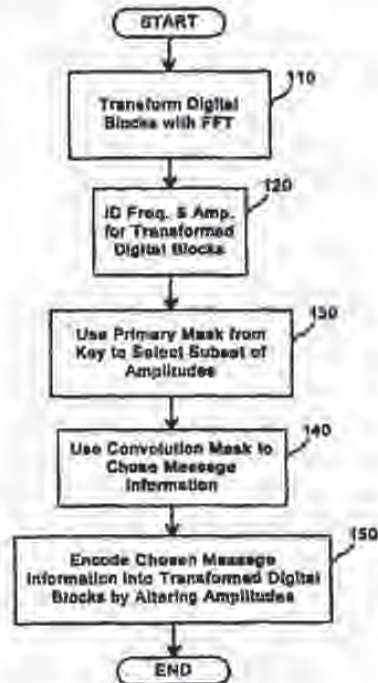
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04N 1/32</p>	<p>A1</p>	<p>(11) International Publication Number: WO 99/52271 (43) International Publication Date: 14 October 1999 (14.10.99)</p>
<p>(21) International Application Number: PCT/US99/07262 (22) International Filing Date: 2 April 1999 (02.04.99) (30) Priority Data: 09/053,628 2 April 1998 (02.04.98) US (71)(72) Applicant and Inventor: MOSKOWITZ, Scott, A. [US/US]; 1671 Collins Avenue #2505, Miami, FL 33160 (US). (74) Agents: CHAPMAN, Floyd, B. et al.; Baker & Botts, L.L.P., The Warner, 1299 Pennsylvania Avenue, N.W., Washing- ton, DC 20004 (US).</p>		<p>(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, MC, NL, PT, SE). Published <i>With international search report.</i></p>

(54) Title: MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

(57) Abstract

Multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

BACKGROUND

5 Field of the Invention

The invention relates to the protection of digital information. More particularly, the invention relates to multiple transform utilization and applications for secure digital watermarking.

Cross-Reference To Related Applications

10 This application claims the benefit of U.S. patent application Serial No. 08/587,943, filed January 17, 1996, entitled "Method for Stega-Cipher Protection of Computer Code," the entire disclosure of which is hereby incorporated by reference.

Description of the Background

15 Increasingly, commercially valuable information is being created and stored in "digital" form. For example, music, photographs and video can all be stored and transmitted as a series of numbers, such as 1's and 0's. Digital techniques let the original information be recreated in a very accurate manner. Unfortunately, digital techniques also let the information be easily copied without the owner's permission.

20 Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand local, secure identification and authentication of content. Because piracy discourages the distribution of valuable digital information, establishing responsibility for copies and derivative copies of such works is important. The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave little or no artifacts, with one standard being perceptibility, 25 in the underlying content signal, while maximizing its encoding level and "location sensitivity" in the signal to force damage to the content signal when removal is attempted. In considering the various forms of multimedia content, whether "master," stereo, National Television Standards Committee (NTSC) video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying 30 commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content undergoes damage, and therefore

reduction of its value, with subsequent unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns and research in the field has provided a rich basis for extremely robust and secure implementations.

Of particular concern is the balance between the value of a digitized "piece" of content and the cost of providing worthwhile "protection" of that content. In a parallel 5 to real world economic behavior, the perceived security of a commercial bank does not cause people to immediately deposit cash because of the expense and time required to perform a bank deposit. For most individuals, possession of a US\$100 bill does not require any protection beyond putting it into a wallet. The existence of the World Wide 10 Web, or "Web," does not implicitly indicate that value has been created for media which can be digitized, such as audio, still images and other media. The Web is simply a medium for information exchange, not a determinant for the commercial value of content. The Web's use to exchange media does, however, provide information that helps determine this value, which is why responsibility over digitized content is 15 desirable. Note that digital watermarks are a tool in this process, but they do not replace other mechanisms for establishing more public issues of ownership, such as copyrights. Digital watermarks, for example, do not replace the "historical average" approach to value content. That is, a market of individuals willing to make a purchase based solely on the perceived value of the content. By way of example, a picture distributed over the 20 Internet, or any other electronic exchange, does not necessarily increase the underlying value of the picture, but the opportunity to reach a greater audience by this form of "broadcast" may be a desirable mechanism to create "potentially" greater market-based valuations. That decision rests solely with the rights holder in question.

Indeed, in many cases, depending on the time value of the content, value may 25 actually be reduced if access is not properly controlled. With a magazine sold on a monthly basis, it is difficult to assess the value of pictures in the magazine beyond the time the magazine is sold. Compact disc valuations similarly have time-based variables, as well as tangible variables such as packaging versus the package-less electronic exchange of the digitized audio signals. The Internet only provides a means 30 to more quickly reach consumers and does not replace the otherwise "market-based"

value. Digital watermarks, properly implemented, add a necessary layer of ownership determination which will greatly assist in determining and assessing value when they are "provably secure." The present invention improves digital watermarking technology while offering a means to properly "tamper proof" digitized content in a manner
5 analogous to methods for establishing authenticity of real world goods.

A general weakness in digital watermark technology relates directly to the way watermarks are implemented. Too many approaches leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This fundamental aspect of various watermark technologies removes proper
10 economic incentives for improvement of the technology when third parties successfully exploit the implementation. One specific form of exploitation obscures subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time.

A set of secure digital watermark implementations address this fundamental control issue, forming the basis of "key-based" approaches. These are covered by the
15 following patents and pending applications, the entire disclosures of which are hereby incorporated by reference: US Patent No. 5,613,004 entitled "Steganographic Method and Device" and its derivative US patent application Serial No. 08/775,216, US patent application Serial No. 08/587,944 entitled "Human Assisted Random Key Generation
20 and Application for Digital Watermark System," US Patent Application Serial No. 08/587,943 entitled "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/677,435 entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data," and US Patent Application Serial No. 08/772,222 entitled "Z-Transform Implementation of
25 Digital Watermarks." Public key crypto-systems are described in US Patents No. 4,200,770, 4,218,582, 4,405,829 and 4,424,414, the entire disclosures of which are also hereby incorporated by reference.

By way of improving these digital watermark security methods, utilization of multiple transforms, manipulation of signal characteristics and the requisite relationship
30 to the mask set or "key" used for encoding and decoding operations are envisioned, as

are optimized combinations of these methods. While encoding a watermark may ultimately differ only slightly in terms of the transforms used in the encoding algorithm, the greater issues of an open, distributed architecture requires more robust approaches to survive attempts at erasure, or even means for making detection of the watermark impossible. These "attacks," when computationally compared, may be diametrically related. For instance, cropping and scaling differ in signal processing orientation, and can result in the weakening of a particular watermarking approach but not all watermarking approaches.

Currently available approaches that encode using either a block-based or entire data set transform necessarily encode data in either the spatial or frequency domains, but never both domains. A simultaneous crop and scale affects the spatial and frequency domains enough to obscure most available watermark systems. The ability to survive multiple manipulations is an obvious benefit to those seeking to ensure the security of their watermarked media. The present invention seeks to improve on key-based approaches to watermarking previously disclosed, while offering greater control of the subsequently watermarked content to rights owners and content creators.

Many currently available still image watermarking applications are fundamentally different from the key-based implementations. Such products include products offered by Digimarc and Signum, which seek to provide a robust watermark by encoding watermark messages that rely entirely on comparisons with the original image for decode operations. The subsequent result of the transform, a discrete cosine transform performed in blocks, is digital signed. The embedded watermarks lack any relationship to the perceptual qualities of the image, making inverse application of the publicly available decoders a very good first line of attack. Similarly, the encoding process may be applied by third parties, as demonstrated by some robustness tests, using one process to encode over the result of an image watermarked with another process. Nonrepudiation of the watermark is not possible, because Digimarc and Signum act as the repository of all registrations of the image's ownership.

Another line of attack is a low pass filter that removes some of the high frequency noise that has been added, making error-free detection difficult or impossible.

Finally, many tests of a simple JPEG transform indicate the watermarks may not survive as JPEG is based on the same transforms as the encoding transforms used by the watermarking process. Other notable implementations, such as that offered by Signafy (developed by NEC researchers), appear to encode watermark messages by performing a transform of the entire image. The goal of this process is to more consistently identify "candidate" watermark bits or regions of the image to encode in perceptually significant regions of the signal. Even so, Signafy relies on the original unwatermarked image to accomplish decoding.

All of these methods still rely on the original unwatermarked image to ensure relatively error-free detection of the watermarks. The steganographic method seeks to provide watermark security without an original unwatermarked copy of the media for decode operations, as well as providing users cryptographic security with ciphered symmetric keys. That is, the same key is used for encode and decode operations. Public key pairs, where each user has a public/private key pair to perform asymmetric encode and decode operations, can also be used. Discussions of public key encryption and the benefits related to encryption are well documented. The growing availability of a public key infrastructure also indicates recognition of provable security. With such key-based implementations of watermarking, security can be off-loaded to the key, providing for a layered approach to security and authentication of the watermark message as well as the watermarked content.

It is known that attacks on the survivability of other implementations are readily available. Interesting network-based attacks on the watermark message are also known which fool the central registration server into assuming an image is owned by someone other than the registered owner. This also substantiates the concern that centralized watermarking technologies are not robust enough to provide proper assurances as to the ownership of a given digitized copy of an multimedia work.

Because the computational requirements of performing multiple transforms may not be prohibitive for certain media types, such as still images and audio, the present invention seeks to provide a means to securely watermark media without the need for an original unwatermarked copy to perform decoding. These transforms may be

performed in a manner not plainly evident to observers or the owner of the content, who may assume the watermark is still detectable. Additionally, where a particular media type is commonly compressed (JPEG, MPEG, etc.), multiple transforms may be used to properly set the mask sets, prior to the watermarking process, to alert a user to

5 survivability prior to the release of a watermarked, and thus perceived, "safe" copy to unknown parties. The result of the present invention is a more realistic approach to watermarking taking the media type, as well as the provable security of the keys into consideration. A more trusted model for electronic commerce is therefore possible.

The creation of an optimized "envelope" for insertion of watermarks to establish

10 secured responsibility for digitally-sampled content provides the basis of much watermark security but is also a complementary goal of the present invention. The predetermined or random key that is generated is not only an essential map to access the hidden information signal, but is also the a subset of the original signal making direct comparisons with the original signal unnecessary. This increases the overall security

15 of the digital watermark.

Survival of simultaneous cropping and scaling is a difficult task with image and audio watermarking, where such transformations are common with the inadvertent use of images and audio, and with intentional attacks on the watermark. The corresponding effects in audio are far more obvious, although watermarks which are strictly

20 "frequency-based," such as variations of spread spectrum, suffer from alignment issues in audio samples which have been "cropped," or clipped from the original length of the piece. Scaling is far more noticeable to the human auditory system, though slight changes may affect frequency-only-type watermarks while not being apparent to a consumer. The far greater threat to available audio watermark applications, most of

25 which are variations of frequency-based embedded signaling, are generally time-based transformations, including time-based compression and expansion of the audio signal. Signafy is an example of spread spectrum-based watermarking, as are applications by Solana Technology, CRL, BBN, MIT, etc. "Spatial domain" approaches are more appropriate designations for the technologies deployed by Digimarc, Signum, ARIS,

30 Arbitron, etc. Interestingly, a time-based approached when considered for images is

basically a "spatial-based" approach. The pixels are "convolutional." The difference being that the "spread spectrum-ed" area of the frequencies is "too" well-defined and thus susceptible to over-encoding of random noise at the same sub-bands as that of the embedded signal.

5 Giovanni uses a block-based approach for the actual watermark. However, it is accompanied by image-recognition capable of restoring a scaled image to its original scale. This "de-scaling" is applied before the image is decoded. Other systems used a "differencing" of the original image with the watermarked image to "de-scale." It is clear that de-scaling is inherently important to the survival of any image, audio or video
10 watermark. What is not clear is that the differencing operation is acceptable from a security standpoint. Moreover, differencing that must be carried out by the watermarking "authority," instead of the user or creator of the image, causes the rights owner to lose control over the original unwatermarked content. Aside from utilizing the mask set within the encoding/decoding key/key pair, the original signal must be
15 used. The original is necessary to perform detection and decoding, although with the attacks described above it is not possible to clearly establish ownership over the watermarked content.

In view of the foregoing, it can be appreciated that a substantial need exists for multiple transform utilization and applications for secure digital watermarking that
20 solve the problems discussed above.

Summary of the Invention

The disadvantages of the art are alleviated to a great extent by multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be
25 protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The

chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.

With these and other advantages and features of the invention that will become hereinafter apparent, the nature of the invention may be more clearly understood by
5 reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

Brief Description of the Drawings

FIG. 1 is a block flow diagram of a method for encoding digital information according to an embodiment of the present invention.

10 FIG. 2 is a block flow diagram of a method for descaling digital information according to an embodiment of the present invention.

FIG. 3 is a block flow diagram of a method for decoding digital information according to an embodiment of the present invention.

Detailed Description

15 In accordance with an embodiment of the present invention, multiple transforms are used with respect to secure digital watermarking. There are two approaches to watermarking using frequency-domain or spatial domain transformations: using small blocks or using the entire data-set. For time-based media, such as audio or video, it is only practical to work in small pieces, since the entire file can be many megabytes in
20 size. For still images, however, the files are usually much smaller and can be transformed in a single operation. The two approaches each have their own strengths. Block-based methods are resistant to cropping. Cropping is the cutting out or removal of portions of the signal. Since the data is stored in small pieces, a crop merely means the loss of a few pieces. As long as enough blocks remain to decode a single, complete
25 watermark, the crop does not remove the mark. Block-based systems, however, are susceptible to scaling. Scaling, such as affine scaling or "shrinking," leads to a loss of the high frequencies of the signal. If the block size is 32 samples and the data is scaled by 200%, the relevant data now covers 64 samples. However, the decoder still thinks that the data is in 32 samples, and therefore only uses half the space necessary to
30 properly read the watermark. Whole-set approaches have the opposite behavior. They

are very good at surviving scaling, since they approach the data as a whole, and generally scale the data to a particular size before encoding. Even a small crop, however, can throw off the alignment of the transform and obscure the watermark.

With the present invention, and by incorporation of previously disclosed material, it is now possible to authenticate an image or song or video with the encoding key/key pair, eliminating false positive matches with cryptography and providing for the communication of a copyright through registration with third party authorities, instead of the original unwatermarked copy.

The present invention provides an obvious improvement over the prior art while improving on previous disclosures by offsetting coordinate values of the original signal onto the key, which are then subsequently used to perform decode or detection operations by the user or authorized "key-holder." This offsetting is necessary with content which may have a watermark "payload," the amount of data that may successfully be encoded, based on Shannon's noisy channel coding theorem, that prevents enough invisible "saturation" of the signal with watermark messages to afford the owner the ability to detect a single message. An example, it is entirely possible that some images may only have enough of a payload to carry a single 100 bit message, or 12 ASCII characters. In audio implementations tested by the present inventor, 1000 bits per second are inaudibly encoded in a 16 bit 44.1 kHz audio signal. Most electronically available images do not have enough data to afford similar "payload" rates. Thus the premise that simultaneous cropping and scaling survival is more difficult for images than a comparable commercially available audio or video track. The added security benefit is that the more limited randomizer of a watermarking system based on spread spectrum or frequency-only applications, the random value of the watermark data "hopping" over a limited signaling band, is that the key is also an independent source of ciphered or random data used to more effectively encode in a random manner. The key may actually have random values larger than the watermark message itself, measured in bits. The watermark decoder is assured that the image is in its original scale, and can decide whether it has been cropped based on its "de-scaled" dimensions.

The benefits of a system requiring keys for watermarking content and validating the distribution of said content is obvious. Different keys may be used to encode different information while secure one way hash functions, digital signatures, or even one-time pads may be incorporated in the key to secure the embedded signal and afford nonrepudiation and validation of the watermarked image and "its" key/key pair. Subsequently, these same keys may be used to later validate the embedded digital signature only, or fully decode the digital watermark message. Publishers can easily stipulate that content not only be digitally watermarked, but that distributors must check the validity of the watermarks by performing digital signature checks with keys that lack any other functionality.

Some discussion of secure digital watermarking has begun to appear. Leighton describes a means to prevent collusion attacks in digital watermarks in US Patent No. 5,664,018. Leighton, however, may not actually provide the security described. For example, in particularly instances where the watermarking technique is linear, the "insertion envelope" or "watermarking space" is well-defined and thus susceptible to attacks less sophisticated than collusion by unauthorized parties. Over encoding at the watermarking encoding level is but one simple attack in such linear implementations. Another consideration ignored by Leighton is that commercially-valuable content in many cases may already exist in a unwatermarked form somewhere, easily accessible to potential pirates, gutting the need for any type of collusive activity. Such examples as compact disc or digitally broadcast video abound. Digitally signing the embedded signal with preprocessing of watermark data is more likely to prevent successful collusion. Depending on the media to be watermarked, highly granular watermarking algorithms are far more likely to successfully encode at a level below anything observable given quantization artifacts, common in all digitally-sampled media, than expectations that a baseline watermark has any functionality.

Furthermore, a "baseline" watermark as disclosed is quite subjective. It is simply described elsewhere in the art as the "perceptually significant" regions of a signal: so making a watermarking function less linear or inverting the insertion of watermarks would seem to provide the same benefit without the additional work

required to create a "baseline" watermark. Indeed, watermarking algorithms should already be capable of defining a target insertion envelope or region without additional steps. Further, earlier disclosed applications by the present invention's inventor describe watermarking techniques that can be set to encode fewer bits than the available watermarking region's "bit-space" or encoding unrelated random noise in addition to watermark data to confuse possible collusive or other attempts at erasure. The region of "candidate bits" can be defined by any number of compression schemes or transformations, and the need to encode all of the bits is simply unnecessary. What is evident is that Leighton does not allow for initial prevention of attacks on an embedded watermark as the content is visibly or audibly unchanged. Moreover, encoding all of the bits may actually act as a security weakness to those who can replicate the regions with a knowledge of the encoding scheme. Again, security must also be offset outside of the actual watermark message to provide a truly robust and secure watermark implementation.

15 In contrast, the present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks. These masks may include primary, convolution and message delimiters but may extend into additional domains such as digital signatures of the message. In previous disclosures, the functionality of these masks is defined solely for mapping. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in descrambling and subsequent detection or decode operation.

25 These same cryptographic protocols can be combined with embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play said streamed content in an unscrambled manner. As with

digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations, where transmission security is a concern.

5 The following describes a sample embodiment of a system that protects digital information according to the present invention. Referring now in detail to the drawings wherein like parts are designated by like reference numerals throughout, there is illustrated in FIG. 1 a block flow diagram of a method for encoding digital information according to an embodiment of the present invention. An image is processed by
10 "blocks," each block being, for example, a 32 x 32 pixel region in a single color channel. At step 110, each block is transformed into the frequency domain using a spectral transform or a Fast Fourier Transform (FFT). The largest 32 amplitudes are identified and a subset of these 32 are selected using the primary mask from the key at steps 120 and 130. One message bit is then encoded into each block at steps 140 and
15 150. The bit is chosen from the message using a transformation table generated using the convolution mask. If the bit is true, the selected amplitudes are reduced by a user defined strength fraction. If the bit is false, the amplitudes are unchanged.

Each of the selected amplitudes and frequencies are stored in the key. After all of the image has been processed, a diagonal stripe of pixels is saved in the key. This
20 stripe can, for example, start in the upper left corner and proceed at a 45 degree angle through the image. The original dimensions of the image are also stored in the key.

FIG. 2 is a block flow diagram of a method for descoding digital information according to an embodiment of the present invention. When an image is chosen to be decoded, it first is checked to determine if it has been cropped and/or scaled. If so, the
25 image is scaled to the original dimensions at step 210. The resulting "stripe," or diagonal line of pixels, is fit against the stripe stored in the key at step 220. If the fit is better than the previous best fit, the scale is saved at steps 230 and 240. If desired, the image can be padded with, for example, a single row or column of zero pixels at step 260 and the process can be repeated to see if the fit improves.

If a perfect fit is found at step 250, the process concludes. If no perfect fit is found, the process continues up to a crop "radius" set by the user. For example, if the crop radius is 4 the image can be padded up to 4 rows and/or 4 columns. The best fit is chosen and the image is restored to its original dimension, with any cropped area
5 replaced by zeroes.

Once the information has been descaled, it can be decoded according to an embodiment of the present invention shown in FIG. 3. Decoding is the inverse process of encoding. The decoded amplitudes are compared with the ones stored in the key in order to determine the position of the encoded bit at steps 310 and 320. The message
10 is assembled using the reverse transformation table at step 330. At step 340, the message is then hashed and the hash is compared with the hash of the original message. The original hash had been stored in the key during encoding. If the hashes match, the message is declared valid and presented to the user at step 350.

Although various embodiments are specifically illustrated and described
15 herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention. Moreover, similar operations have been applied to audio and video content for time-based manipulations of the signal as well as amplitude and pitch operations. The
20 ability to descale or otherwise quickly determine differencing without use of the unwatermarked original is inherently important for secure digital watermarking. It is also necessary to ensure nonrepudiation and third part authentication as digitized content is exchanged over networks.

What is claimed is:

1. A method for encoding a message into digital information, the digital information including a plurality of digital blocks, comprising the steps of:
 - transforming each of the digital blocks into the frequency domain using a spectral transform;
 - 5 identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;
 - selecting a subset of the identified amplitudes for each of the digital blocks using a primary mask from a key;
 - 10 choosing message information from the message using a transformation table generated with a convolution mask; and
 - encoding the chosen message information into each of said transformed digital blocks by altering the selected amplitudes based on the chosen message information.
- 15 2. The method of claim 1 wherein the transforming step comprises:
 - transforming each of the digital blocks into the frequency domain using a fast Fourier transform.
3. The method of claim 2, wherein the digital information contains pixels in a plurality of color channels forming an image, and each of the digital blocks
20 represents a pixel region in one of the color channels.
4. The method of claim 1, wherein the digital information contains audio information.
5. The method of claim 2, wherein said step of identifying comprises:
 - 25 identifying a predetermined number of amplitudes having the largest values for each of the transformed digital blocks.
6. The method of claim 2, wherein the chosen message information is a message bit and wherein said step of encoding comprises the step of:
 - 30 encoding the chosen message bit into each of said transformed digital blocks by reducing the selected amplitudes using a strength fraction if the message bit is true, and not reducing the selected amplitudes if the message bit is false.

7. The method of claim 6, wherein the strength fraction is user defined.

8. The method of claim 2, further comprising the step of storing each of the selected amplitudes and associated frequencies in the key.

9. The method of claim 2, further comprising the step of storing a reference subset of the digital information into the key.

10. The method of claim 2, wherein the digital information contains pixels forming an image; further comprising the steps of:
saving a reference subset of the pixels in the key; and
storing original dimensions of the image in the key.

11. The method of claim 1, wherein the digital information contains audio information, further comprising the steps of:
saving a reference subset of audio information in the key; and
storing original dimensions of the audio signal in the key.

12. The method of claim 10, wherein the reference subset of pixels form a line of pixels in the image.

13. The method of claim 11, wherein the reference subset of audio information includes an amplitude setting.

14. The method of claim 8, wherein the image is a rectangle and the reference subset of pixels form a diagonal of the rectangle.

15. The method of claim 2, further comprising the step of:
requiring a predetermined key to decode the encoded message information.

16. The method of claim 2, further comprising the step of:
requiring a public key pair to decode the encoded message information.

17. The method of claim 2, further comprising the steps of:
calculating an original hash value for the message; and
storing the original hash value in the key.

18. A method for descaling digital information using a key, comprising the steps of:
determining original dimensions of the digital information from the key;
scaling the digital information to the original dimensions;

obtaining a reference subset of information from the key; and
comparing the reference subset with corresponding information in the scaled
digital information.

19. The method of claim 18 wherein the digital information being descaled
5 is a digital image and the step of obtaining a reference subset of information from
the key comprises obtaining a reference subset of pixels from the key.

20. The method of claim 18 wherein the digital information being descaled
is audio digital information and the step of obtaining a reference subset of
information from the key comprises obtaining a reference subset of audio
10 information from the key.

21. The method of claim 19, wherein said step of comparing determines a
first fit value based on the comparison, and wherein the method further comprises
the steps of:

padding the scaled digital image with an area of pad pixels; and
15 re-comparing the reference subset of pixels with corresponding pixels in the
padded image to determine a second fit value.

22. The method of claim 20, wherein the area of pad pixels is a row of single
pixels.

23. The method of claim 20, wherein the area of pad pixels is a column of
20 single pixels.

24. The method of claim 20, wherein said steps of padding and re-comparing
are performed a plurality of times.

25. The method of claim 20, further comprising the step of choosing a best
fit value among the determined fit values and restoring the digital image to the
25 original size, including any pad pixels associated with the best fit value.

26. A method of extracting a message from encoded digital information
using a predetermined key, comprising the steps of:

decoding the encoded digital information into digital information, including
a plurality of digital blocks, using the predetermined key;

transforming each of the digital blocks into the frequency domain using a spectral transform;

identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;

5 selecting a subset of the identified amplitudes for each of the transformed digital blocks using a primary mask from the key;

comparing the selected amplitudes with original amplitudes stored in the predetermined key to determine the position of encoded message information; and

10 assembling the message using the encoded message information and a reverse transformation table.

27. The method of claim 26 wherein the step of transforming comprises:

transforming each of the digital blocks into the frequency domain using a fast Fourier transform.

28. The method of claim 27, further comprising the steps of:

15 calculating a hash value for the assembled message; and

comparing the calculated hash value with an original hash value in the predetermined key.

29. A method for descaling a digital signal using a key, comprising the steps of:

20 determining original dimensions of the digital signal from the key;

scaling the digital signal to the original dimensions;

obtaining a reference signal portion from the key; and

25 comparing the reference signal portion with a corresponding signal portion in the scaled signal.

30. A method for protecting a digital signal comprising the step of:

creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal; and

encoding the digital signal using the predetermined key.

31. The method of claim 30, wherein the digital signal represents a
30 continuous analog waveform.

32. The method of claim 30, wherein the predetermined key comprises a plurality of mask sets.

33. The method of claim 30, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

5 34. The method of claim 30, further comprising the step of:
using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

35. The method of claim 30, wherein the digital signal represents a still image, audio or video.

10 36. The method of claim 30, further comprising the steps of:
selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

validating the mask set at the start of the transfer function-based mask set.

15 37. The method of claim 36, wherein said step of validating comprises the step of:
comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

38. The method of claim 36, wherein said step of validating comprises the step of:

20 comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

39. The method of claim 36, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal;

25 and

wherein said step of validating is dependent on validation of the embedded information.

40. The method of claim 30, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital signal, wherein the hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying the transfer function-based mask set.

41. A method for protecting a digital signal, comprising the steps of:

- 5 creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal;
 authenticating the predetermined key containing the correct transfer function-based mask set during playback of the data; and
 metering the playback of the data to monitor content to determine if the
10 digital signal has been altered.

42. The method of claim 30, wherein the digital signal is a bit stream and further comprising the steps of:

- generating a plurality of masks to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;
15 generating a message bit stream to be encoded;
 loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;
 initializing the state of a primary mask index, a convolution mask index, and a message bit index; and
20 setting a message size equal to the total number of bits in the message bit stream.

43. The method of claim 42 wherein the digital information has a plurality of windows, further comprising the steps of:

- 25 calculating over which windows in the sample stream the message will be encoded;
 computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and
 encoding the computed hash values in an encoded stream of data.

44. The method of claim 40, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

- 5 processing the initial series of random bits through an MD5 algorithm;
 using the results of the MD5 processing to seed a triple-DES encryption loop;
 cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and
 concatenating the triple-DES output bits into the random series of bits.

10

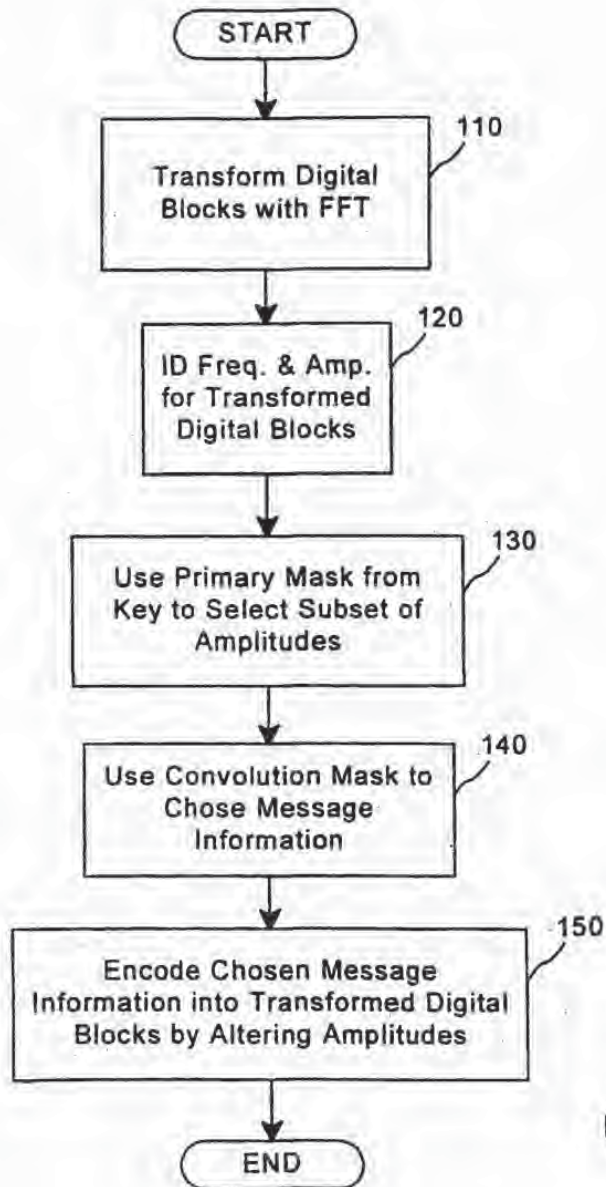


FIG. 1

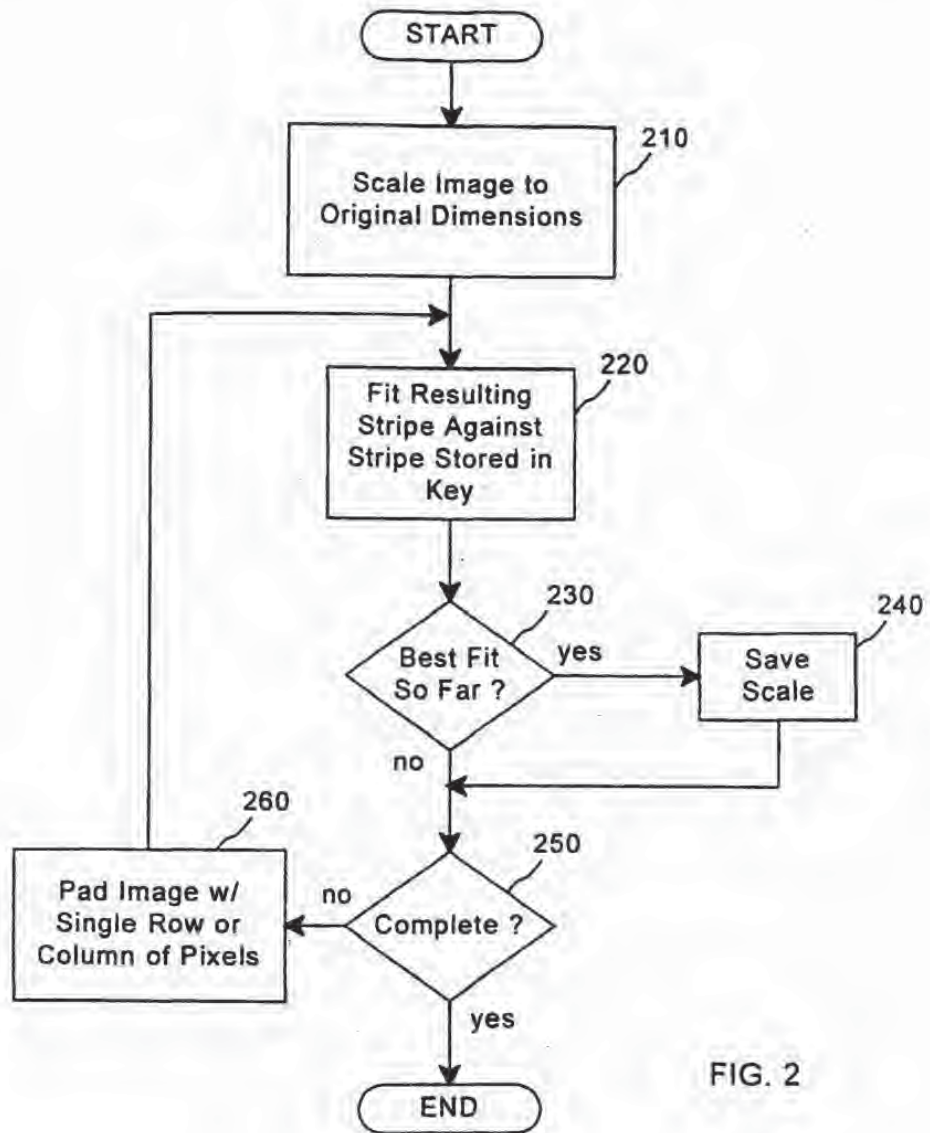


FIG. 2

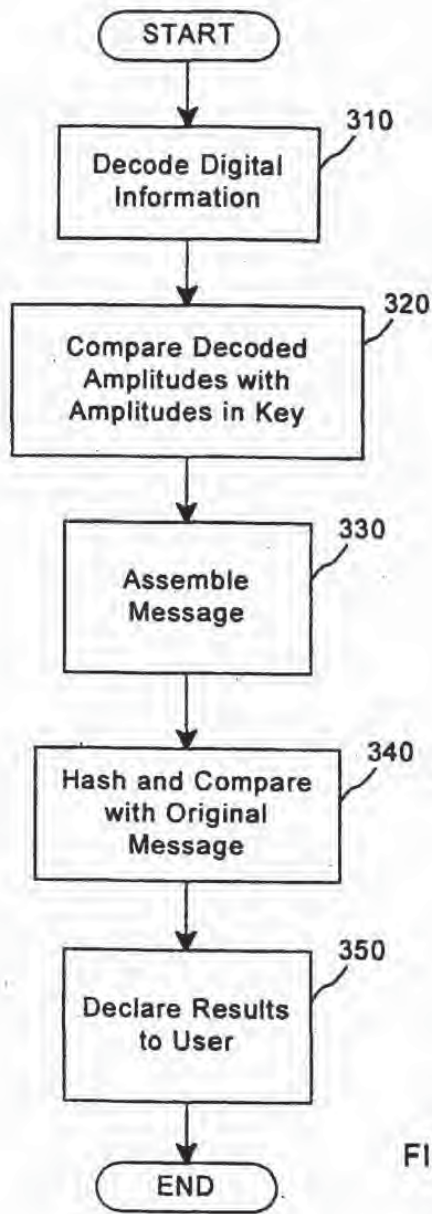


FIG. 3

INTERNATIONAL SEARCH REPORT

Int. Appl. No.
PCT/US 99/07262

<p>A. CLASSIFICATION OF SUBJECT MATTER IPC 6 HO4N1/32</p> <p>According to International Patent Classification (IPC) or to both national classification and IPC</p>										
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols) IPC 6 HO4N HO4L</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched</p> <p>Electronic data base consulted during the international search (name of data base and, where practical, search terms used)</p>										
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category *</th> <th>Classification of document, with indicators, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64</td> <td>1, 2, 15-17, 26-28, 30-38, 42</td> </tr> <tr> <td>A</td> <td>DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document</td> <td>1, 5, 6</td> </tr> </tbody> </table>		Category *	Classification of document, with indicators, where appropriate, of the relevant passages	Relevant to claim No.	A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64	1, 2, 15-17, 26-28, 30-38, 42	A	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document	1, 5, 6
Category *	Classification of document, with indicators, where appropriate, of the relevant passages	Relevant to claim No.								
A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64	1, 2, 15-17, 26-28, 30-38, 42								
A	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document	1, 5, 6								
<p><input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.</p> <p><input checked="" type="checkbox"/> Patent family members are listed in annex.</p>										
<p>* Special categories of cited documents:</p> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*E* earlier document but published on or after the international filing date</p> <p>*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)</p> <p>*O* documents referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p> <p>*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</p> <p>*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</p> <p>*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.</p> <p>*A* document member of the same patent family</p>										
<p>Date of the actual completion of the international search</p> <p>12 July 1999</p>	<p>Date of mailing of the international search report</p> <p>21/07/1999</p>									
<p>Name and mailing address of the ISA</p> <p>European Patent Office, P.O. Box 1, 5011 Patentlaan 1 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx. 31 851 epo nl, Fax: (+31-70) 340-3018</p>	<p>Authorized officer</p> <p>Hubeau, R</p>									

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 99/07262

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING (IC, LAUSANNE, SEPT. 16 - 19, 1996, vol. 3, 16 September 1996 (1996-09-16), pages 227-230, XP002090178 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS ISBN: 0-7803-3259-8 the whole document	1,17,18, 26-28
A	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 6, no. 12, 1 December 1997 (1997-12-01), pages 1673-1686, XP000724633 ISSN: 1057-7149 the whole document	1-3,5,6, 26,27
A,P	PING WAH WONG: "A Public Key Watermark for Image Verification and Authentication" IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, vol. 1, 4 - 7 October 1998, pages 455-459, XP002108799 Los Alamitos, CA, USA the whole document	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/07262

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5613004 A	18-03-1997	EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
		US 5687236 A	11-11-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

Your Ref.: 066358.0102JP

Our Ref.: S-1181-1/002365

JAPANESE TRANSLATION OF PCT APPLICATION

International Patent Application No.

PCT/US99/07262

Date of International Application:

April 2, 1999

TITLE OF THE INVENTION

Multiple Transform Utilization and Applications
for Secure Digital Watermarking

INVENTOR

SCOTT A. MOSKOWITZ

APPLICANT

SCOTT A. MOSKOWITZ

YUASA AND HARA

受領書

平成12年10月 2日

特許庁長官

識別番号 100089705

氏名(名称) 社本 一夫 殿

提出日 平成12年10月 2日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知(事件の表示)
1	国内書面	002365	50001273422	PCT/US99/ 7262

以上

【書類名】 国内書面

【整理番号】 002365

【提出日】 平成12年10月 2日

【あて先】 特許庁長官殿

【出願の表示】

【国際出願番号】 PCT/US99/07262

【出願の区分】 特許

【発明者】

【住所又は居所】 アメリカ合衆国フロリダ州33160、マイアミ、コ
リンズ・アベニュー 16711, ナンバー 2505

【氏名】 モスコウィッツ, スコット・エイ

【特許出願人】

【住所又は居所】 アメリカ合衆国フロリダ州33160、マイアミ、コ
リンズ・アベニュー 16711, ナンバー 2505

【氏名又は名称】 スコット・エイ・モスコウィッツ

【代理人】

【識別番号】 100089705

【住所又は居所】 東京都千代田区大手町二丁目2番1号 新大手町ビル2
06区 ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】 社本 一夫

【電話番号】 03-3270-6641

【選任した代理人】

【識別番号】 100071124

【弁理士】

【氏名又は名称】 今井 庄亮

【選任した代理人】

【識別番号】 100076691

【弁理士】

【氏名又は名称】 増井 忠式
【選任した代理人】
【識別番号】 100075270
【弁理士】
【氏名又は名称】 小林 泰
【選任した代理人】
【識別番号】 100096013
【弁理士】
【氏名又は名称】 富田 博行
【選任した代理人】
【識別番号】 100087424
【弁理士】
【氏名又は名称】 大塚 就彦
【手数料の表示】
【予納台帳番号】 051806
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書の翻訳文 1
【物件名】 図面の翻訳文 1
【物件名】 要約書の翻訳文 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 安全なデジタル透かしのための複数の変換の利用及び適用

【特許請求の範囲】

【請求項1】 メッセージをデジタル情報に符号化する方法であって、前記デジタル情報は複数のデジタル・ブロックを含んでいる。方法において、

前記デジタル・ブロックのそれぞれをスペクトル変換を用いて周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記デジタル・ブロックのそれぞれに対して、鍵からの基本マスクを用いて、前記識別された振幅の部分集合を選択するステップと、

畳み込みマスクを用いて発生された変換テーブルを用いて、前記メッセージからメッセージ情報を選ぶステップと、

前記選ばれたメッセージ情報に基づいて前記選択された振幅を変更することによって、前記選ばれたメッセージ情報を前記変換されたデジタル・ブロックのそれぞれに符号化するステップと、

を含むことを特徴とする方法。

【請求項2】 請求項1記載の方法において、前記変換するステップは、

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを前記周波数領域に変換するステップを含むことを特徴とする方法。

【請求項3】 請求項2記載の方法において、前記デジタル情報は、画像を形成する複数のカラー・チャンネルにおけるピクセルを含み、前記デジタル・ブロックのそれぞれは、前記カラー・チャンネルの1つにおけるピクセル領域を表すことを特徴とする方法。

【請求項4】 請求項1記載の方法において、前記デジタル情報はオーディオ情報を含むことを特徴とする方法。

【請求項5】 請求項2記載の方法において、前記識別するステップは、

前記変換されたデジタル・ブロックのそれぞれに対して最大の値を有する所定の数の振幅を識別するステップを含むことを特徴とする方法。

【請求項6】 請求項2記載の方法において、前記選ばれたメッセージ情報はメッセージ・ビットであり、前記符号化するステップは、

前記メッセージ・ビットが真である場合には強度率を用いて前記選択された振幅を減少させ、前記メッセージ・ビットが偽である場合には前記選択された振幅を減少させないことによって、前記選ばれたメッセージ・ビットを前記変換されたデジタル・ブロックのそれぞれに符号化するステップを含むことを特徴とする方法。

【請求項7】 請求項6記載の方法において、前記強度率はユーザによって定義されることを特徴とする方法。

【請求項8】 請求項2記載の方法において、前記選択された振幅と関連する周波数とのそれぞれを前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項9】 請求項2記載の方法において、前記デジタル情報の基準部分集合を前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項10】 請求項2記載の方法において、前記デジタル情報は画像を形成するピクセルを含んでおり、更に、

前記ピクセルの基準部分集合を前記鍵にセーブするステップと、
前記画像の元の寸法を前記鍵に記憶するステップと、
を含むことを特徴とする方法。

【請求項11】 請求項1記載の方法において、前記デジタル情報はオーディオ情報を含んでおり、更に、

オーディオ情報の基準部分集合を前記鍵にセーブするステップと、
前記オーディオ情報の元の寸法を前記鍵に記憶するステップと、
を含むことを特徴とする方法。

【請求項12】 請求項10記載の方法において、ピクセルの前記基準部分集合は前記画像におけるピクセルの線を形成することを特徴とする方法。

【請求項13】 請求項11記載の方法において、オーディオ情報の前記基準部分集合は振幅設定を含むことを特徴とする方法。

【請求項14】 請求項8記載の方法において、前記画像は矩形であり、ピ

クセルの前記基準部分集合は前記矩形の対角線を形成することを特徴とする方法

【請求項15】 請求項2記載の方法において、

所定の鍵が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項16】 請求項2記載の方法において、

公開鍵の対が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項17】 請求項2記載の方法において、

前記メッセージに対する元のハッシュ値を計算するステップと、
前記元のハッシュ値を前記鍵に記憶するステップと、
を更に含むことを特徴とする方法。

【請求項18】 鍵を用いてでる情報をデスケーリングする方法であって、

前記デジタル情報の元の寸法を前記鍵から決定するステップと、
前記デジタル情報を前記元の寸法にスケーリングするステップと、
情報の基準部分集合を前記鍵から取得するステップと、
前記基準部分集合を前記スケーリングされたデジタル情報における対応する情報と比較するステップと、
を含むことを特徴とする方法。

【請求項19】 請求項18記載の方法において、デスケーリングされる前記デジタル情報はデジタル画像であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からピクセルの基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項20】 請求項18記載の方法において、デスケーリングされる前記デジタル情報はオーディオ・デジタル情報であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からオーディオ情報の基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項21】 請求項19記載の方法において、前記比較するステップは前記比較に基づいて第1の適合する値を決定し、この方法は、更に

前記スケーリングされたデジタル画像をパッド・ピクセルのエリアを用いてパディングするステップと、

ピクセルの前記基準部分集合を前記パディングされた画像における対応するピクセルと再度比較して第2の適合する値を決定するステップと、
を含むことを特徴とする方法。

【請求項22】 請求項20記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのローであることを特徴とする方法。

【請求項23】 請求項20記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのコラムであることを特徴とする方法。

【請求項24】 請求項20記載の方法において、前記パディング及び再度比較するステップは複数回実行されることを特徴とする方法。

【請求項25】 請求項20記載の方法において、前記決定された適合する値の中で最良の適合する値を選び、前記デジタル画像を元のサイズに回復し、前記最良の適合する値と関連する任意のパッド・ピクセルを含むステップを更に含むことを特徴とする方法。

【請求項26】 所定の鍵を用いて符号化されたデジタル情報からメッセージを抽出する方法であって、

前記所定の鍵を用いて、前記符号化されたデジタル情報を複数のデジタル・ブロックを含むデジタル情報に復号化するステップと、

スペクトル変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記鍵からの基本マスクを用いて、前記変換されたデジタル・ブロックのそれぞれに対して、前記識別された振幅の部分集合を選択するステップと、

前記選択された振幅と前記所定の鍵に記憶された元の振幅とを比較し、符号化されたメッセージ情報の位置を決定するステップと、

前記符号化されたメッセージ情報と逆変換テーブルとを用いて、前記メッセージをアセンブルするステップと、

を含むことを特徴とする方法。

【請求項27】 請求項26記載の方法において、前記変換するステップは

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップを含むことを特徴とする方法。

【請求項28】 請求項27記載の方法において、

前記アセンブルされたメッセージに対するハッシュ値を計算するステップと、前記計算されたハッシュ値を前記所定の鍵の中の元のハッシュ値と比較するステップと、

を更に含むことを特徴とする方法。

【請求項29】 鍵を用いてデジタル信号をデスケーリングする方法であって、

前記鍵から前記デジタル信号の元の寸法を決定するステップと、

前記デジタル信号を前記元の寸法にスケーリングするステップと、

前記鍵から基準信号部分を取得するステップと、

前記基準信号部分を前記スケーリングされた信号における対応する信号部分と比較するステップと、

を含むことを特徴とする方法。

【請求項30】 デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とから構成される所定の鍵を作成するステップと、

前記デジタル信号を前記所定の鍵を用いて符号化するステップと、

を含むことを特徴とする方法。

【請求項31】 請求項30記載の方法において、前記デジタル信号は連続的なアナログ波形を表すことを特徴とする方法。

【請求項32】 請求項30記載の方法において、前記所定の鍵は複数のマスク・セットを含むことを特徴とする方法。

【請求項33】 請求項30記載の方法において、前記マスク・セットは、公開鍵と秘密鍵とを含む鍵の対によって暗号化されることを特徴とする方法。

【請求項34】 請求項30記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に符号化するステップを更に含むことを特徴とする方法。

【請求項35】 請求項30記載の方法において、前記デジタル信号は静止画像、オーディオ又はビデオを表すことを特徴とする方法。

【請求項36】 請求項30記載の方法において、

ランダム又は疑似ランダムな一連のビットを有する1つ又は複数のマスクを含むマスク・セットを選択するステップと、

前記マスク・セットを、前記伝達関数ベースのマスク・セットの開始において有効化するステップと、

を更に含むことを特徴とする方法。

【請求項37】 請求項36記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始において計算されたハッシュ値を前記ハッシュ値の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項38】 請求項36記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始におけるデジタル署名を前記デジタル署名の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項39】 請求項36記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に埋め込むステップを更に含む、

前記有効化するステップは、前記埋め込まれた情報の有効化に依存することを特徴とする方法。

【請求項40】 請求項30記載の方法において、

前記デジタル信号においてキャリア信号データの安全な一方ハッシュ関数を

計算するステップを更に含んでおり、前記ハッシュ関数は、前記伝達関数ベースのマスク・セットを搬送する目的で前記キャリア信号の中に導入された変化を感じないことを特徴とする方法。

【請求項41】 デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とで構成された所定の鍵を作成するステップと、

正しい伝達関数ベースのマスク・セットを含む前記所定の鍵を前記データの再生の間に認証するステップと、

前記データの再生を測定してコンテンツをモニタし、前記デジタル信号が変更されたかどうかを判断するステップと、

を含むことを特徴とする方法。

【請求項42】 請求項30記載の方法において、前記デジタル信号はビット・ストリームであり、この方法は、更に、

符号化のために用いられ、ランダム基本マスクと、ランダム畳み込みマスクと、メッセージ・デリミタのランダム開始とを含む複数のマスクを発生するステップと、

符号化されるメッセージ・ビット・ストリームを発生するステップと、

前記メッセージ・ビット・ストリームと、ステガ・サイファ・マップ真理テーブルと、前記基本マスクと、前記畳み込みマスクと、メッセージ・デリミタの前記開始とをメモリにロードするステップと、

基本マスク・インデクスと、畳み込みマスク・インデクスと、メッセージ・ビット・インデクスとの状態を初期化するステップと、

前記メッセージ・ビット・ストリームにおける全ビット数と等しくなるようにメッセージ・サイズを設定するステップと、

を含むことを特徴とする方法。

【請求項43】 請求項42記載の方法において、前記デジタル情報は複数のウィンドウを有しており、この方法は、更に、

サンプル・ストリームにおけるどのウィンドウの上で前記メッセージが符号化されるかを計算するステップと、

前記計算されたウィンドウにおける情報の安全な一方ハッシュ関数を計算するステップであって、前記ハッシュ関数はステガ・サイファによって導かれるサンプルにおける変化を感知しないハッシュ値を発生する、ステップと、

データの符号化されたストリームにおける前記計算されたハッシュ値を符号化するステップと、

を含むことを特徴とする方法。

【請求項44】 請求項40記載の方法において、前記選択するステップは

ランダム・タイピングにおけるキーボード・レイテンシ期間から導かれた一連のランダム・ビットを収集するステップと、

初期の一連のランダム・ビットをMD5アルゴリズムを介して処理するステップと、

前記MD処理の結果を用いて、トリプルDES暗号化ループを供給し、各サイクルの後のそれぞれの結果の最下位ビットを抽出するステップと、

前記トリプルDES出力ビットをランダムな一連のビットの中に連結するステップと、

を含むことを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル情報の保護に関する。更に詳しくは、本発明は、安全なデジタル透かしのための複数の変換の利用及び適用に関する。

【0002】

【関連出願への相互参照】

本発明は、1996年1月17日に出願された米国特許出願第08/587,943号"Method for Stega-Cipher Protection of Computer Code"に基づいて優先権を主張している。この米国特許出願の開示のすべてを、本出願において援用する。

【0003】

【従来の技術】

商業的に価値のある情報が「デジタル」形式で制作され記憶されることが増加している。例えば、音楽、写真及び画像のすべてが、1及び0などの一連の数字として記憶され伝送されることが可能である。デジタル技術によると、元の情報を非常に正確に再生することができる。しかし、不運なことに、デジタル技術によると、その持ち主の許可を得ることなく、情報を容易にコピーすることもできるのである。

【0004】

デジタル透かし（電子透かし、digital watermark）は、デジタル化されたマルチメディア・コンテンツの制作者（creators）と出版業者（publishers）とがコンテンツのローカルで安全な識別及び認証を要求する収束点に存在している。侵害行為（piracy）は貴重なデジタル情報の流通を損なう方向に作用するから、そのような作品のコピーや二次的（derivative）なコピーに対する責任を確立することが重要である。デジタル透かしシステムの目的は、基礎となるコンテンツ信号の中に、ほとんど又は全く痕跡を残すことなく、そして知覚可能であることが標準となるように、与えられた1つ又は複数の情報信号を挿入することである。その際に、基礎となる信号における符号化レベルと位置感度（location sensitivity）とを最大化することにより、この透かしを除去しようと試みるとコンテンツ信号に強制的に損傷が生じるようになっていく。「マスタ」、ステレオ、NTSC（National Television Standards Committee）ビデオ、オーディオ・テープ又はコンパクト・ディスクであるかどうかなど、マルチメディア・コンテンツの様々な形態を考慮すると、真に関する寛容度は、個人ごとに変動し、そのコンテンツの基礎となる商業的及び美的な価値に影響を与える。従って、著作権、所有権（ownership right）、購入者情報又はこれらの何らかの組合せや関連データをそのコンテンツの中に結合させ、それにより、それが商業的であってもそれ以外の態様であっても認証されていない流通がそれ以後なされる場合には、そのコンテンツが損傷を受け、従って、その価値が低下するようにすることが望ましい。デジタル透かしは、このような関心の多くに向けられたものであり、この技術分野における研究は、これまでに、極めて堅固で安全な実現に対する豊かな

基礎を提供してきている。

【0005】

特に関心が向けられているのは、コンテンツのデジタル化された「作品」(piece)の価値とそのコンテンツに値する「保護」を提供するためのコストとのバランスである。現実の世界における経済行動と並行するように、商業銀行の安全性(セキュリティ)を知覚できるからといって、銀行預金をするのに要する費用及び時間のために、人々は直ちに現金を銀行に預金することにはならない。ほとんどの個人にとっては、100米ドルをもっているからといって、それを財布にしまっておく以上の保護が必要とされることはない。また、ワールド・ワイド・ウェブ(WWW)すなわちウェブが存在するからといって、オーディオや、静止画像等の媒体のようなデジタル化することができる媒体に対して価値が創造されたことを意味しない。ウェブは、単に、情報交換のための媒体であり、コンテンツの商業的な価値を決定することはない。しかし、媒体を交換するためにウェブを用いることにより、その価値を決定するのに役立つ情報が提供されるため、デジタル化されたコンテンツに対する責任が要求される。デジタル透かしは、このプロセスにおけるツール(道具)であって、著作権などの法的権利に関するより公的な課題を確立するそれ以外の機構に代わるものではないことに注意してほしい。例えば、デジタル透かしは、コンテンツの価値を判断する際の「履歴平均」(historical average)アプローチに代わるものではない。これは、コンテンツの知覚された価値だけに基づいて購入をしようとする個人の市場(マーケット)のことである。例えば、インターネット又はそれ以外の任意の電子的な交換手段を介して写真が流通しても、その写真の基礎的な価値が増加することは必ずしもない。しかし、そのような形式の「放送」によってより大きな観客に到達する機会が生じることは、「潜在的」により大きな市場に基づく価値を生じさせる望ましい機構でありうる。この決定は、当該権利者のみが唯一なすことができる。

【0006】

実際、多くの場合に、コンテンツの時間的な価値に依存して、アクセスが適切に制御されていない場合には、価値が現実的に低下することがありうる。月刊誌と

して販売されている雑誌の場合には、その雑誌が販売されている期間を超えて、その雑誌に掲載されている写真の価値を評価することは困難である。コンパクト・ディスクの価値に関しても、同様な時間に関する変動要素があるし、デジタル化されたオーディオ信号のパッケージングとパッケージを伴わない電子的な交換とのような有形的な変動要素もある。インターネットは、単に、消費者により迅速に到達する手段を提供するだけであって、それ以外の「市場に基づく」価値に取って代わるものではない。デジタル透かしは、適切に実現されるのであれば、権利者の決定に関する必要な層を追加することになり、デジタル透かしが「証明可能な程度に安全」(provably secure)であるときには、価値を決定し評価する際に大いに役立つ。本発明は、デジタル透かし技術の改良であり、現実世界における商品の真偽判定方法と類似する態様で、デジタル化されたコンテンツを「改ざん不能」(tamper-proof)にする手段を与える。

【0007】

デジタル透かし技術における一般的な弱点は、透かしを実現する方法に関する。ほとんどのアプローチにおいて、保護されるべき作品の制作者ではなくデジタル透かしを実現する者に、検出及び復号制御に関して依存している。様々な透かし技術が有するこの基本的側面のために、第三者がそのようなデジタル透かしの実現を成功裏に利用する際には、この技術の改良に対する適切な経済的インセンティブが失われる。特定の形式の利用がいったんなされると、それ以後の透かしの検出が曖昧になる。そして、それ以後の時点において同じ透かしプロセスを用いた符号化を成功であると思なすことになる。

【0008】

安全なデジタル透かしのいくつかの実現例がこの基本的な制御の課題に取り組んでおり、「キー・ベース」(key-based)のアプローチの基礎を形成している。これらは、以下の米国特許及び出願中の米国特許出願がカバーしている。すなわち、"Steganographic Method and Device"と題する米国特許第5,613,004号及びそれから生じた米国特許出願第0.8/775,216号;"Human Assisted Random Key Generation and Application for Digital Watermark System"と題する米国特許出願第0.8/587,944号;"Method for Stega-Cipher

Protection of Computer Code」と題する米国特許出願第08/587,943号 ; "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data"と題する米国特許出願第08/677,435号 ; 及び Z-Transform implementation of Digital Watermarks」と題する米国特許出願第08/772,222号である。これらの米国特許及び米国特許出願における開示内容は本出願において援用する。公開鍵暗号システムは、米国特許第4,200,770号、第4,218,582号、第4,405,829号及び第4,424,414号に記載されている。これらの米国特許における開示内容は、本出願において援用する。

【0009】

これらのデジタル透かしによるセキュリティ方法を改良することによって、複数の変換を用い、信号特性を操作し、必要な関係を符号化及び復号化動作に用いられるマスク・セットすなわち「鍵」に適用することが、これらの方法の最適化された組合せとして考察される。透かしの符号化は、符号化アルゴリズムにおいて用いられる変換に関して最終的にほんの僅かに異なるが、公開された分散型のアーキテクチャというより大きな課題によって、抹消しようとする試みに打ち勝つ、より堅固なアプローチが要求され、更には、透かしの検出を不可能にする手段が要求される。これらの「攻撃」は、計算論的に比較すると、正反対な態様 (diametrically) で関連している。例えば、クロッピング (cropping) とスケーリング (scaling) とは、信号処理の向きが異なり、結果的には特定の透かしアプローチを脆弱化する可能性があるが、すべての透かしアプローチについてはそういうことはない。

【0010】

ブロック・ベース又は全体のデータ・セット変換のいずれかを用いて符号化を行う現時点で利用できるアプローチは、必ず、空間領域又は周波数領域のどちらか一方においてデータを符号化するが、両方の領域においてそうすることは決してない。同時的なクロッピング及びスケーリングは、空間及び周波数領域に影響し、それによって、使用可能な透かしシステムのほとんどを曖昧にする。複数の操作を生き延びる能力は、透かしの入れられた媒体のセキュリティを確実にしよ

うとしている者にとっては明確な利点である。本発明は、鍵ベースのアプローチを用いて既存の透かしを改良することを目指している。その際に、それ以後に透かしが入れられるコンテンツを権利者やコンテンツ制作者がより広く制御できるようにする。

{0011}

現時点で利用可能な多くの静止画透かしアプリケーションは、鍵ベースの実現例とは根本的に異なっている。これらの製品としては、デジマーク (Digimarc) 社やシグナム (Signum) 社による製品があるが、これらの製品は、復号化動作に関してはオリジナルの画像との比較に完全に依存している透かしメッセージを符号化することによって、堅固 (robust) な透かしを提供することを目指している。ブロックごとに実行される離散コサイン変換である変換のそれ以後の結果は、デジタル的に符号が付される。埋め込まれた透かしは、画像の知覚的な質とは全く関係がなく、従って、一般的に利用可能なデコーダの逆方向の適用が、攻撃の非常によい最初のラインとなる。同様に、符号化プロセスは、第三者によって適用されることもありうる。これは、いくつかの堅固性のテストにおいて示されているように、或るプロセスを用いて他のプロセスを用いて透かしが入れられた画像の結果を符号化するものである。透かしを放棄しないこと (nonrepudiation) はできない。その理由は、デジマーク社とシグナム社とが、画像の権利に関するすべての登録の機関として機能しているからである。

{0012}

攻撃の別のラインとして、エラーのない検出が困難又は不可能であるように追加されている高周波ノイズの一部を除去するローパス・フィルタがある。最終的には、単純なJPEG変換の多くのテストがこのような透かしは生き延びることができないことを示す。その理由は、JPEGが、透かしを入れるプロセスによって用いられる符号化変換と同じ変換に基づいているからである。これ以外の注意すべき実現例としては、例えば、NECの研究者たちによって開発されたシグナファイ (Signafy) によるものなどがあるが、画像の全体の変換を実行することによって、透かしメッセージを符号化しているようである。このプロセスの目的は、画像の「候補となる」透かしビット又は領域をより一貫性をもって識別し

て、信号の知覚的に著しい領域において符号化を行うことである。そうであっても、シグナファイは、復号化を達成するのに、オリジナルの透かしの入れられていない画像に依存する。

【0013】

これらの方法は、すべてが、透かしを比較的エラーのない態様で検出することを確認するために、オリジナルの透かしの入れられていない画像に依然として依存している。ステガノグラフィック (steganographic) な方法では、復号化動作のためにその媒体のオリジナルな透かしの入れられていないコピーを用いることなく透かしのセキュリティを提供すると共に、ユーザに暗号化された鍵を用いて暗号的なセキュリティをも提供することが目的とされる。すなわち、符号化動作と復号化動作とのために、同じ鍵が用いられる。それぞれのユーザが非対称的な符号化及び復号化動作を実行するための公開/秘密鍵対を有するような公開鍵対を用いることもできる。公開鍵暗号に関する議論と暗号化に関する利点とは、広く文書化がなされている。公開鍵インフラストラクチャの利用可能性が増加していることは、証明可能なセキュリティを認識しうるということを示している。透かしの実現化がこのように鍵ベースであることにより、セキュリティについては鍵に依存することが可能であり、それによって、透かしメッセージと透かしの入れられたコンテンツとのセキュリティ及び認証に対する多層化 (layered) されたアプローチが得られる。

【0014】

これ以外の実現例が生き延びること (survivability) に対する攻撃も容易に利用可能であることが知られている。透かしメッセージに対する興味深いネットワーク・ベースの攻撃も知られているが、これは、中央の登録サーバを騙して、画像が登録されている権利者とは別の誰かが権利を有していると想定させるものである。また、これによると、集中的な透かし技術は十分に堅固なものではなく、マルチメディア作品のデジタル化されたコピーの権利者に関する適切な確認を行うことはできないという懸念が現実のものとなる。

【0015】

【発明が解決しようとする課題】

複数の変換を実行することに関する計算論的な要求は、静止画やオーディオなどのある種の媒体にとっては禁止されないものであるから、本発明は、復号化を実行するのにオリジナルの透かしの入れられていないコピーを必要とすることなしに、媒体に確実に透かしを入れる手段を提供することを目的とする。これらの変換は、コンテンツの観察者又は権利者に対して単純には明らかでない態様で実行することができる。しかし、これらの観察者や権利者は、透かしが依然として検出可能であると考えることができる。更に、特定の媒体のタイプが一般的に圧縮されている場合（JPEG、MPEGなど）には、複数の変換を用いて、透かしを入れるプロセスに先立ってマスク・セットを適切に設定し、透かしの入れられた従って知覚された「安全」なコピーを未知の第三者に解放する前に、ユーザに生き残り可能性について警告することができる。本発明の結果は、透かしへのより現実的なアプローチであって、鍵の証明可能なセキュリティだけでなく媒体のタイプも考慮している。従って、電子商取引のためのより信頼性の高いモデルも可能である。

【0016】

透かしを挿入するために最適化された「封筒」を作成し、デジタル的にサンプリングされたコンテンツに対する確実な責任を確立することにより、大きな透かしセキュリティの基礎が得られるが、これは、本発明の補助的な目的である。発生される所定の又はランダムな鍵は、隠された情報信号にアクセスするために不可欠な地図であるだけでなく、オリジナルな信号の部分集合であって、それにより、オリジナルな信号との比較が不要になる。これによって、デジタル透かしの全体的なセキュリティが向上する。

【0017】

同時的なクロッピング及びスケールリングが生き延びること（生き残ること、survival）は、画像及びオーディオ透かしに関しては、困難である。というのは、そのような変換は、画像やオーディオの偶然的（inadvertent）な使用と、透かしへの意図的な攻撃とで共通だからである。対応の効果は、オーディオの場合にはるかに明らかであるが、広帯域の変動などのように狭い意味で「周波数ベース」である透かしは、作品の元の長さから「クロッピング」又はクリップされたオ

オーディオ・サンプルにおけるアライメントの問題を有している。スケーリングは人間の聴覚系にとってはるかにより顕著であるが、僅かな変化が、消費者には明らかではないにもかかわらず、周波数だけのタイプの透かしに影響することがありうる。ほとんどが周波数ベースの埋め込み形信号処理である、利用可能なオーディオ透かしアプリケーションに対するはるかに大きな脅威は、時間ベースの変換であり、これには、オーディオ信号の時間ベースの圧縮及び解凍が含まれる。シグナファイは、広帯域ベースの透かしの例であり、ソラナ (Solana) テクノロジー、CRL、BBN、MITなどによるアプリケーションも同様である。「空間領域」アプローチというのが、デジマルク、シグナム、ARIS、アービトロシ (Arbiter) などによって開発された技術に対するより適切な名称である。興味深いことに、時間ベースのアプローチは、画像について考察される場合には、基本的には空間ベースのアプローチである。ピクセルは、「畳み込み的」(convolutional) である。これら間の差異は、周波数の広帯域化された (spread-spectrum-ed) 領域は「あまりに」うまく定義されているために、埋め込まれた信号と同じサブバンドでのランダム・ノイズの過剰な符号化を受けることになるという点である。

{0018}

ジョバンニ (Giovanni) は、現実の透かしに対して、ブロック・ベースのアプローチを用いる。しかし、それには、スケーリングされた画像をその元のスケールに回復させることができる画像認識が伴っている。この「デスケーリング」は、画像が復号化される前に適用される。他のシステムでは、元の画像を透かし入りの画像と「区別」して「デスケーリング」を行っている。デスケーリングが、あらゆる画像、オーディオ又はビデオ透かしの生き残りにとって固有の重要性を有していることは明らかである。明らかでないのは、区別の動作がセキュリティの見地から受け入れ可能であるが、ということである。更に、画像のユーザ又は制作者ではなく、透かし「機関」によって区別が実行されなければならない場合には、権利者は、元の透かしの入っていないコンテンツを支配できないことになる。符号化/復号化鍵/鍵の対の内部でマスク・セットを用いることは別に元の信号を用いなければならない。オリジナルは、検出及び復号化を実行する

のに必要であるが、以上で説明した攻撃に関しては、透かしの入れられたコンテンツに対する権利を明確に確立することは不可能である。

【0019】

以上を鑑みると、以上で論じた課題を解決する安全なデジタル透かしのための複数の変換の利用及び適用に対する実質的な必要性が存在することを理解することができるであろう。

【0020】

【課題を解決するための手段】

安全なデジタル透かしのための複数の変換の利用及び適用によってこの技術における短所は大幅に改善することができる。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報は、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

【0021】

以下で明らかになる本発明のこれらの及びそれ以外の効果及び特徴により、本発明の性質は、以下で行う本発明の詳細な説明と、冒頭の特許請求の範囲と、添付の図面とを参照することによって、より明確に理解することができるはずである。

【0022】

【発明の実施の形態】

本発明の或る実施例によると、安全なデジタル透かしのために複数の変換が用いられる。周波数領域又は空間領域の変換を用いる透かしには2つのアプローチが存在する。すなわち、小さなブロックを用いる場合とデータ・セット全体を用いる場合とである。オーディオやビデオのような時間ベースの媒体に対しては、

小さな部分において作業するのが実務的である。というのは、ファイル全体では、サイズが数メガバイトにもなりうるからである。しかし、静止画については、ファイルははるかに小さいのが通常であり、1回の操作で変換することができる。2つのアプローチは、それぞれが、各自の利点を有している。ブロック・ベースの方法は、クロッピングに対する抵抗性を有する。クロッピング (cropping) というのは、信号の部分的な切り取り又は除去である。データは複数の小さな部分 (piece) に記憶されるので、クロッピングは、単に、いくつかの部分が失われることを意味する。1つの完全な透かしを復号化するのに十分なブロックが残っている限り、クロッピングによって、その透かしが除去されることはない。しかし、ブロック・ベースのシステムは、スケーリングに弱い。アフィン・スケーリング (affine scaling) 又は「収縮」 (shrinking) などのスケーリングは、信号の高周波の損失につながる。ブロックのサイズが32サンプルであり、データが200%スケーリングされる場合には、関係のあるデータは、64サンプルをカバーすることになる。しかし、デコーダは、依然として、データは32サンプルにあると考えるので、透かしを適切に読み取るのに必要な空間の半分しか用いない。セット全体のアプローチは、逆の振る舞いを有する。このアプローチは、スケーリングを生き延びるのは非常に得意である。その理由は、このアプローチでは、データを全体として扱い、符号化の前にデータを特定のサイズにスケーリングするのが一般的であるからである。しかし、どのように小さなクロッピングであっても、変換のアライメントを混乱させ、透かしを曖昧にしまう可能性がある。

【0023】

本発明を用いると、そして、これまでに開示されている材料を組み入れることによって、符号化鍵/鍵の対を用いて画像や歌やビデオを認証し、暗号による誤った肯定的な一致を排除し、オリジナルな透かしの入れられていない作品の代わりに第三者の権限を備えた登録を通じて著作権の通信を提供することが可能となる。

【0024】

本発明は、従来技術に対する明らかな改良を提供するのであるが、元（オリジ

ナル)の信号の座標値を鍵の上にオフセットし、次にそれを用いてユーザ又は認証を受けた「鍵の持ち主」による復号化又は検出動作が行われることによって、過去に開示された内容に対する改良がなされる。このオフセットは、透かしが、成功裏に符号化されるデータの量を、シャノンのノイズを含むチャネルの符号化定理に基づいて「運ばせる」(パイロードさせる)ことができるコンテンツにおいて必要であり、これによって、透かしメッセージを有する信号の十分に不可視的な「飽和」が回避され、権利者が単一のメッセージを検出することが可能となる。例えば、或る画像が単一の100ビットのメッセージ又は12のASCII文字を運ぶのに十分なパイロードだけを有するというのも、全くありうることである。本発明の発明者によってテストがなされたオーディオでの実現例では、毎秒1000ビットが、16ビットの44.1kHzのオーディオ信号において、不可聴的に符号化される。電子的に利用可能なほとんどの画像は、同じ「パイロード」率を与えることができるほどに十分なデータを有していない。従って、クロッピング及びスケーリングが同時に生き延びることは画像の場合の方が、それに対応する商業的に利用可能なオーディオ又はビデオ・トラックの場合よりも困難であることになる。追加されるセキュリティの効果は、広帯域又は周波数のみのアプリケーションに基づく透かしシステムのランダムライザが制限されているほど、透かしデータのランダム値は、制限された信号帯域上で「ホッピング」することになり、また、鍵もまた、ランダムな態様でより効果的に符号化を行うのに用いられる暗号化された又はランダムなデータの独立なソースである、ということである。鍵は、実際に、ビット数で測定した場合に、透かしメッセージ自体よりも大きなランダム値を有しうる。透かしデコーダは、画像が、そのオリジナルのスケールに含まれていることを求められ、また、その「デスケーリング」された寸法に基づいてクロッピングされたかどうかを決定することができる。

【0025】

コンテンツに透かしを入れそのコンテンツの流通を有効化するために鍵を要求するシステムの利点は明らかである。異なる情報を符号化するには異なる鍵を用いることができる。その際に、安全な一方ハッシュ関数や、デジタル署名や、更には一時的パッド(one-time pads)でさえも鍵の中に組み入れることによつ

て、埋め込まれた信号を保護し、透かしの入れられた画像とその鍵/鍵の対を拒絶せずに有効化することができる。後に、これらの同じ鍵を用いて、埋め込まれたデジタル署名だけを後で有効化する。又は、デジタル透かしメッセージを完全に復号化する。コンテンツにデジタル透かしが入れられているということだけでなく、流通業者はそれ以外にはどのような機能も有していない鍵を用いてデジタル署名のチェックを実行することによって透かしの有効性をチェックしなければならないということも、出版業者は、容易に要求することができる。

【0026】

安全なデジタル透かしが、いくらか論じられ始めている。レイトン (Leighton) は、米国特許第5,664,018号に、デジタル透かしにおける共謀的な攻撃 (collusion attack) を防止する手段を記載している。しかし、レイトンは、記載されているセキュリティを現実的には提供できない可能性がある。例えば、透かし技術が線形であるような特定の場合には、「挿入封筒」又は「透かし空間」が矛盾なく定義されており (well-defined) 。従って、認証を受けていないものによる共謀よりは複雑でない攻撃を受ける可能性がある。透かし符号化レベルにおける過剰符号化 (over encoding) は、そのような線形の実現例における一つの単純な攻撃に過ぎない。レイトンによって無視された別の考慮として、商業的価値のあるコンテンツは、多くの場合に、既に透かしの入れられていない形態でいずれかの場所に既に存在しており、潜在的な侵害行為に容易にさらされる状態にあるので、どのようなタイプの共謀行為も不要であるということがある。この例として、コンパクト・ディスクやデジタル放送されたビデオなど多くがある。透かしデータの前処理を用いて埋め込まれた信号にデジタル署名をすることによって、共謀の成功を回避することができる可能性が大きい。透かしを入れる媒体に依存するが、非常に個別化された (granular) 透かしアルゴリズムは、ベースラインとなる透かしが何らかの機能を有しているという予測よりも、デジタル的にサンプリングがなされるあらゆる媒体において共通な与えられた量子化人工物を、何か観測可能なものよりも低いレベルで成功裏に符号化できる可能性が高い。

【0027】

更に、ここで開示されている「ベースライン」透かしは、かなり主観的なものである。これは、この技術分野のいずれかの場所で信号の「知覚的に意義のある」領域として説明されるだけである。すなわち、透かし関数の線形性を減少させる。又は、透かしの挿入を反転させることにより、「ベースライン」透かしの振幅を小さくせしめるのに要求される追加的な作業なしに同じ効果が得られるように思われる。実際、透かしアルゴリズムは、追加的なステップなしに、ターゲット挿入領域又は領域を既に定義することができるべきである。更に、本発明の発明者によって既に開示されている出願では、透かしデータに加えて、利用可能な透かし領域の「ビット空間」又は符号化とは関係のないランダム・ノイズよりも少ないビットを符号化するように設定することにより、可能性のある攻撃やそれ以外の抹消の試みを混乱させることができる透かし技術が説明されている。「候補ビット」の領域は、任意の数の圧縮方式又は変換によって定義することができ、すべてのビットを符号化する必要はない。更に、すべてのビットを符号化することは、符号化方式を知らずながら領域を複製することができるものによっては、現実的には、セキュリティ上の弱点として作用する可能性がある。やはり、セキュリティは、実際の透かしメッセージの外部にオフセットされていなければならず、それによって、真に堅固で安全な透かしの実現が得られるのである。

【0028】

対照的に、本発明は、様々な暗号化プロトコルを用いて実現し、基礎となるシステムにおける信頼性及びセキュリティの両方を強化することができる。所定の鍵は、マスクの組として説明される。これらのマスクには、基本、畳み込み及びメッセージ・デリミタが含まれるが、メッセージのデジタル署名などの追加的な領域にも拡張することができる。これまでに開示されている技術では、これらのマスクの機能は、写像に対してだけ定義されていた。公開及び秘密鍵を鍵の対として用いて、鍵が危険にさらされる可能性を増加させることができる。符号化の前に、上述のマスクは、暗号的な見地から安全なランダム発生プロセスによって発生される。DESなどのブロック暗号は、十分にランダムなシード値 (seed value) と組み合わせられて、暗号的に安全なランダム・ビット発生器をエミュレートする。これらの鍵は、考察しているサンプル・ストリームにそれら

を一致させる情報と共にデータベースにセーブされ、デスクランプリング（スクランブル解除）や後の検出又は復号化動作に用いられる。

【0029】

これらの同じ暗号化プロトコルを、スクランブルされていない状態でストリームされたコンテンツを正しく表示又は再生するために認証された鍵を要求するストリームされたコンテンツを管理する際に、本発明の実施例と組み合わせることができる。デジタル透かしの場合と同様に、対称的又は非対称的な公開鍵の対が、様々な実現例において用いられる。更に、真正の鍵の対を維持する認証機関に対する必要性も、対称的な鍵の実現例以上のセキュリティを得るためには、伝送の際のセキュリティを考える際には考慮すべき問題となる。

【0030】

次に、本発明によるデジタル情報保護システムの或る実施例を説明する。ここで添付の図面を参照するが、同じ要素については、複数の図面にわたって同じ参照番号が付されている。図1には、本発明の実施例によるデジタル情報符号化方法のブロック流れ図が図解されている。1つの画像が「ブロック」ごとに処理されるのであるが、ここで、各ブロックは、例えば、単色チャネルにおける 32×32 のピクセル領域である。ステップ110では、各ブロックが、スペクトル変換又は高速フーリエ変換（FFT）を用いて、周波数領域に変換される。ステップ120及び130において、最大の 32 の振幅が識別され、これら 32 の中の部分集合が、鍵からの基本マスクを用いて選択される。次に、1メッセージ・ビットが、ステップ140及び150において各ブロックの中に符号化される。このビットは、畳み込みマスクを用いて発生された変換テーブルを用いてメッセージから選ばれる。このビットが真である場合には、選択された振幅は、ユーザによって定義された強度率（Strength Fraction）だけ減少される。ビットが偽である場合には、振幅は不変である。

【0031】

選択された振幅と周波数とは、それぞれが、鍵の中に記憶される。すべての画像が処理された後で、ピクセルの対角線方向のストライプが鍵にセーブされる。このストライプは、例えば、左上の角で開始して、画像を通過して45度の角度で

進むことができる。画像の元の寸法も、鍵に記憶される。

【0032】

図2は、本発明の実施例によるデジタル情報デスケーリング方法のブロック流れ図である。画像が復号化のために選ばれると、最初に、クロッピング及びノ又はスケーリングがなされているかどうかチェックされる。されている場合には、画像は、ステップ210において、元の寸法にスケーリングされる。結果的に得られる「ストライプ」すなわちピクセルの対角線は、ステップ220において、鍵に記憶されているストライプとの適合が調べられる。適合がそれ以前の最良の適合よりも優れている場合には、スケールがステップ230及び240においてセーブされる。望むのであれば、例えば、ステップ260において、ゼロ・ピクセルの単一のロー又はコラムを用いて、画像をパディングすることができる。そして、このプロセスを反復して、適合が改善するかどうかを見ることができる。

【0033】

ステップ250において完全な適合が見出される場合には、プロセスは終了する。完全な適合が得られない場合には、ユーザによって設定されるクロップ「半径」まで、プロセスが継続される。例えば、クロップ半径が4である場合には、画像を、4つのロー及びノ又は4つのコラムまでパディングすることができる。ゼロによって置き換えられた任意のクロッピングされた領域を用いて、最良の適合が選ばれ、画像は、元もとの寸法まで回復される。

【0034】

情報は、いったんデスケーリングされると、図3に示されている本発明の実施例に従って復号化される。復号化は、符号化の逆プロセスである。復号化された振幅は、鍵に記憶されたものと比較され、ステップ310及び320において、符号化されたビットの位置が決定される。メッセージは、ステップ330において、逆変換テーブルを用いてアセンブルされる。次に、ステップ340では、メッセージはハッシュ化され、このハッシュが元のメッセージのハッシュと比較される。元のハッシュは、符号化の間に鍵に記憶される。ハッシュが一致する場合には、メッセージは有効であると宣言され、ステップ350においてユーザに与

えられる。

【0035】

この出願においては様々な実施例が特に図解され説明されているが、本発明の修正及び変形は、以上の説明によってカバーされ、本発明の精神と意図された範囲とから逸脱することなく、冒頭の特許請求の範囲に含まれる。更に、オーディオ及びビデオ・コンテンツに対して、時間ベースの信号操作や振幅及びピッチ動作のために、同様の動作が適用された。透かしの入れられていないオリジナルを用いることなくデスクーリング又はそれ以外の態様で迅速に差異を判断できる能力が、安全なデジタル透かしにとっては、固有の重要性を有している。デジタル化されたコンテンツはネットワークを介して交換されるので、拒絶されないことと第三者による認証とを保証することも重要である。

【図面の簡単な説明】

【図1】

本発明の或る実施例によるデジタル情報の符号化方法のブロック流れ図である

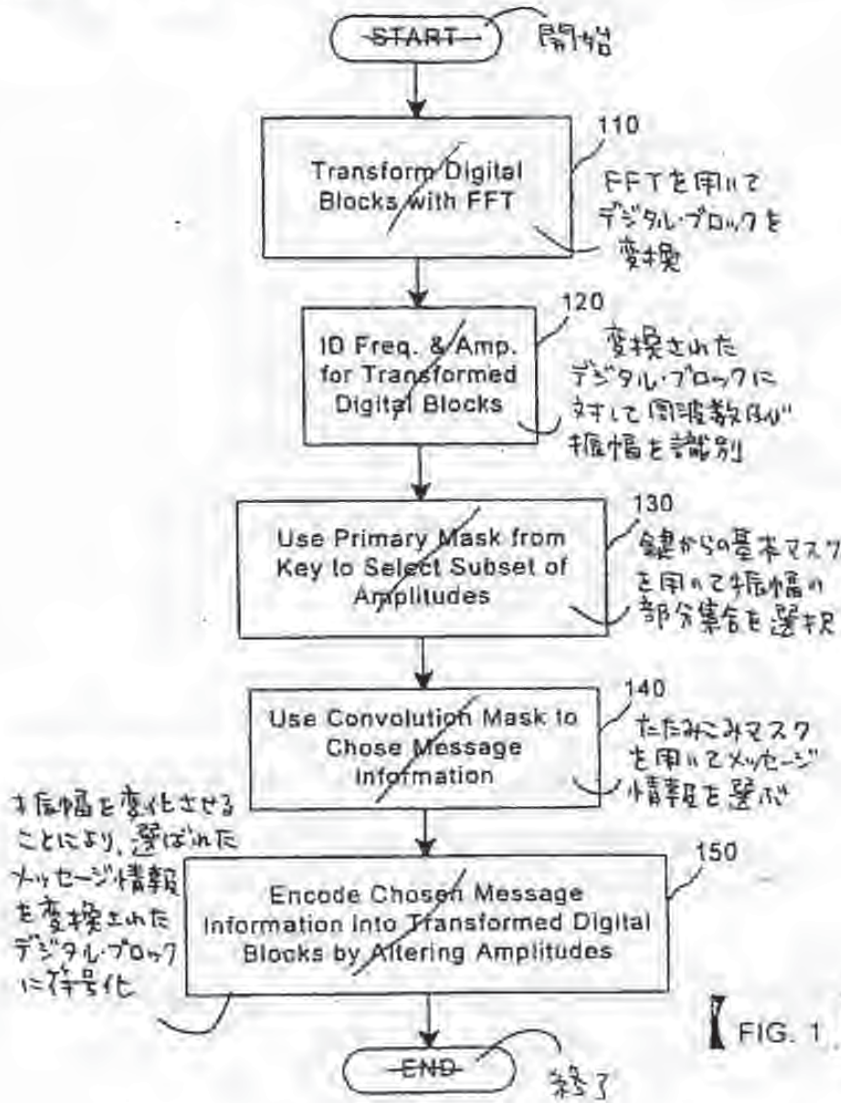
【図2】

本発明の或る実施例によるデジタル情報のデスクーリング方法のブロック流れ図である。

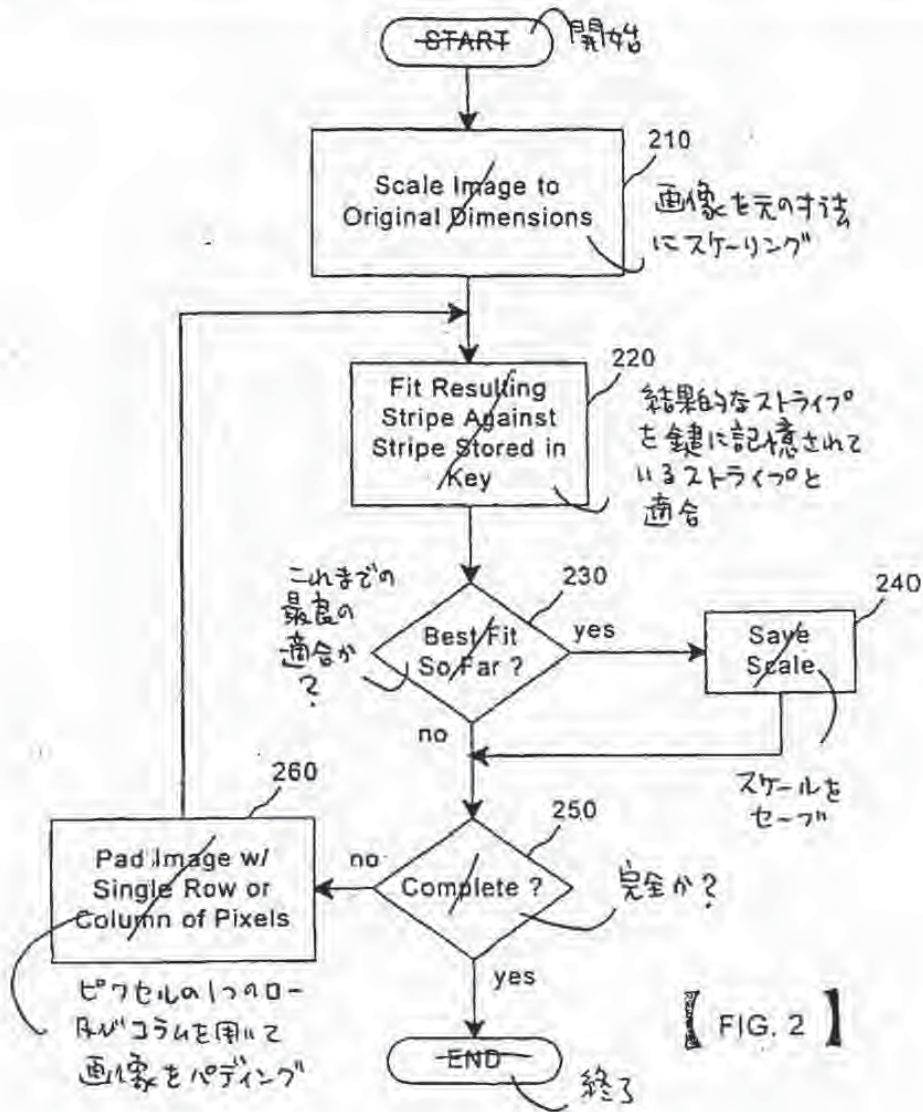
【図3】

本発明の或る実施例によるデジタル情報の復号化方法のブロック流れ図である

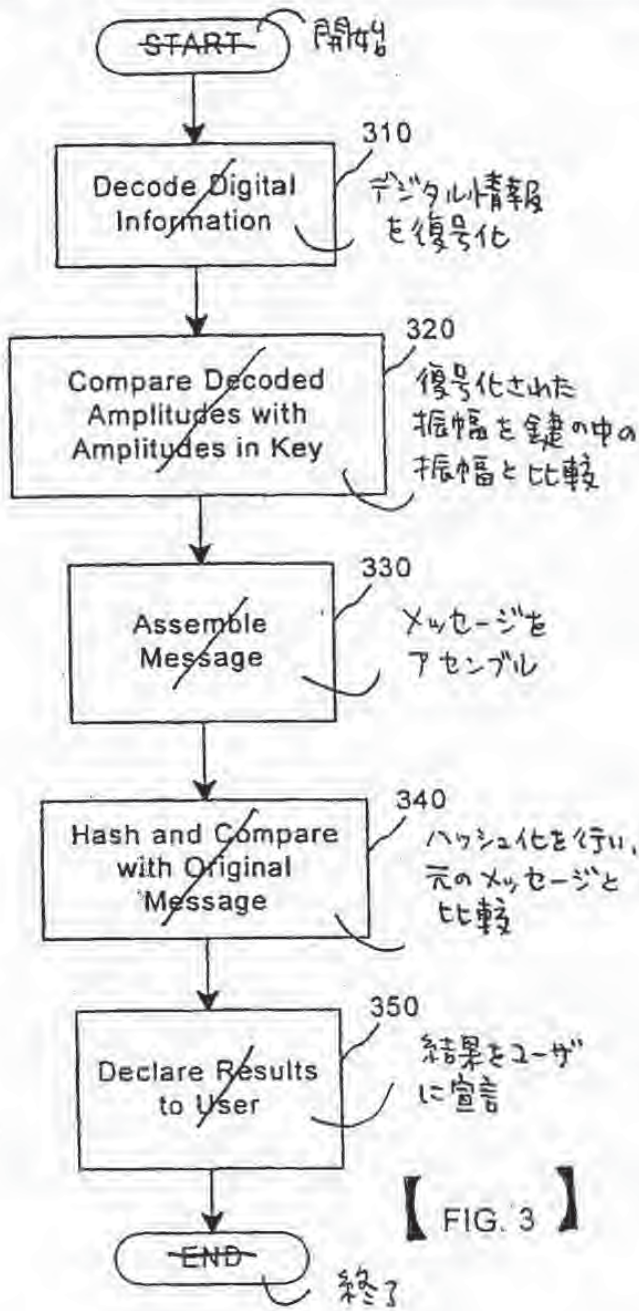
【書類名】 図面



【 FIG. 1 】

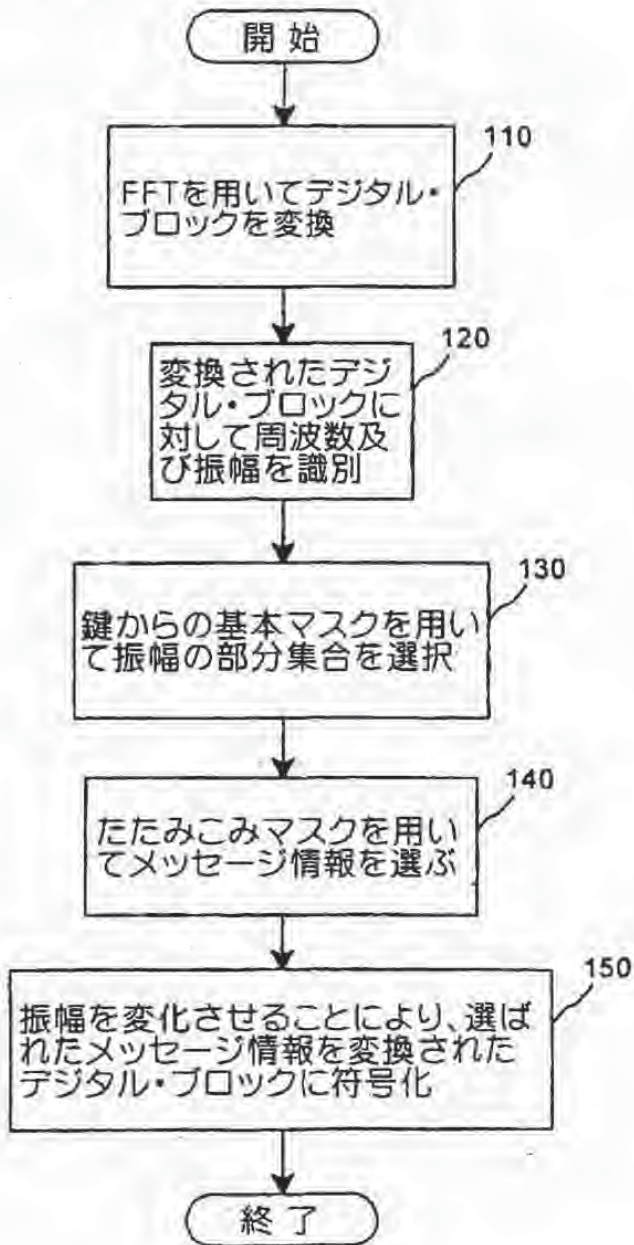


【 FIG. 2 】

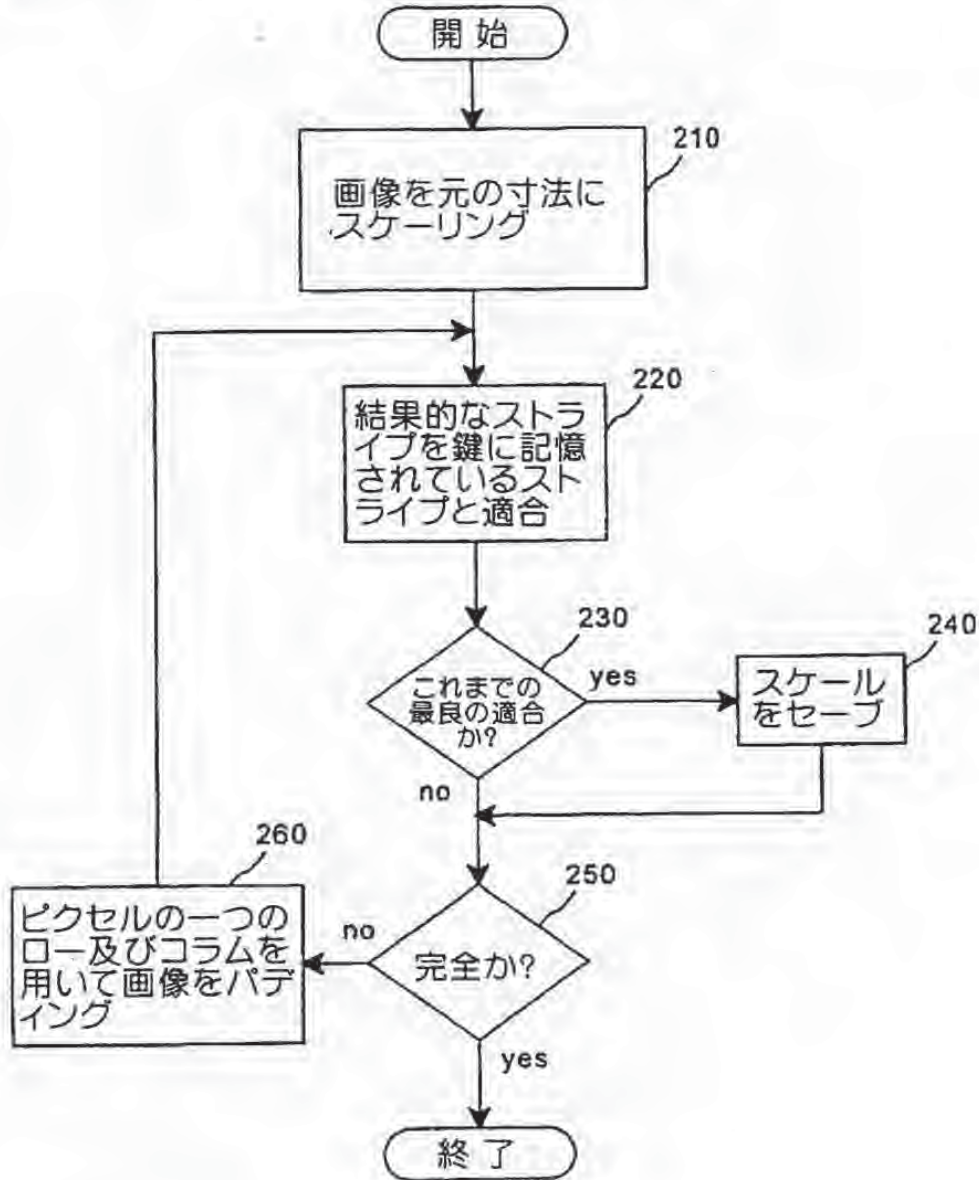


【書類名】 図面

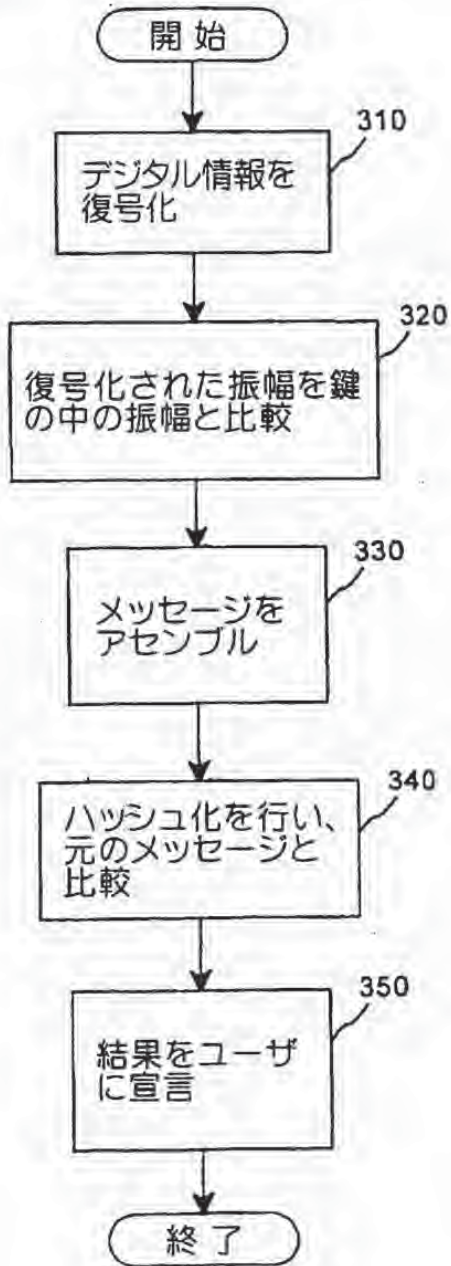
【図1】



【図2】



【図3】



【書類名】 要約書

【要約】 安全なデジタル透かしのための複数の変換の利用及び適用である。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報が、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

Amendment

提出日 平成12年10月13日
整理番号=002365I PCT/US99/07262 頁: 1/ 1

【書類名】 手続補正書 Filed: October 13, 2000

【整理番号】 002365I

【提出日】 平成12年10月13日

【あて先】 特許庁長官 殿

【事件の表示】

【国際出願番号】 PCT/US99/07262

【出願の区分】 特許

【補正をする者】

【住所又は居所】 アメリカ合衆国フロリダ州33160, マイアミ, コリ
ンズ・アベニュー 16711, ナンバー 2505

【氏名又は名称】 スコット・エイ・モスコウィッツ

【代理人】

【識別番号】 100089705

【住所又は居所】 東京都千代田区大手町二丁目2番1号 新大手町ビル2
06区 ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】 社本 一夫

【手続補正 1】

【補正対象書類名】 図面

【補正対象項目名】 全図

【補正方法】 変更

【補正の内容】 1

【その他】 浄書につき、図面の実体的内容には変更なし。

【ブルーフの要否】 要



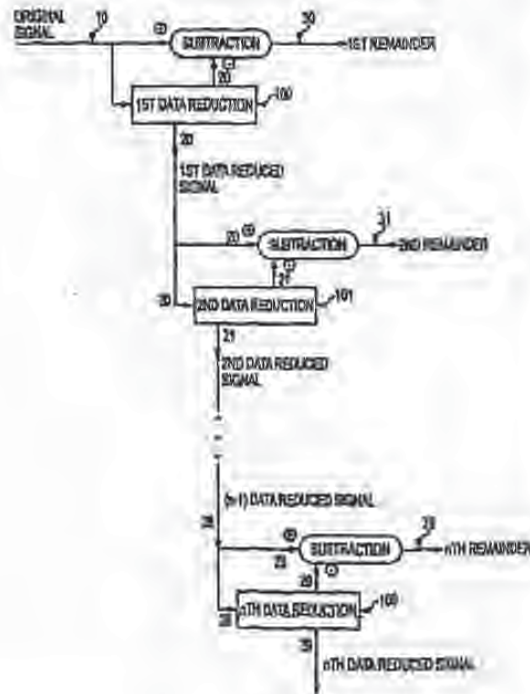
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification 7: H04N 7/167</p>	<p>A1</p>	<p>(11) International Publication Number: WO 00/57643 (43) International Publication Date: 28 September 2000 (28.09.00)</p>
<p>(21) International Application Number: PCT/US00/06522 (22) International Filing Date: 14 March 2000 (14.03.00) (30) Priority Data: 60/125,990 24 March 1999 (24.03.99) US (71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US). (74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, L.L.P., 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).</p>	<p>(81) Designated States: JP, US, 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. Before the expiration of the time limits for amending the claims and to be republished in the event of the receipt of amendments.</p>	

(54) Title: UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

(57) Abstract

The present invention is a method for protecting a data signal where the method comprises the following steps: applying a data reduction technique (200) to the signal to produce a reduced signal, subtracting (60) the reduced data signal from the original signal to produce a remainder signal (39), embedding (300) a first watermark into the reduced data signal to produce a watermarked reduced data signal, and adding (50) the watermarked reduced signal to the remainder signal to produce an output signal (90). A second watermark (301) may be embedded into the remainder signal (39) before the final addition (50) step. Cryptographic techniques may be employed to encrypt the remainder signal and/or the reduced signal prior to the addition step (50).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroun	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

FIELD OF INVENTION

This invention relates to digital signal processing, and more particularly to a method and a system for encoding at least one digital watermark into a signal as a means of conveying information relating to the signal and also protecting against unauthorized manipulation of the signal.

BACKGROUND OF INVENTION

Digital watermarks help to authenticate the content of digitized multimedia information, and can also discourage piracy. Because piracy is clearly a disincentive to the digital distribution of copyrighted content, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content must undergo damage, and therefore reduction of its value, with subsequent, unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns.

A matter of general weakness in digital watermark technology relates directly to the manner of implementation of the watermark. Many approaches to digital watermarking leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This weakness removes proper economic incentives for improvement of the technology. One specific form of exploitation mostly regards efforts to obscure subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time. Yet another way to perform secure digital watermark implementation is through "key-based" approaches.

This paper draws a distinction between a "forensic watermark," based on provably-secure methods, and a "copy control" or "universal" watermark which is intended to be low cost and easily implemented into any general computing or consumer electronic device. A watermark can be forensic if it can identify the source of the data from which a copy was made. For example, assume that digital data are stored on a disk and provided to "Company A" (the "A disk"). Company A makes an unauthorized copy and delivers the copy to "Company B" (the "B disk"). A forensic watermark, if present in the digital data stored on the "A disk," would identify the "B disk" as having been copied from the "A disk."

On the other hand, a copy control or universal watermark is an embedded signal which is governed by a "key" which may be changed (a "session key") to increase security, or one that is easily accessible to devices that may offer less than strict cryptographic security. The "universal" nature of the watermark is the computationally inexpensive means for accessing or other associating the watermark with operations that can include playback, recording or manipulations of the media in which it is embedded.

A fundamental difference is that the universality of a copy control mechanism, which must be redundant enough to survive many signal manipulations to eliminate most casual piracy, is at odds with the far greater problem of establishing responsibility for a given instance of a suspected copying of a copyrighted media work. The more dedicated pirates must be dealt with by encouraging 3rd party authentication with "forensic watermarks" or those that constitute "transactional watermarks" (which are encoded in a given copy of said content to be watermarked as per the given transaction).

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave little or no evidence of the presence of the information signal in the underlying content signal. A separate but equal goal is maximizing the digital watermark's encoding level and "location sensitivity" in the underlying content signal such that the watermark cannot be removed without damage to the content signal.

One means of implementing a digital watermark is to use key-based security. A predetermined or random key can be generated as a map to access the hidden information signal. A key pair may also be used. With a typical key pair, a party possesses a public and a private key. The private key is maintained in confidence by the owner of the key, while the owner's public key is disseminated to those persons in the public with whom the owner would regularly communicate. Messages being communicated, for example by the owner to another, are encrypted with the private key and can only be read by another person who possesses the corresponding public key. Similarly, a message encrypted with the person's public key can only be decrypted with the corresponding private key. Of course, the keys or key pairs may be processed in separate software or hardware devices handling the watermarked data.

SUMMARY OF THE INVENTION

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A system for securing a data signal comprises: means to apply a data reduction technique to reduce the data signal into a reduced data signal; means to subtract said reduced data signal from the data signal to produce a remainder signal; means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

A method of protecting a data signal comprises: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal; using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

There are two design goals in an overall digital watermarking system's low cost, and universality. Ideally, a method for encoding and decoding digital watermarks in digitized media for copy control purposes should be inexpensive and universal. This is essential in preventing casual piracy. On the other hand, a more secure form of protection, such as a "forensic watermarks," can afford to be computationally intensive to decode, but must be unaffected by repeated re-encoding of a copy control watermark. An ideal method for achieving these results would separate the signal into different areas, each of which can be accessed independently. The embedded signal or may simply be "watermark bits" or "executable binary code," depending on the application and type of security sought. Improvements to separation have been made possible by enhancing more of the underlying design to meet a number of clearly problematic issues. The present invention interprets the signal as a stream which may be split into separate streams of digitized samples or may undergo data reduction (including both lossy and lossless compression, such as MPEG lossy compression and Meridian's lossless compression, down sampling, common to many studio operations, or any

related data reduction process). The stream of data can be digital in nature, or may also be an analog waveform (such as an image, audio, video, or multimedia content). One example of digital data is executable binary code. When applied to computer code, the present invention allows for more efficient, secure, copyright protection when handling functionality and associations with predetermined keys and key pairs in software applications or the machine readable versions of such code in microchips and hardware devices. Text may also be a candidate for authentication or higher levels of security when coupled with secure key exchange or asymmetric key generation between parties. The subsets of the data stream combine meaningful and meaningless bits of data which may be mapped or transferred depending on the application intended by the implementing party.

The present invention utilizes data reduction to allow better performance in watermarking as well as cryptographic methods concerning binary executable code, its machine readable form, text and other functionality-based or communication-related applications. Some differences may simply be in the structure of the key itself, a pseudo random or random number string or one which also includes additional security with special one way functions or signatures saved to the key. The key may also be made into key pairs, as is discussed in other disclosures and patents referenced herein. The present invention contemplates watermarks as a plurality of digitized sample streams, even if the digitized streams originate from the analog waveform itself. The present invention also contemplates that the methods disclosed herein can be applied to non-digitized content. Universally, data reduction adheres to some means of "understanding" the reduction. This disclosure looks at data reduction which may include down sampling, lossy compression, summarization or any means of data reduction as a novel means to speed up watermarking encode and decode operations. Essentially a lossy method for data reduction yields the best results for encode and decode operations.

It is desirable to have both copy control and forensic watermarks in the same signal to address the needs of the hardware, computer, and software industries while

also providing for appropriate security to the owners of the copyrights. This will become clearer with further explanation of the sample embodiments discussed herein.

The present invention also contemplates the use of data reduction for purposes of speedier and more tiered forms of security, including combinations of these methods with transfer function functions. In many applications, transfer functions (e.g., scrambling), rather than mapping functions (e.g., watermarking), are preferable or can be used in conjunction with mapping. With "scrambling," predetermined keys are associated with transfer functions instead of mapping functions, although those skilled in the art may recognize that a transfer function is simply a subset of mask sets encompassing mapping functions. It is possible that tiered scrambling with data reduction or combinations of tiered data reduction with watermarking and scrambling may indeed increase overall security to many applications.

The use of data reduction can improve the security of both scrambling and watermarking applications. All data reduction methods include coefficients which affect the reduction process. For example, when a digital signal with a time or space component is down sampled, the coefficient would be the ratio of the new sample rate to the original sample rate. Any coefficients that are used in the data reduction can be randomized using the key, or key pair, making the system more resistant to analysis. Association to a predetermined key or key pair and additional measure of security may include biometric devices, tamper proofing of any device utilizing the invention, or other security measures.

Tests have shown that the use of data reduction in connection with digital watermarking schemes significantly reduces the time required to decode the watermarks, permitting increases in operational efficiency.

Particular implementations of the present invention, which have yielded incredibly fast and inexpensive digital watermarking systems, will now be described. These systems may be easily adapted to consumer electronic devices, general purpose computers, software and hardware. The exchange of predetermined keys or key pairs may facilitate a given level of security. Additionally, the complementary increase in

security for those implementations where transfer functions are used to "scramble" data, is also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

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

FIG. 1 is a functional block diagram that shows a signal processing system that generates "n" remainder signals and "n" data reduced signals.

FIG. 2 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a first remainder signal.

FIG. 3 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a watermarked, first remainder signal.

FIG. 4 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 2.

FIG. 5 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 3.

FIG. 6 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, scrambled signal and a first remainder signal.

FIG. 7 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, scrambled signal and a scrambled, first remainder signal.

FIG. 8 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 6.

FIG. 9 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 7.

DETAILED DESCRIPTION

The embodiments of the present invention and its advantages are best understood by referring to the drawings, like numerals being used for like and corresponding parts of the various drawings.

An Overview

A system for achieving multiple levels of data reduction is illustrated in FIG. 1. An input signal 10 (for example, instructional text, executable binary computer code, images, audio, video, multimedia or even virtual reality imaging) is subjected to a first data reduction technique 100 to generate a first data reduced signal 20. First data reduced signal 20 is then subtracted from input signal 10 to generate a first remainder signal 30.

First data reduced signal 20 is subjected to a second data reduction technique 101 to generate a second data reduced signal 21. Second data reduced signal 21 is then subtracted from first data reduced signal 20 to generate a second remainder signal 31.

Each of the successive data reduced signals is, in turn, subjected to data reduction techniques to generate a further data reduced signal, which, in turn, is subtracted from its respective parent signal to generate another remainder signal. This process is generically described as follows. An $(n-1)$ data reduced signal 28 (i.e., a signal that has been data reduced $n-1$ times) is subjected to an n th data reduction technique 109 to generate an n th data reduced signal 29. The n th data reduced signal 29 is then subtracted from the $(n-1)$ data reduced signal 28 to produce an n^{th} remainder signal 39.

An output signal can be generated from the system illustrated in FIG. 1 in numerous ways. For example, each of the n remainder signals (which, through represented by reference numerals 30-39, are not intended to be limited to 10 signals) and the n^{th} data signal may optionally be subjected to a watermarking technique, or even optionally subjected to an encryption technique, and each of the $(n+1)$ signals (whether

watermarked or encrypted, or otherwise untouched) may then be added together to form an output signal. By way of more particular examples, each of the $(n+1)$ signals (i.e., the n remainder signals and the n^{th} data reduced signal) can be added together without any encryption or watermarking to form an output signal; or one or more of the $(n+1)$ signals may be watermarked and then all $(n+1)$ signals may be added together; or one or more of the $(n+1)$ signals may be encrypted and then all $(n+1)$ signals may be added together. It is anticipated that between these three extremes lie numerous hybrid combinations involving one or more encryptions and one or more watermarks.

Each level may be used to represent a particular data density. E.g., if the reduction method is down-sampling, for a DVD audio signal the first row would represent data sampled at 96 kHz, the second at 44.1 kHz, the third at 6 kHz, etc. There is only an issue of deciding what performance or security needs are contemplated when undertaking the data reduction process and choice of which types of keys or key pairs should be associated with the signal or data to be reduced. Further security can be increased by including block ciphers, special one way functions, one time stamps or even biometric devices in the software or hardware devices that can be embodied. Passwords or biometric data are able to assist in the determination of the identity of the user or owner of the data, or some relevant identifying information.

An example of a real world application is helpful here. Given the predominant concern, at present, of MPEG 1 Layer 3, or MP3, a perceptual lossy compression audio data format, which has contributed to a dramatic re-evaluation of the distribution of music, a digital watermark system must be able to handle casual and more dedicated piracy in a consistent manner. The present invention contemplates compatibility with MP3, as well as any perceptual coding technique that is technically similar. One issue, is to enable a universal copy control "key" detect a watermark as quickly as possible from a huge range of perceptual quality measures. For instance, DVD 24 bit 96 kHz, encoded watermarks, should be detected in at least "real time," even after the signal has been down sampled, to say 12 kHz of the 96 kHz originally referenced. By delineating and starting with less data, since the data-reduced signal is obviously smaller though

still related perceptually to the original DVD signal, dramatic increases in the speed and survival of the universal copy control bits can be achieved. The present invention also permits the ability to separate any other bits which may be associated with other more secure predetermined keys or key pairs.

Where the data stream is executable computer code, the present invention contemplates breaking the code into objects or similar units of functionality and allowing for determination of what is functionally important. This may be more apparent to the developer or users of the software or related hardware device. Data reduction through the use of a subset of the functional objects related to the overall functionality of the software or executable code in hardware or microchips, increase the copyright protection or security sought, based on reducing the overall data to be associated with predetermined keys or key pairs. Similarly, instead of mapping functions, transfer functions, so-called "scrambling," appear better candidates for this type of security although both mapping and transferring may be used in the same system. By layering the security, the associated keys and key pairs can be used to substantially improve the security and to offer easier methods for changing which functional "pieces" of executable computer code are associated with which predetermined keys. These keys may take the form of time-sensitive session keys, as with transactions or identification cards, or more sophisticated asymmetric public key pairs which may be changed periodically to ensure the security of the parties' private keys. These keys may also be associated with passwords or biometric applications to further increase the overall security of any potential implementation.

An example for text message exchange is less sophisticated but, if it is a time sensitive event, e.g., a secure communication between two persons, benefits may also be encountered here. Security may also be sought in military communications. The ability to associate the securely exchanged keys or key pairs while performing data reduction to enhance the detection or decoding performance, while not compromising the level of security, is important. Though a steganographic approach to security, the present invention more particularly addresses the ability to have data reduction to

increase speed, security, and performance of a given steganographic system. Additionally, data reduction affords a more layered approach when associating individual keys or key pairs with individual watermark bits, or digital signature bits, which may not be possible without reduction because of considerations of time or the payload of what can be carried by the overall data "coverttext" being transmitted.

Layering through data reduction offers many advantages to those who seek privacy and copyright protection. Serializaton of the detection chips or software would allow for more secure and less "universal" keys, but the interests of the copyright owners are not always aligned with those of hardware or software providers. Similarly, privacy concerns limit the amount of watermarking that can be achieved for any given application. The addition of a pre-determined and cryptographic key-based "forensic" watermark, in software or hardware, allows for 3rd party authentication and provides protection against more sophisticated attacks on the copy control bits. Creating a "key pair" from the "predetermined" key is also possible.

Separation of the watermarks also relates to separate design goals. A copy control mechanism should ideally be inexpensive and easily implemented, for example, a form of "streamed watermark detection." Separating the watermark also may assist more consistent application in broadcast monitoring efforts which are time-sensitive and ideally optimized for quick detection of watermarks. In some methods, the structure of the key itself, in addition to the design of the "copy control" watermark, will allow for few false positive results when seeking to monitor radio, television, or other streamed broadcasts (including, for example, Internet) of copyrighted material. As well, inadvertent tampering with the embedded signal proposed by others in the field can be avoided more satisfactorily. Simply, a universal copy control watermark may be universal in consumer electronic and general computing software and hardware implementations, but less universal when the key structure is changed to assist in being able to log streaming, performance, or downloads, of copyrighted content. The embedded bits may actually be paired with keys in a decode device to assure accurate broadcast monitoring and tamper proofing, while not requiring a watermark to exceed

the payload available in an inaudible embedding process. E.g., A full identification of the song, versus time-based digital signature bits, embedded into a broadcast signal, may not be recovered or may be easily over encoded without the use of block ciphers, special one way functions or one time pads, during the encoding process, prior to broadcast. Data reduction as herein disclosed makes this operation more efficient at higher speeds.

A forensic watermark is not time sensitive, is file-based, and does not require the same speed demands as a streamed or broadcast-based detection mechanism for copy control use. Indeed, a forensic watermark detection process may require additional tools to aid in ensuring that the signal to be analyzed is in appropriate scale or size, ensuring signal characteristics and heuristic methods help in appropriate recovery of the digital watermark. Simply, all aspects of the underlying content signal should be considered in the embedding process because the watermarking process must take into account all such aspects, including for example, any dimensional or size of the underlying content signal. The dimensions of the content signal may be saved with the key or key pair, without enabling reproduction of the unwatermarked signal. Heuristic methods may be used to ensure the signal is in proper dimensions for a thorough and accurate detection authentication and retrieval of the embedded watermark bits. Data reduction can assist in increasing operations of this nature as well, since the data reduction process may include information about the original signal, for example, signal characteristics, signal abstracts, differences between samples, signal patterns, and related work in restoring any given analog waveform.

The present invention provides benefits, not only because of the key-based approach to the watermarking, but the vast increase in performance and security afforded the implementations of the present invention over the performance of other systems.

The architecture of key and key-pair based watermarking is superior to statistical approaches for watermark detection because the first method meets an evidentiary level of quality and are mathematically provable. By incorporating a level

of data reduction, key and key paired based watermarking is further improved. Such levels of security are plainly necessary if digital watermarks are expected to establish responsibility for copies of copyrighted works in evidentiary proceedings. More sophisticated measures of trust are necessary for use in areas which exceed the scope of copyright but are more factually based in legal proceedings. These areas may include text authentication or software protection (extending into the realm of securing microchip designs and compiled hardware as well) in the examples provided above and are not contemplated by any disclosure or work in the art.

The present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks: a plurality of mask sets. These masks may include primary, convolution and message delimiters but may extend into additional domains. In previous disclosures, the functionality of these masks is defined solely for mapping. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised. Examples of public key cryptosystems may be found in the following U.S. Patents Nos: 4,200,770; 4,218,582; 4,405,829; and 4,424,414, which examples are incorporated herein by reference. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. Mask sets may be limited only by the number of dimensions and amount of error correction or concealment sought, as has been previously disclosed.

A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys, or key pairs, will be saved along with information matching them to the sample stream in question in a database for use in subsequent detection or decode operation. These same cryptographic protocols may be combined with the embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play said streamed content in an unscrambled manner. As with digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of

implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations, where transmission security is a concern.

Signal Processing in a Multi-watermark System (A Plurality of Streams May Be Watermarked)

FIG. 2 illustrates a system and method of implementing a multiple-watermark system. An input signal 11 (e.g., binary executable code, instruction text, or other data), is first processed by a lossy data-reduction scheme 200 (e.g., down-sampling, bit-rate reduction, or compression method) to produce a data-reduced signal 40. Data-reduced signal 40 is then embedded with a watermark (process step 300) to generate a watermarked, data-reduced signal 50, while a copy of the unmarked, data-reduced signal 40 is saved.

The saved, unwatermarked data-reduced signal (signal 40) is subtracted from the original input signal 11, yielding a remainder signal 60 composed only of the data that was lost during the data-reduction. A second watermark is then applied (process step 301) to remainder signal 60 to generate a watermarked remainder signal 70. Finally, the watermarked remainder 70 and the watermarked, data-reduced signal 50 are added to form an output signal 80, which is the final, full-bandwidth, output signal.

The two watermarking techniques (process steps 300 and 301) may be identical (i.e., be functionally the same), or they may be different.

To decode the signal, a specific watermark is targeted. Duplicating the data-reduction processes that created the watermark in some cases can be used to recover the signal that was watermarked. Depending upon the data-reduction method, it may or may not be necessary to duplicate the data-reduction process in order to read a watermark embedded in a remainder signal. Because of the data-reduction, the decoding search can occur much faster than it would in a full-bandwidth signal. Detection speed of the remainder watermark remains the same as if there were no other watermark present.

FIG. 4 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 2. A signal to be analyzed 80 (e.g., the same output from FIG. 2) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal. Further, data reduced signal 41 can be subtracted from signal to be analyzed 80 to form a differential signal 61 which can then be decoded to remove the message that was watermarked in the original remainder signal. A decoder may only be able to perform one of the two decodings. Differential access and/or different keys may be necessary for each decoding.

Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

Signal Processing in a Single Watermark System

FIG. 3 illustrates a system and method of implementing a single watermark system. The process and system contemplated here is identical to process described in connection to FIG. 2, above, except that no watermark is embedded in the remainder signal. Hence, the watermarked, data-reduced signal 50 is added directly to the remainder signal 60 to generate an output signal 90. Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

In either process, an external key can be used to control the insertion location of either watermark. In a copy-control system, a key is not generally used, whereas in a forensic system, a key must be used. The key can also control the parameters of the data-reduction scheme. The dual scheme can allow a combination of copy-control and forensic watermarks in the same signal. A significant feature is that the copy-control watermark can be read and rewritten without affecting the forensic mark or compromising its security.

FIG. 5 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 3. A signal to be analyzed 90 (e.g., the same output from FIG. 3) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal.

Signal Processing in a Multi-scrambler System (A Plurality of Streams May Be Scrambled)

FIG. 6 illustrates a system and method of implementing a multi-scrambler system. An input signal 12 (e.g., binary executable code, instruction text, or other data), is first processed by a lossy data-reduction scheme 400 (e.g., down-sampling, bit-rate reduction, or compression method) to produce a data-reduced signal 45. Data-reduced signal 45 is then scrambled using a first scrambling technique (process step 500) to generate a scrambled, data-reduced signal 55, while a copy of the unscrambled, data-reduced signal 45 is saved.

The saved, unscrambled data-reduced signal (signal 45) is subtracted from the original input signal 12, yielding a remainder signal 65 composed only of the data that was lost during the data-reduction. A second scrambling technique is then applied (process step 501) to remainder signal 65 to generate a scrambled remainder signal 75. Finally, the scrambled remainder signal 75 and the scrambled data-reduced signal 55 are added to form an output signal 85, which is the final, full-bandwidth, output signal.

The two scrambling techniques (process steps 500 and 501) may be identical (i.e., be functionally the same), or they may be different.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

To decode the signal, unscrambling follows the exact pattern of the scrambling process except that the inverse of the scrambling transfer function is applied to each portion of the data, thus returning it to its pre-scrambled state.

FIG. 8 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 6. A signal to be analyzed 85 (e.g., the same output from FIG. 6) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 85 to form a differential signal 66, which signal can then be descrambled in process 551 using the inverse transfer function of the process that scrambled the original remainder signal (e.g., the inverse of scrambling process 501). Descrambling process 551 generates an descrambled signal 76. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to descrambled signal 76 to form an output signal 98.

Signal Processing in a Single Scrambling Operation

FIG. 7 illustrates a system and method of implementing a single scrambling system. The process and system contemplated here is identical to process described in connection to FIG. 6, above, except that no scrambling is applied to the remainder signal. Hence, the scrambled data-reduced signal 55 is added directly to the remainder signal 65 to generate an output signal 95.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

FIG. 9 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 7. A signal to be analyzed 95 (e.g., the same output from FIG. 7) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 95 to form a differential

signal 66. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to differential signal 66 to form an output signal 99.

Sample Embodiment: Combinations

Another embodiment may combine both watermarking and scrambling with data reduction. Speed, performance and computing power may influence the selection of which techniques are to be used. Decisions between data reduction schemes ultimately must be measured against the types of keys or key pairs to use, the way any pseudo random or random number generation is done (chaotic, quantum or other means), and the amount of scrambling or watermarking that is necessary given the needs of the system.

It is quite possible that some derived systems would yield a fairly large decision tree, but the present invention offers many benefits to applications in security that are not disclosed in the art.

Conclusions

Data signals fall into two categories: those which can undergo lossy data reduction and remain functional and those which cannot. Audio, images, video are examples of the first. Computer code is an example of the second. In general, all members of the first category contain an aesthetic component, which may be reduced and/or manipulated during a data reduction, in addition to a functional component which serves to identify the signal. For example, an audio signal may have noise added while still remaining recognizably identifiable as a particular song. However, beyond a certain point, the addition of more noise will cause the signal to become unidentifiable, thus impairing the functional character of the signal. In the absence of

an aesthetic component, as with computer code where every bit of data is necessary, lossy compression that retains functionality is not possible.

Signals in the first category are the only candidates for watermarking. A watermark is a distortion of the aesthetic component, generally of an imperceptible nature. This category will gain speed benefits during the watermark decoding process when a lossy data-reduction method is used as described above.

Scrambling, on the other hand, may be applied to any signal, regardless of its aesthetic component, since it allows for perfect reconstruction of the original signal. A scrambling system can be made more secure by applying a data reduction method prior to scrambling, even if this data reduction makes the intermediate signals non-functional, as is the case with signals in category two.

Data reduction can make both watermarking and scrambling more secure. Data reduction can also speed the decoding process for watermarks. Finally, data reduction can allow natural channelization of watermarks for different purposes.

While the invention has been particularly shown and described in 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.

WHAT IS CLAIMED IS:

1. A method of securing a data signal comprising:
 - applying a data reduction technique to reduce the data signal into a reduced data signal;
 - subtracting said reduced data signal from the data signal to produce a remainder signal;
 - embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal;
 - embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and
 - adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.
2. The method of claim 1 wherein the step of subtracting is comprised of
 - storing a copy of the data signal; and
 - subtracting said reduced data signal from the copy of the data signal to produce a remainder signal.
3. The method of claim 1, wherein at least one of the watermarks is embedded using at least one key.
4. The method of claim 1, wherein at least one of the watermarks is embedded using a key pair.
5. The method of claim 4, wherein one key of the key pair is publicly available while the other key of the key pair is secret.
6. A method of protecting a data signal comprising:
 - applying a data reduction technique to reduce the data signal into a reduced data signal;
 - subtracting said reduced data signal from the data signal to produce a remainder signal;
 - embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; and

adding said watermarked, reduced data signal to said remainder signal to produce an output signal.

7. The method of claim 6 wherein the step of adding said watermarked, reduced data signal to said remainder signal comprises:

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

8. The method of claim 7, wherein at least one of the watermarks is embedded using at least one key.

9. The method of claim 7, wherein at least one of the watermarks is embedded using a key pair.

10. The method of claim 9, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

11. A method of protecting a data signal:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal;

using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and

adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

12. The method of claim 11 wherein said first and second scrambling techniques are identical.

13. A method of securing a data signal comprising:
 - applying a data reduction technique to reduce the data signal into a reduced data signal;
 - subtracting said reduced data signal from the data signal to produce a remainder signal;
 - using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;
 - using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and
 - adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.
14. The method of claim 13 wherein said first and second cryptographic techniques are identical.
15. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a watermarking technique.
16. The method of claim 15, wherein at least one of the watermarks is embedded using at least one key.
17. The method of claim 15, wherein at least one of the watermarks is embedded using a key pair.
18. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a scrambling technique.
19. The method of claim 13 wherein one of said first and second cryptographic techniques is a watermarking technique and the other is a scrambling technique.
20. The method of claim 13 wherein said first and second cryptographic techniques are identical.
21. A system for securing a data signal comprising:
 - means to apply a data reduction technique to reduce the data signal into a reduced data signal;

means to subtract said reduced data signal from the data signal to produce a remainder signal;

means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

22. The system of claim 2) wherein said first and second cryptographic techniques are identical.
23. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a watermarking technique.
24. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a scrambling technique.
25. The system of claim 13 wherein said means to apply a first cryptographic technique is a means to apply a watermarking technique and said means to apply a second cryptographic technique is a means to apply a scrambling technique.

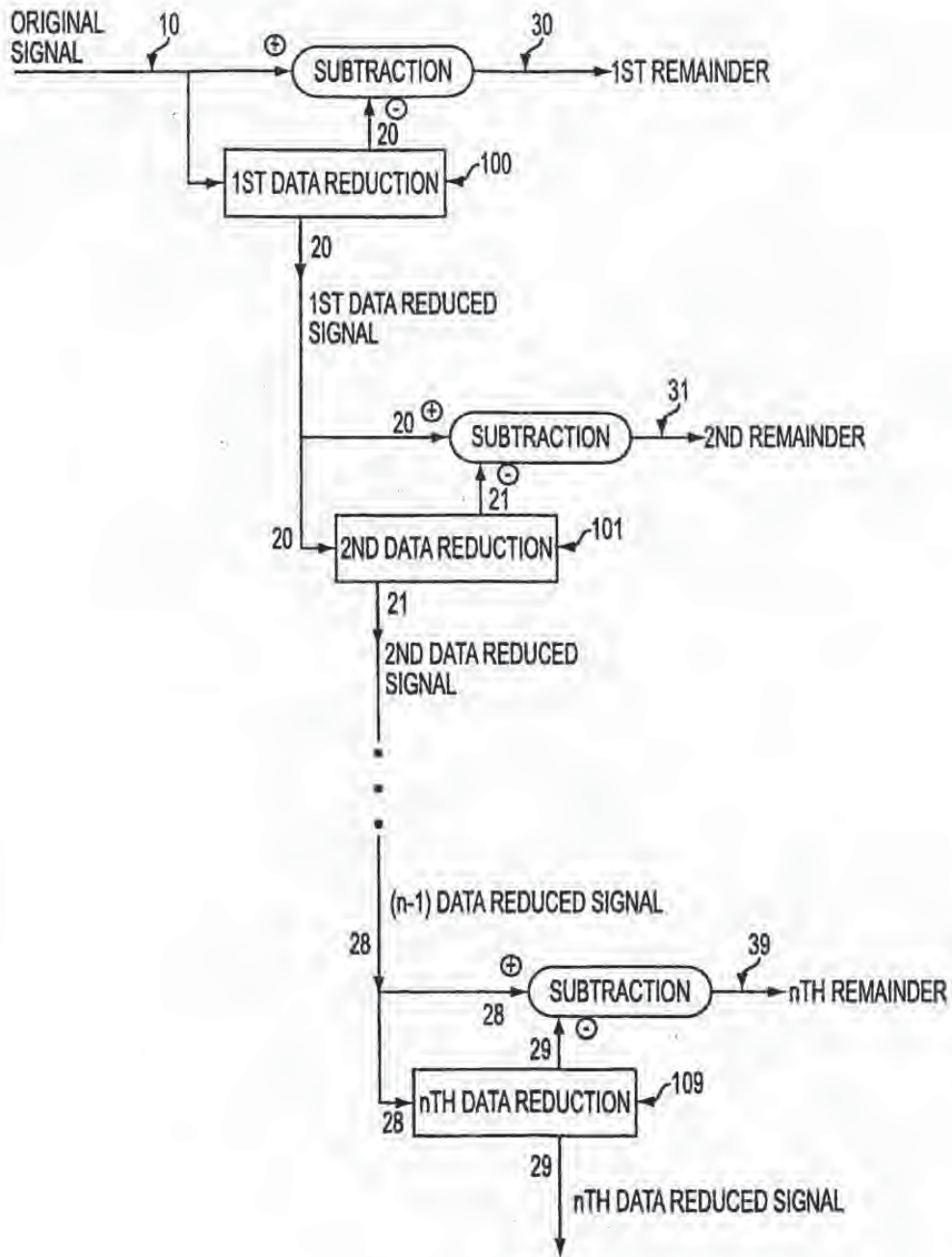


FIG. 1

SUBSTITUTE SHEET (RULE 26)

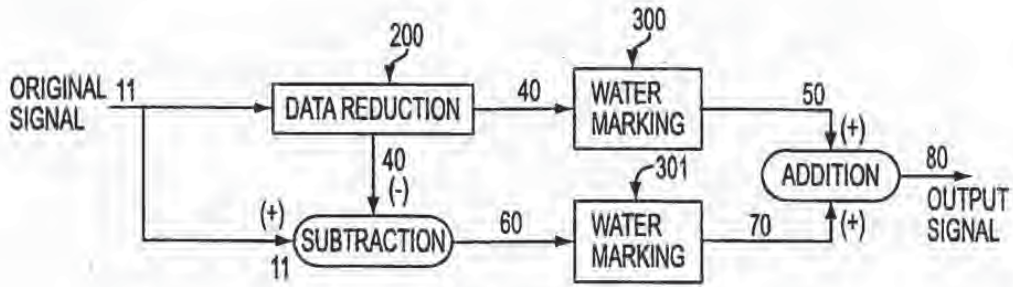


FIG. 2

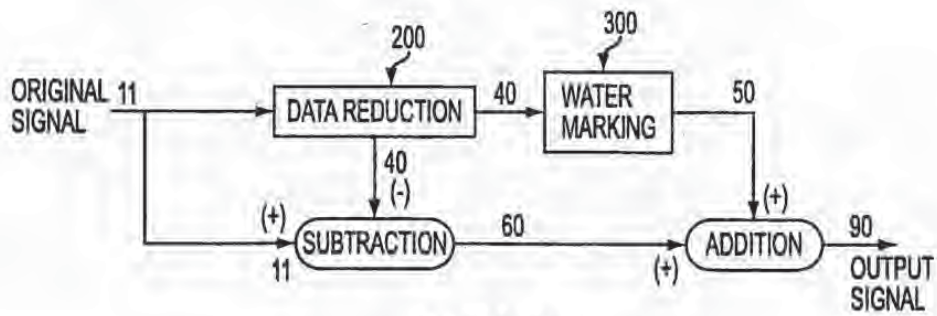


FIG. 3

SUBSTITUTE SHEET (RULE 26)

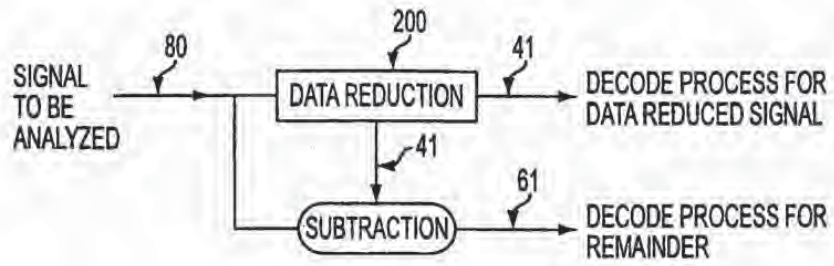


FIG. 4

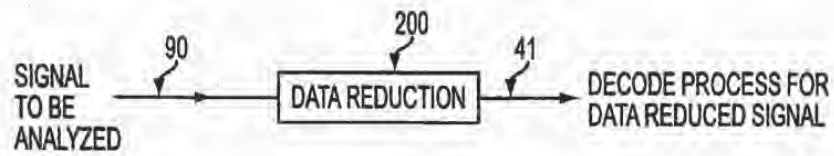


FIG. 5

SUBSTITUTE SHEET (RULE 26)

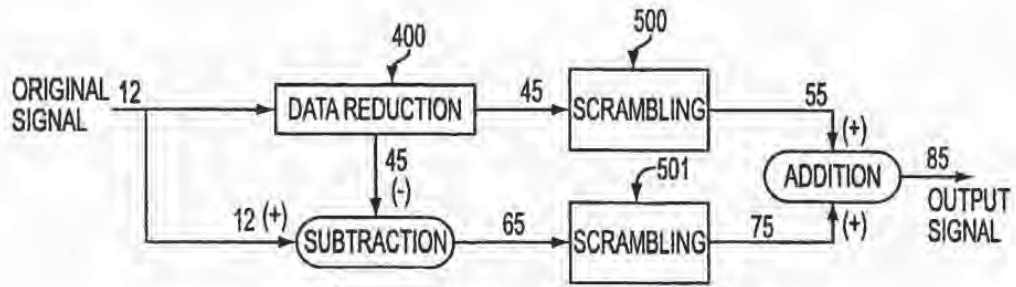


FIG. 6

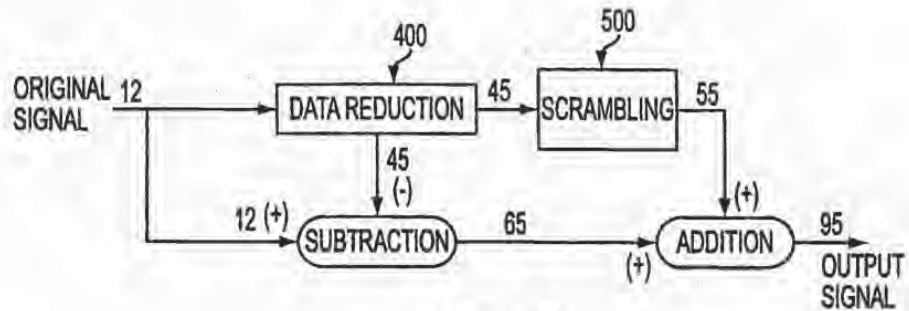


FIG. 7

SUBSTITUTE SHEET (RULE 26)

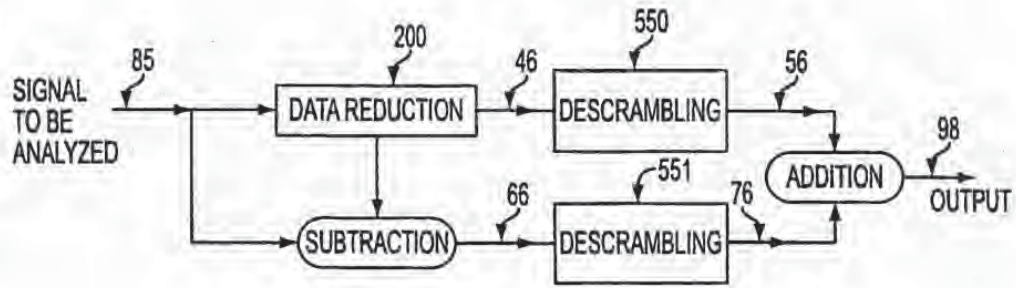


FIG. 8

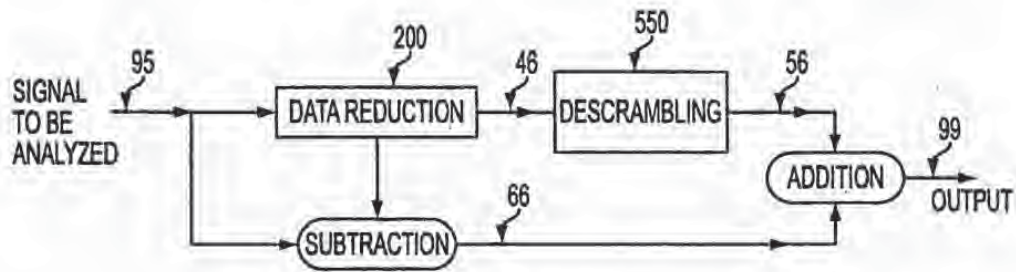



FIG. 9

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : H04N 7/167 US CL : 713/176 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. : 380/200,205,207,237,238; 703/54; 704/216-218, 226-228, 500, 501, 503,504; 713/176, 160/49; 348/461,462 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Watermark Digest: Art Unit 2767 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) IEEE, EAST, Internet, Dialog		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 6,061,793 A [TEWFIK et al.] 09 MAY 2000, Entire Document	1-25
X	US 5,809,139 A [GIROD et al.] 15 SEPTMBER 1998, Entire Document	1-25
X	US 5,848,155 A [COX] 08 DECEMBER 1998, Entire Document	1-25
A,P	US 5,889,868 A [MOSKOWITZ et al.] 30 MARCH 1999, Entire Document	1-25
A,P	US 5,915,027 A [COX et al.] 22 JUNE 1999, Entire Document	1-25
A,P	US 5,940,134 A [WIRTZ] 17 AUGUST 1999, Entire Document	1-25
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document published on or after the international filing date *L* document which may throw doubt on priority claims or which is cited to establish the publication date of another claim or other special reason (see specification) *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 used 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 considered with one or more other such documents; such combination being obvious to a person skilled in the art *A* document member of the same patent family		
Date of the actual completion of the international search 30 JUNE 2000		Date of mailing of the international search report 18 AUG 2000
Name and mailing address of the ISA/IJS Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-1230		Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1230 

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,426 A [COX et al.] 23 NOVEMBER 1999, Entire Document	1-25
A,E	US 6,069,914 A [COX] 30 MAY 2000, Entire Document	1-25
A,P	US 5,943,422 A [VAN WIE et al.] 24 AUGUST 1999, Entire Document	1-25

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



European Patent
Office

**SUPPLEMENTARY
EUROPEAN SEARCH REPORT**

Application Number
EP 00 91 9398

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (InCL.7)
X	WO 98 37513 A (TELSTRA R & D MAN PTY LTD ;BIGGAR MICHAEL (AU); JOHNSON ANDREW (AU)) 27 August 1998 (1998-08-27) * page 5, line 25 - page 7, line 10 *	6	H04N7/167 H04N7/26 H04N1/32 G06F17/30
Y	US 4 969 204 A (MELNYCHUCK PAUL W ET AL) 6 November 1990 (1990-11-06) * column 2, line 9 - column 2, line 48 *	1-10	
Y	EP 0 651 554 A (EASTMAN KODAK CO) 3 May 1995 (1995-05-03) * column 6, line 43 - column 9, line 19; figure 2 *	1-10	
A	JOHNSON A ET AL: "TRANSFORM PERMUTED WATERMARKING FOR COPYRIGHT PROTECTION OF DIGITAL VIDEO" IEEE GLOBECOM 1998. GLOBECOM '98. THE BRIDGE TO GLOBAL INTEGRATION. SYDNEY, NOV. 8 - 12, 1998, IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, NEW YORK, NY: IEEE, US, vol. 2, 1998, pages 684-689, XP000825846 ISBN: 0-7803-4985-7 * page 685, left-hand column, paragraph 2 - page 685, left-hand column, paragraph 3 *	1-10	TECHNICAL FIELDS SEARCHED (InCL.7) H04N G06F
P,X	WO 99 62044 A (HANDEL THEODORE G ;UNIV CALIFORNIA (US); SANDFORD MAXELL T II (US)) 2 December 1999 (1999-12-02) * abstract * * page 4, line 17 - page 5, line 5 *	6	
The supplementary search report has been based on the last set of claims valid and available at the start of the search.			
Place of search MUNICH		Date of completion of the search 27 June 2002	Examiner Schoeyer, M
CATEGORY OF CITED DOCUMENTS		T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons A: member of the same patent family, corresponding document	
X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document			

EPO FORM 1523 (03.02) (No. 10/04)

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03385 A1

(51) International Patent Classification: G11B 20/00,
G06F 1/00

(21) International Application Number: PCT/US00/18411

(22) International Filing Date: 5 July 2000 (05.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and

(72) Inventor: MOSKOWITZ, Scott, A. [US/US]; 16711
Collins Avenue #2505, Miami, FL 33160 (US).

(74) Agents: CHAPMAN, Floyd, B. et al.; Wiley Rein &
Fielding, Intellectual Property Department, 1776 K Street,
N.W., Washington, DC 20006 (US).

(81) Designated States (national): AE, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK,

DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,
LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT,
RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA,
UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG,
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

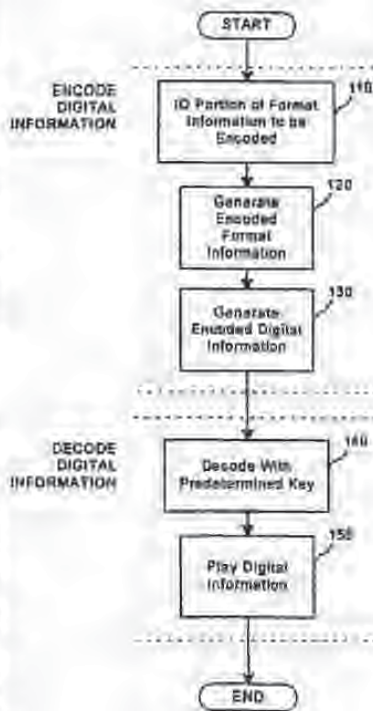
Published:
— with international search report

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.

(54) Title: COPY PROTECTION OF DIGITAL DATA COMBINING STEGANOGRAPHIC AND CRYPTOGRAPHIC TECHNIQUES



WO 02/03385 A1



(57) Abstract: A method for combining transfer functions with predetermined key creation. In one embodiment, digital information, including a digital sample and format information, is protected by identifying and encoding a portion of the format information. Encoded digital information, including the digital sample and the encoded format information generated to protect the original digital information. In another embodiment, a digital signal, including digital samples in a file format having an inherent granularity, is protected by creating a predetermined key. The predetermined key is comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

COPY PROTECTION OF DIGITAL DATA COMBINING STEGANOGRAPHIC AND CRYPTOGRAPHIC TECHNIQUES

BACKGROUND OF THE INVENTION

5 Increasingly, commercially valuable information is being created and stored in "digital" form. For example, music, photographs and video can all be stored and transmitted as a series of numbers, such as 1's and 0's. Digital techniques let the original information be recreated in a very accurate manner. Unfortunately, digital techniques also let the information be easily copied without the information
10 owner's permission.

 Because unauthorized copying is clearly a disincentive to the digital distribution of valuable information, it is important to establish responsibility for copies and derivative copies of such works. For example, if each authorized digital copy of a popular song is identified with a unique number, any unauthorized copy of
15 the song would also contain the number. This would allow the owner of the information, such as a song publisher, to investigate who made the unauthorized copy. Unfortunately, it is possible that the unique number could be erased or altered if it is simply tacked on at the beginning or end of the digital information.

 As will be described, known digital "watermark" techniques give
20 creators and publishers of digitized multimedia content localized, secured identification and authentication of that content. In considering the various forms of multimedia content, such as "master," stereo, National Television Standards Committee (NTSC) video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the
25 content. For example, if a digital version of a popular song sounds distorted, it will be less valuable to users. It is therefore desirable to embed copyright, ownership or purchaser information, or some combination of these and related data, into the content in a way that will damage the content if the watermark is removed without authorization.

30 To achieve these goals, digital watermark systems insert ownership information in a way that causes little or no noticeable effects, or "artifacts," in the underlying content signal. For example, if a digital watermark is inserted into a

digital version of a song, it is important that a listener not be bothered by the slight changes introduced by the watermark. It is also important for the watermark technique to maximize the encoding level and "location sensitivity" in the signal to force damage to the content signal when removal is attempted. Digital watermarks address many of these concerns, and research in the field has provided extremely robust and secure implementations.

What has been overlooked in many applications described in the art, however, are systems which closely mimic distribution of content as it occurs in the real world. For instance, many watermarking systems require the original un-watermarked content signal to enable detection or decode operations. These include highly publicized efforts by NEC, Digimarc and others. Such techniques are problematic because, in the real world, original master copies reside in a rights holders vaults and are not readily available to the public.

With much activity overly focused on watermark survivability, the security of a digital watermark is suspect. Any simple linear operation for encoding information into a signal may be used to erase the embedded signal by inverting the process. This is not a difficult task, especially when detection software is a plug-in freely available to the public, such as with Digimarc. In general, these systems seek to embed cryptographic information, not cryptographically embed information into target media content.

Other methods embed ownership information that is plainly visible in the media signal, such as the method described in US Patent No. 5,530,739 to Braudaway et al. The system described in Braudaway protects a digitized image by encoding a visible watermark to deter piracy. Such an implementation creates an immediate weakness in securing the embedded information because the watermark is plainly visible. Thus, no search for the embedded signal is necessary and the watermark can be more easily removed or altered. For example, while certainly useful to some rights owners, simply placing the symbol "©" in the digital information would only provide limited protection. Removal by adjusting the brightness of the pixels forming the "©" would not be difficult with respect to the computational resources required.

Other relevant prior art includes US Patents No. 4,979,210 and 5,073,925 to Nagata et al., which encodes information by modulating an audio signal in the amplitude/time domain. The modulations introduced in the Nagata process carry a "copy/don't copy" message, which is easily found and circumvented by one skilled in the art. The granularity of encoding is fixed by the amplitude and frequency modulation limits required to maintain inaudibility. These limits are relatively low, making it impractical to encode more information using the Nagata process.

Although US Patent No. 5,664,018 to Leighton describes a means to prevent collusion attacks in digital watermarks, the disclosed method may not actually provide the security described. For example, in cases where the watermarking technique is linear, the "insertion envelope" or "watermarking space" is well-defined and thus susceptible to attacks less sophisticated than collusion by unauthorized parties. Over-encoding at the watermarking encoding level is but one simple attack in such linear implementations. Another consideration not made by Leighton is that commercially-valuable content may already exist in a un-watermarked form somewhere, easily accessible to potential pirates, gutting the need for any type of collusive activity. Digitally signing the embedded signal with preprocessing of watermark data is more likely to prevent successful collusion. Furthermore, a "baseline" watermark as disclosed is quite subjective. It is simply described elsewhere in the art as the "perceptually significant" regions of a signal. Making a watermarking function less linear or inverting the insertion of watermarks would seem to provide the same benefit without the additional work required to create a "baseline" watermark. Indeed, watermarking algorithms should already be capable of defining a target insertion envelope or region without additional steps. What is evident is the Leighton patent does not allow for initial prevention of attacks on an embedded watermark as the content is visibly or audibly unchanged.

It is also important that any method for providing security also function with broadcasting media over networks such as the Internet, which is also referred to as "streaming." Commercial "plug-in" products such as RealAudio and RealVideo, as well as applications by vendors VDO.Net and Xtreme, are common in such network environments. Most digital watermark implementations focus on

common file base signals and fail to anticipate the security of streamed signals. It is desirable that any protection scheme be able to function with a plug-in player without advanced knowledge of the encoded media stream.

5 Other technologies focus solely on file-based security. These technologies illustrate the varying applications for security that must be evaluated for different media and distribution environments. Use of cryptolopes or cryptographic containers, as proposed by IBM in its Cryptolope product, and InterTrust, as described in U.S. Patents No. 4,827,508, 4,977,594, 5,050,213 and 5,410,598, may discourage certain forms of piracy. Cryptographic containers, 10 however, require a user to subscribe to particular decryption software to decrypt data. IBM's InfoMarket and InterTrust's DigiBox, among other implementations, provide a generalized model and need proprietary architecture to function. Every user must have a subscription or registration with the party which encrypts the data. Again, as a form of general encryption, the data is scrambled or encrypted without 15 regard to the media and its formatting. Finally, control over copyrights or other neighboring rights is left with the implementing party, in this case, IBM, InterTrust or a similar provider. Methods similar to these "trusted systems" exist, and Cerberus Central Limited and Liquid Audio, among a number of companies, offer systems which may functionally be thought of as subsets of IBM and InterTrust's more generalized security offerings. Both Cerberus and Liquid Audio propose 20 proprietary player software which is registered to the user and "locked" in a manner parallel to the locking of content that is distributed via a cryptographic container. The economic trade-off in this model is that users are required to use each respective companies' proprietary player to play or otherwise manipulate content that is downloaded. If, as is the case presently, most music or other media is not available 25 via these proprietary players and more companies propose non-compatible player formats, the proliferation of players will continue. Cerberus and Liquid Audio also by way of extension of their architectures provide for "near-CD quality" but proprietary compression. This requirement stems from the necessity not to allow 30 content that has near-identical data make-up to an existing consumer electronic standard, in Cerberus and Liquid Audio's case the so-called Red Book audio CD standard of 16 bit 44.1 kHz, so that comparisons with the proprietary file may not

yield how the player is secured. Knowledge of the player's file format renders its security ineffective as a file may be replicated and played on any common player, not the intended proprietary player of the provider of previously secured and uniquely formatted content. This is the parallel weakness to public key crypto-
5 systems which have gutted security if enough plain text and cipher text comparisons enable a pirate to determine the user's private key.

Many approaches to digital watermarking leave detection and decoding control with the implementing party of the digital watermark, not the creator of the work to be protected. A set of secure digital watermark
10 implementations address this fundamental control issue forming the basis of key-based approaches. These are covered by the following patents and pending applications, the entire disclosures of which are hereby incorporated by reference: US Patent No. 5,613, 004 entitled "Steganographic Method and Device" and its derivative US patent application Serial No. 08/775,216, US patent application Serial
15 No. 08/587,944 entitled "Human Assisted Random Key Generation and Application for Digital Watermark System," US Patent Application Serial No. 08/587,943 entitled "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/677,435 entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data," and US Patent
20 Application Serial No. 08/772,222 entitled "Z-Transform Implementation of Digital Watermarks." Public key crypto-systems are described in US Patents No. 4,200,770, 4,218,582, 4,405,829 and 4,424,414, the entire disclosures of which are also hereby incorporated by reference.

In particular, an improved protection scheme is described in "Method
25 for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/587,943. This technique uses the key-based insertion of binary executable computer code within a content signal that is subsequently, and necessarily, used to play or otherwise manipulate the signal in which it is encoded. With this system, however, certain computational requirements, such as one digital player per digital
30 copy of content, may be necessitated. For instance, a consumer may download many copies of watermarked content. With this technique, the user would also be downloading as many copies of the digital player program. While this form of

security may be desirable for some applications, it is not appropriate in many circumstances. Finally, even when digital information is distributed in encoded form, it may be desirable to allow unauthorized users to play the information with a digital player, perhaps with a reduced level of quality. For example, a popular song
5 may be encoded and freely distributed in encoded form to the public. The public, perhaps using commonly available plug-in digital players, could play the encoded content and hear the music in some degraded form. The music may sound choppy, or fuzzy or be degraded in some other way. This lets the public decide, based on the available lower quality version of the song, if they want to purchase a key from the
10 publisher to decode, or "clean-up," the content. Similar approaches could be used to distribute blurry pictures or low quality video. Or even "degraded" text, in the sense that only authenticated portions of the text can be determined with the predetermined key or a validated digital signature for the intended message.

In view of the foregoing, it can be appreciated that a substantial need
15 exists for a method allowing encoded content to be played, with degraded quality, by a plug-in digital player, and solving the other problems discussed above.

SUMMARY OF THE INVENTION

The disadvantages of the art are alleviated to a great extent by a method for combining transfer functions with predetermined key creation. In one
20 embodiment, digital information, including a digital sample and format information, is protected by identifying and encoding a portion of the format information. Encoded digital information, including the digital sample and the encoded format information, is generated to protect the original digital information.

In another embodiment, a digital signal, including digital samples in a
25 file format having an inherent granularity, is protected by creating a predetermined key. The predetermined key is comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

With these and other advantages and features of the invention that
30 will become hereinafter apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block flow diagram of a method for copy protection or authentication of digital information according to an embodiment of the present invention.

5 DETAILED DESCRIPTION

In accordance with an embodiment of the present invention, a method combines transfer functions with predetermined key creation. Increased security is achieved in the method by combining elements of "public-key steganography" with cryptographic protocols, which keep in-transit data secure by scrambling the data with "keys" in a manner that is not apparent to those with access to the content to be distributed. Because different forms of randomness are combined to offer robust, distributed security, the present invention addresses an architectural "gray space" between two important areas of security: digital watermarks, a subset of the more general art of steganography, and cryptography. One form of randomness exists in the mask sets that are randomly created to map watermark data into an otherwise unrelated digital signal. The second form of randomness is the random permutations of data formats used with digital players to manipulate the content with the predetermined keys. These forms can be thought of as the transfer function versus the mapping function inherent to digital watermarking processes.

20 According to an embodiment of the present invention, a predetermined, or randomly generated, key is used to scramble digital information in a way that is unlike known "digital watermark" techniques and public key cryptosystems. As used herein, a key is also referred to as a "mask set" which includes one or more random or pseudo-random series of bits. Prior to encoding, a mask can be generated by any cryptographically secure random generation process. A block cipher, such as a Data Encryption Standard (DES) algorithm, in combination with a sufficiently random seed value, such as one created using a Message Digest 5 (MD5) algorithm, emulates a cryptographically secure random bit generator. The keys are saved in a database, along with information matching them to the digital signal, for use in descrambling and subsequent viewing or playback. Additional file format or transfer property information is prepared and made available to the encoder, in a bit addressable manner. As well, any authenticating function can be

combined, such as Digital Signature Standard (DSS) or Secure Hash Algorithm (SHA).

Using the predetermined key comprised of a transfer function-based mask set, the data representing the original content is manipulated at the inherent
5 granularity of the file format of the underlying digitized samples. Instead of providing, or otherwise distributing, watermarked content that is not noticeably altered, a partially "scrambled" copy of the content is distributed. The key is necessary both to register the sought-after content and to descramble the content into its original form.

10 The present invention uses methods disclosed in "Method for Stega-Cipher Protection of Computer Code," US Patent Application Serial No. 08/587,943, with respect to transfer functions related to the common file formats, such as PICT, TIFF, AIFF, WAV, etc. Additionally, in cases where the content has not been altered beyond being encoded with such functional data, it is possible for a
15 digital player to still play the content because the file format has not been altered. Thus, the encoded content could still be played by a plug-in digital player as discrete, digitally sampled signals, watermarked or not. That is, the structure of the file can remain basically unchanged by the watermarking process, letting common file format based players work with the "scrambled" content.

20 For example, the Compact Disc-Digital Audio (CD-DA) format stores audio information as a series of frames. Each frame contains a number of digital samples representing, for example, music, and a header that contains file format information. As shown in FIG. 1, according to an embodiment of the present invention some of the header information can be identified and "scrambled"
25 using the predetermined key at steps 110 to 130. The music samples can remain unchanged. Using this technique, a traditional CD-DA player will be able to play a distorted version of the music in the sample. The amount of distortion will depend on the way, and extent, that the header, or file format, information has been scrambled. It would also be possible to instead scramble some of the digital samples
30 while leaving the header information alone. In general, the digital signal would be protected by manipulating data at the inherent granularity, or "frames," of the CD-

DA file format. To decode the information, a predetermined key is used before playing the digital information at steps 140 and 150.

5 A key-based decoder can act as a "plug-in" digital player of broadcast signal streams without foreknowledge of the encoded media stream. Moreover, the data format orientation is used to partially scramble data in transit to prevent
10 unauthorized descrambled access by decoders that lack authorized keys. A distributed key can be used to unscramble the scrambled content because a decoder would understand how to process the key. Similar to on-the-fly decryption operations, the benefits inherent in this embodiment include the fact that the combination of watermarked content security, which is key-based, and the
15 descrambling of the data, can be performed by the same key which can be a plurality of mask sets. The mask sets may include primary, convolution and message delimiter masks with file format data included. r

The creation of an optimized "envelope" for insertion of watermarks
15 provides the basis of much watermark security, but is also a complementary goal of the present invention. The predetermined or random key that is generated is not only an essential map to access the hidden information signal, but is also the descrambler of the previously scrambled signal's format for playback or viewing.

In a system requiring keys for watermarking content and validating
20 the distribution of the content, different keys may be used to encode different information while secure one way hash functions or one-time pads may be incorporated to secure the embedded signal. The same keys can be used to later validate the embedded digital signature, or even fully decode the digital watermark
25 if desired. Publishers can easily stipulate that content not only be digitally watermarked but that distributors must check the validity of the watermarks by performing digital signature-checks with keys that lack any other functionality. The system can extend to simple authentication of text in other embodiments.

Before such a market is economically feasible, there are other
30 methods for deploying key-based watermarking coupled with transfer functions to partially scramble the content to be distributed without performing full public key encryption, i.e., a key pair is not necessarily generated, simply, a predetermined key's function is created to re-map the data of the content file in a lossless process.

Moreover, the scrambling performed by the present invention may be more dependent on the file in question. Dissimilarly, encryption is not specific to any particular media but is performed on data. The file format remains unchanged, rendering the file useable by any conventional viewer/player, but the signal quality can be intentionally degraded in the absence of the proper player and key. Public-key encryption seeks to completely obscure the sensitive "plaintext" to prevent comparisons with the "ciphertext" to determine a user's private keys. Centralized encryption only differs in the utilization of a single key for both encryption and decryption making the key even more highly vulnerable to attacks to defeat the encryption process. With the present invention, a highly sought after photograph may be hazy to the viewer using any number of commonly available, nonproprietary software or hardware, without the authorized key. Similarly, a commercially valuable song may sound poor.

The benefit of some form of cryptography is not lost in the present invention. In fact, some piracy can be deterred when the target signal may be known but is clearly being protected through scrambling. What is not anticipated by known techniques, is an ala carte method to change various aspects of file formatting to enable various "scrambled states" for content to be subsequently distributed. An image may lack all red pixels or may not have any of the most significant bits activated. An audio sample can similarly be scrambled to render it less-than-commercially viable.

The present invention also provides improvements over known network-based methods, such as those used for the streaming of media data over the Internet. By manipulating file formats, the broadcast media, which has been altered to "fit" within electronic distribution parameters, such as bandwidth availability and error correction considerations; can be more effectively utilized to restrict the subsequent use of the content while in transit as well as real-time viewing or playing.

The mask set providing the transfer function can be read on a per-use basis by issuing an authorized or authenticating "key" for descrambling the signal that is apparent to a viewer or a player or possessor of the authenticating key. The mask set can be read on a per-computer basis by issuing the authorized key that is

more generalized for the computer that receives the broadcast signals. Metering and subscription models become viable advantages over known digital watermark systems which assist in designating the ownership of a copy of digitized media content, but do not prevent or restrict the copying or manipulation of the sampled signal in question. For broadcast or streamed media, this is especially the case. Message authentication is also possible, though not guaranteeing the same security as an encrypted file as with general crypto systems.

The present invention thus benefits from the proprietary player model without relying on proprietary players. No new players will be necessary and existing multimedia file formats can be altered to exact a measure of security which is further increased when coupled with digital watermarks. As with most consumer markets for media content, predominant file formats exist, de facto, and corresponding formats for computers likewise exist. For a commercial compact disc quality audio recording, or 16 bit 44.1 kHz, corresponding file formats include: Audio Interchange File Format (AIFF), Microsoft WAV, Sound Designer II, Sun's .au, Apple's Quicktime, etc. For still image media, formats are similarly abundant: TIFF, PICT, JPEG, GIF, etc. Requiring the use of additional proprietary players, and their complementary file formats, for limited benefits in security is wasteful. Moreover, almost all computers today are multimedia-capable, and this is increasingly so with the popularity of Intel's MMX chip architecture and the PowerPC line of microchips. Because file formatting is fundamental in the playback of the underlying data, the predetermined key can act both as a map, for information to be encoded as watermark data regarding ownership, and a descrambler of the file that has been distributed. Limitations will only exist in how large the key must be retrofitted for a given application, but any manipulation of file format information is not likely to exceed the size of data required versus that for an entire proprietary player.

As with previous disclosures by the inventor on digital watermarking techniques, the present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks. These masks may include primary, convolution and message delimiter mask. In previous disclosures,

the functionality of these masks is defined solely for mapping. The present invention includes a mask set which is also controlled by the distributing party of a copy of a given media signal. This mask set is a transfer function which is limited only by the parameters of the file format in question. To increase the uniqueness or security of each key used to scramble a given media file copy, a secure one way hash function can be used subsequent to transfer properties that are initiated to prevent the forging of a particular key. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised.

These same cryptographic protocols can be combined with the embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play the streamed content in an unscrambled manner. As with digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations. The cryptographic protocols makes possible, as well, a message of text to be authenticated by a message authenticating function in a general computing device that is able to ensure secure message exchanges between authorizing parties.

Although various embodiments are specifically illustrated and described herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention.

What is claimed is:

1. A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:
- 5 identifying a portion of the format information to be encoded;
generating encoded format information from the identified portion of the format information; and
generating encoded digital information, including the digital sample and the encoded format information.
- 10 2. The method of claim 1, further comprising the step of requiring a predetermined key to decode the encoded format information.
3. The method of claim 2, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded format information is decoded with the predetermined key.
- 15 4. The method of claim 3, wherein the information output from the digital player represents a still image, audio or video.
5. The method of claim 3, wherein the information output represents text data to be authenticated.
- 20 6. A method for protecting a digital signal, the digital signal including digital samples in a file format having an inherent granularity, comprising the step of:
- creating a predetermined key comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.
- 25 7. The method of claim 6, wherein the digital signal represents a continuous analog waveform.
8. The method of claim 6, wherein the predetermined key comprises a plurality of mask sets.
- 30 9. The method of claim 6, wherein the digital signal is a message to be authenticated.

10. The method of claim 6, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

11. The method of claim 6, further comprising the step of:
using a digital watermarking technique to encode information that identifies
5 ownership, use, or other information about the digital signal, into the digital signal.

12. The method of claim 6, wherein the digital signal represents a still
image, audio or video.

13. The method of claim 6, further comprising the steps of:
selecting the mask set, including one or more masks having random or
10 pseudo-random series of bits; and
validating the mask set at the start of the transfer function-based mask set.

14. The method of claim 13, wherein said step of validating comprises the
step of:
comparing a hash value computed at the start of the transfer function-based
15 mask set with a determined transfer function of the hash value.

15. The method of claim 6, further comprising the steps of:
selecting the mask set, including one or more masks having random or
pseudo-random series of bits; and
20 authenticating the mask set by comparing a hash value computed at the start
of the transfer function-based mask set with a determined transfer function of the
hash value.

16. The method of claim 13, wherein said step of validating comprises the
step of:
comparing a digital signature at the start of the transfer function-based mask
25 set with a determined transfer function of the digital signature.

17. The method of claim 6, further comprising the steps of:
selecting the mask set, including one or more masks having random or
pseudo-random series of bits; and
30 authenticating the mask set by comparing a digital signature at the start of the
transfer function-based mask set with a determined transfer function of the digital
signature.

18. The method of claim 13, further comprising the step of:
using a digital watermarking technique to embed information that identifies
ownership, use, or other information about the digital signal, into the digital signal;
and

5 wherein said step of validating is dependent on validation of the embedded
information.

19. The method of claim 6, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital
signal, wherein the hash function is insensitive to changes introduced into the carrier
10 signal for the purpose of carrying the transfer function-based mask set.

20. A method for protecting a digital signal, the digital signal including
digital samples in a file format having an inherent granularity, comprising the steps
of:

creating a predetermined key comprised of a transfer function-based mask
set that can manipulate data at the inherent granularity of the file format of the
15 underlying digitized samples;

authenticating the predetermined key containing the correct transfer
function-based mask set during playback of the data; and

metering the playback of the data to monitor content.

20 21. The method of claim 20, wherein the predetermined key is authenticated
to authenticate message information.

22. A method to prepare for the scrambling of a sample stream of data,
comprising the steps of:

generating a plurality of mask sets to be used for encoding, including a
25 random primary mask, a random convolution mask and a random start of message
delimiter;

obtaining a transfer function to be implemented;

generating a message bit stream to be encoded;

30 loading the message bit stream, a stega-cipher map truth table, the primary
mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and
a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

23. A method to prepare for the encoding of stega-cipher information into a sample stream of data, comprising the steps of:

5 generating a mask set to be used for encoding, the set including a random primary mask, a random convolution mask, and a random start of message delimiter;
obtaining a message to be encoded;

compressing and encrypting the message if desired;

generating a message bit stream to be encoded;

10 loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

15 setting the message size equal to the total number of bits in the message bit stream.

24. The method of claim 23 wherein the sample stream of data has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

20 computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

25 25. The method of claim 13, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

processing the initial series of random bits through an MD5 algorithm;

30 using the results of the MD5 processing to seed a triple-DES encryption loop;

cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and

concatenating the triple-DES output bits into the random series of bits.

26. A method for copy protection of digital information, the digital
5 information including a digital sample and format information, comprising the steps of:

a identifying a portion of the digital sample to be encoded;

generating an encoded digital sample from the identified portion of the
digital sample; and

10 generating encoded digital information, including the encoded digital sample and the format information.

27. The method of claim 26, further comprising the step of requiring a predetermined key to decode the encoded digital sample.

28. The method of claim 27, wherein the digital sample and format
15 information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded digital sample is decoded with the predetermined key.

29. The method of claim 27, wherein information output will have non
20 authentic message data unless the encode digital sample is decoded with the predetermined key.

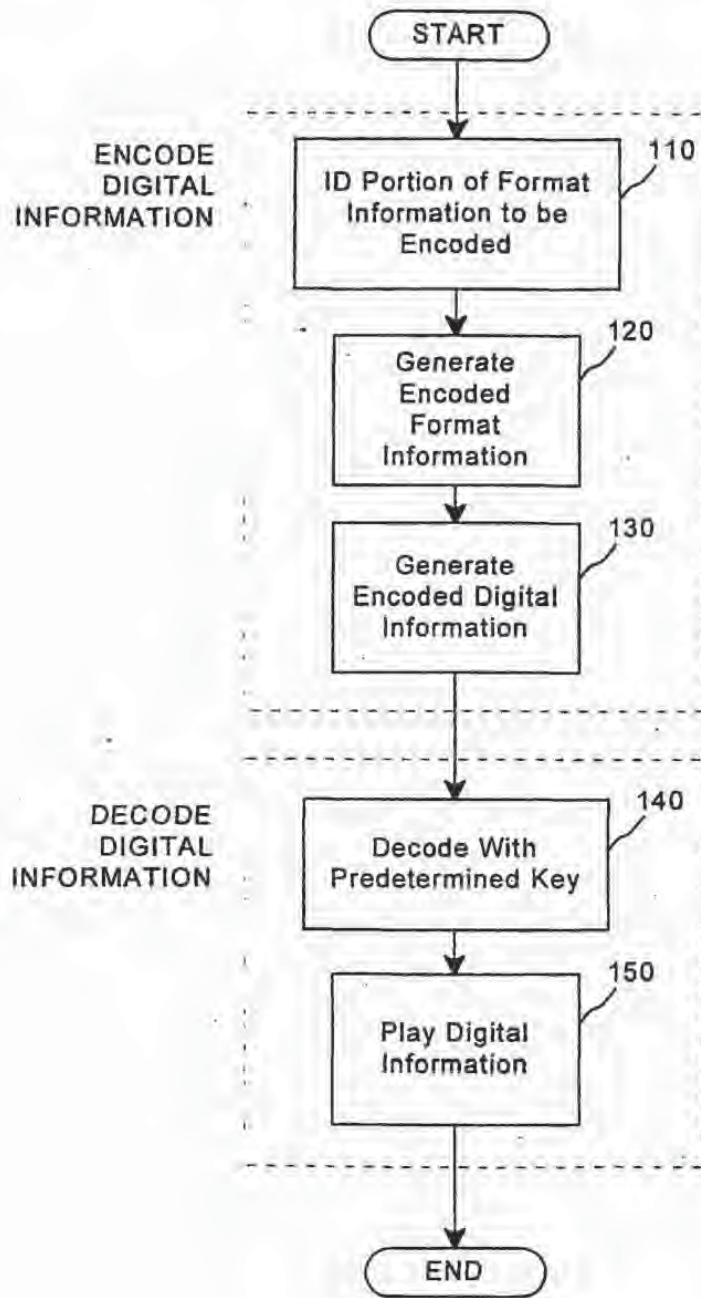


FIG. 1

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/18411

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

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)
IPC 7 G11B G06F H04N

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 used, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category ¹	Citation of document, with indication, where appropriate, of the relevant passages	Relevance to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1, 2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figure 4 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 28	1, 2
Y		3, 4
		-/-

Further documents are listed in the continuation of item C. Patent family members are listed in annex.

Categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "B" prior document but published on or after the international filing date
 "C" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another claim or other special reason (as specified)
 "D" document referring to an oral disclosure, use, exhibition or other means
 "E" document published prior to the international filing date but later than the priority date claimed
 "F" 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
 "G" 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
 "H" 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
 "I" document member of the same patent family

Date of the actual completion of the international search 20 July 2001	Date of mailing of the international search report 30. 07. 2001
Name and mailing address of the ISA European Patent Office, P.O. Box 5816 Palmstein 2 NL - 2200 PH Rijswijk Tel (+31-70) 340-2040, Tx: S1 651 epo nl Fax (+31-70) 340-3010	Authorized officer Sigala, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Serial Application No
PCT/US 00/18411

G.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) cited in the application column 5, line 1 -column 6, line 37 column 7, line 54 -column 10, line 11 column 11, line 31 -column 12, line 10 column 15, line 42 -column 16, line 32	6-12, 19-21
A		22, 23
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-4B column 8, line 24 - line 67	5, 26
X	WO 99 52271 A (MOSKOWITZ SCOTT A) 14 October 1999 (1999-10-14) abstract page 11, line 15 -page 13, line 13	6, 7, 10
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3, 4
A	WO 99 63443 A (DATAMARK TECHNOLOGIES PTE LTD; HO ANTHONY TUNG SHUEN (SG); TAM SIU) 9 December 1999 (1999-12-09) page 2, line 10 -page 5, line 16	6-8, 11, 12

Form PCT/ISA/WO10 (continuation of second sheet) (July 1999)

page 2 of 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 00/18411

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

- 1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

- 2. Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

- 3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

see additional sheet

- 1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
- 2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
- 3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
- 4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5,26-29

Protecting the distribution of digital data to be used with a digital player characterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

Digital signature encrypting technique combining transfer functions with predetermined key creation.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/18411

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
NL 1005523 C	15-09-1998	NONE	
WO 9744736 A	27-11-1997	AU 3206397 A	09-12-1997
US 5687236 A	11-11-1997	US 5613004 A EP 0872073 A WO 9642151 A	18-03-1997 21-10-1998 27-12-1996
US 5974141 A	26-10-1999	US 6076077 A US 6002772 A US 6097818 A	13-06-2000 14-12-1999 01-08-2000
WO 9952271 A	14-10-1999	US 6205249 B EP 1068720 A	20-03-2001 17-01-2001
EP 0649261 A	19-04-1995	JP 7115638 A US 5933499 A	02-05-1995 03-08-1999
WO 9963443 A	09-12-1999	AU 7683398 A EP 1103026 A	20-12-1999 30-05-2001

Form PCT/ISA/210 (patent family annex) (July 1992)

(19) World Intellectual Property Organization
International Bureau



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

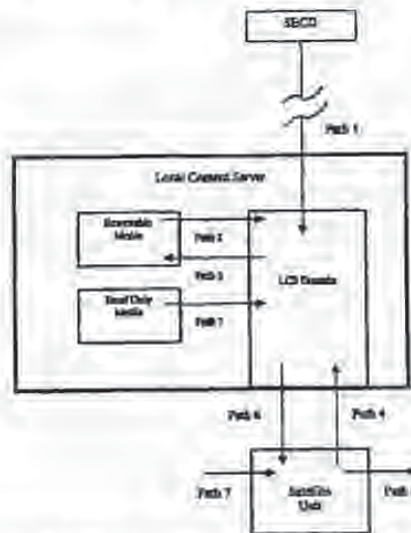
PCT

(10) International Publication Number
WO 01/18628 A2

- (51) International Patent Classification: G06F
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US); BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).
- (21) International Application Number: PCT/US00/21189
- (74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, LLP, The Warner, 1239 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).
- (22) International Filing Date: 4 August 2000 (04.08.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (81) Designated States (national): JP, US.
- (30) Priority Data:
60/147,134 4 August 1999 (04.08.1999) US
60/213,489 23 June 2000 (23.06.2000) 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).
- (71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).
- Published:
— Without international search report and to be republished upon receipt of that report.

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



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

[Continued on next page]

WO 01/18628 A2



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

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

A SECURE PERSONAL CONTENT SERVER

Field of Invention

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

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

10 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."

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

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

Background of the Invention

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

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

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

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

Summary of the Invention

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 These embodiments may include decisions about availability of a particular good or service through electronic means, such as the Internet, or means that can be modularized to conduct a transaction based on interconnection of various users (such as WebTV, a Nintendo or Sony game console with network abilities, cellular phone, PalmPilot, etc.). These embodiments may additionally be implemented in traditional auction types (including Dutch auctions). Consumers may view their anonymous
30 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
5 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
10 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
15 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
20 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
25 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
30 particular set of implementations of value-added content security in markets which may include unsecured and secure versions of the same value-added data (such as

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

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

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

The present invention also seeks to provide improvements to the art in enabling a realistic model for building trust between parties (or their agents) not in a "system", per se. Because prior art systems lack any inherent ability to allow for
25 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 feature in most data-added value markets: predictions, forecasts, and speculation over the value of information is largely an
30 unsuccessful activity for buyers and sellers alike. The additional improvement is the ability to maintain security even with unsecured or legacy versions of value-added information available to those who seek choices that fit less quantitative criteria—

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

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.

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

10 **Detailed Discussion of Invention**

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

A simple example provides insight into the scope of an LCS domain. If an LCS is assigned to an individual, then all music, video, and other content data which has lawfully issued to the individual may be freely used on that person's LCS domain
20 (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
25 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
30 Domain will be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between domains.

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

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

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

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

15 **LCS Functions**

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

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

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

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

SU Functions

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.

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

DETAILED DESCRIPTION OF THE INVENTION

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

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

25 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

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

```

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

25 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

30 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

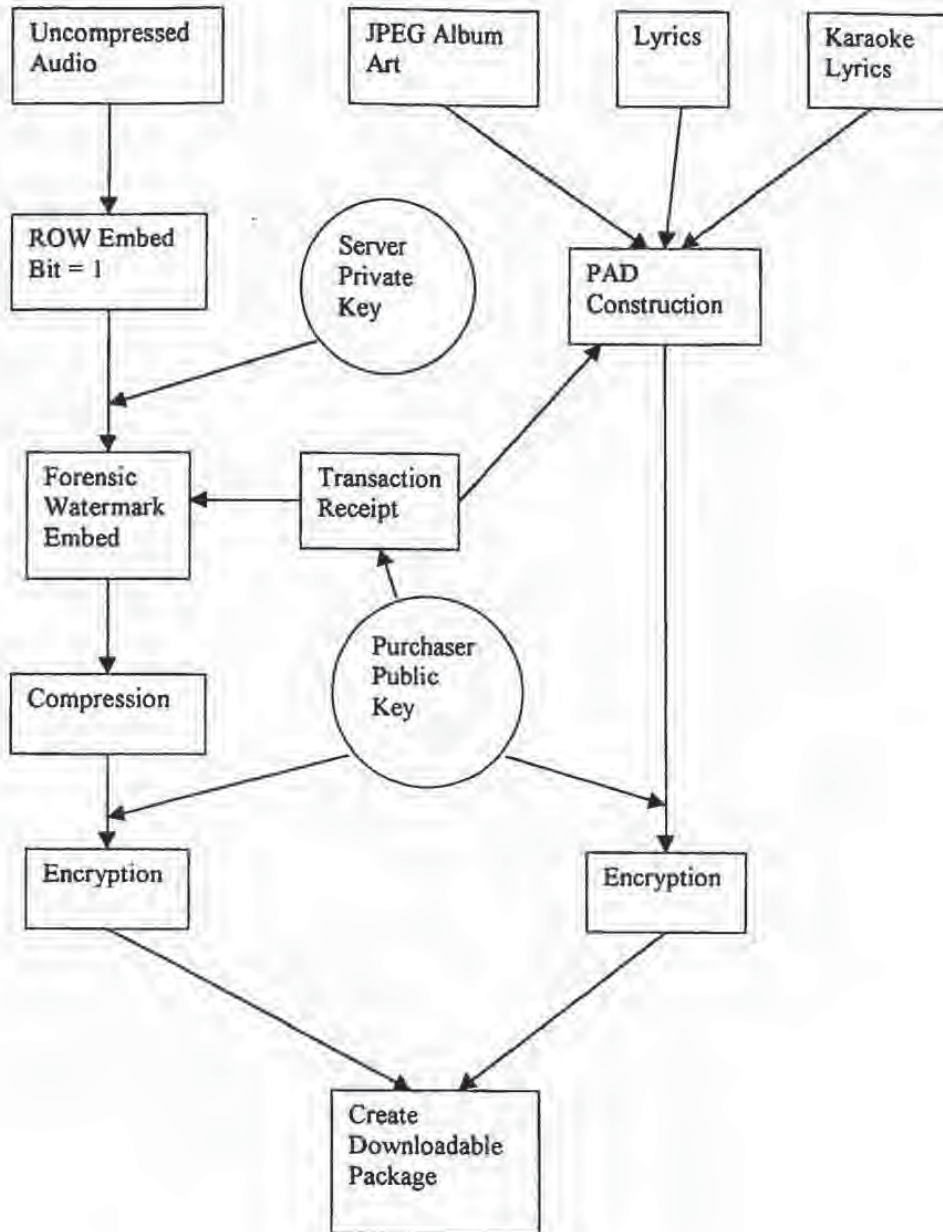


Table 2
SPCS Audio Player Input Stage

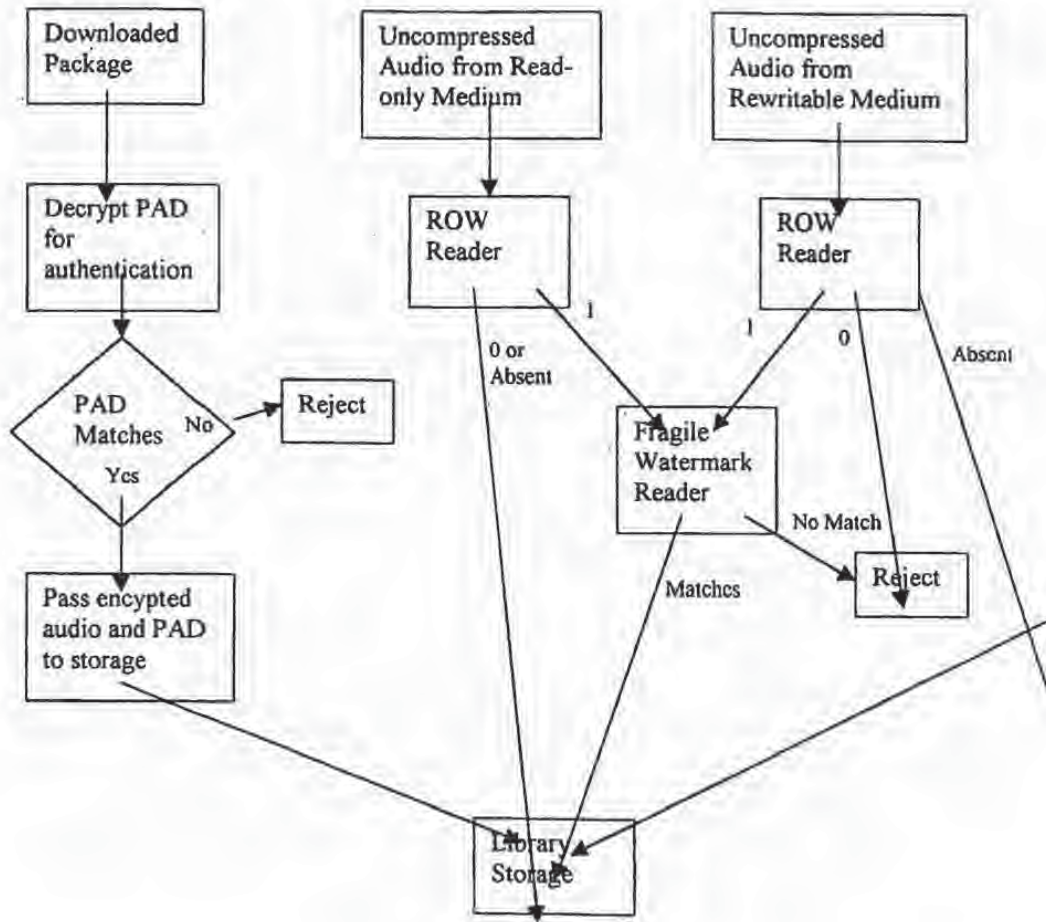
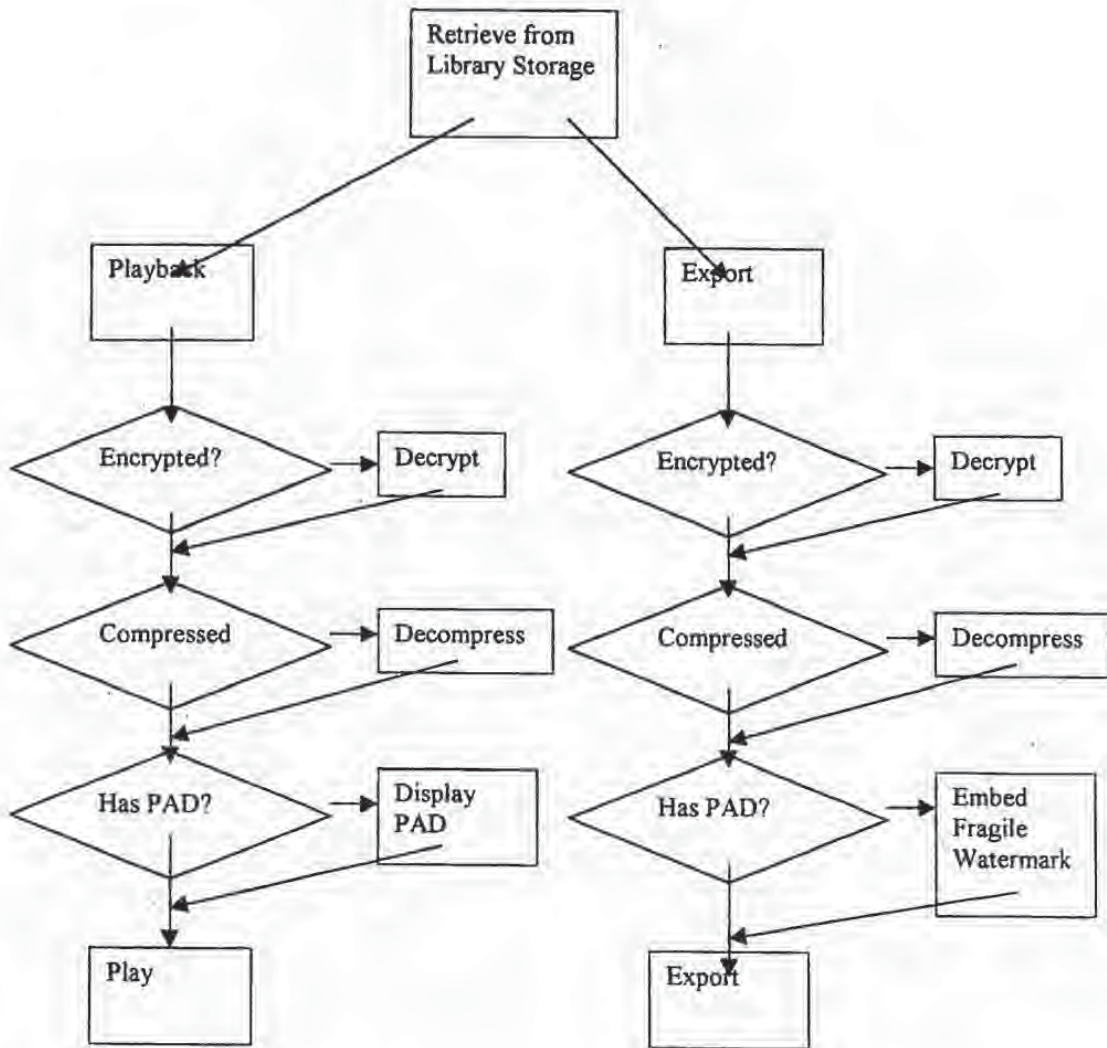


Table 3

SPCS Audio Player Output Stage



Claims:

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

-32-

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

- a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said
5 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
10 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
15 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
20 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
25 determines that digital content being received is authorized for use by the LCS.

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

5. The system of claim 3, wherein said domain processor comprises:
30 means for obtaining an identification code from an SU connected to the LCS's interface;

-33-

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

means for analyzing digital content received from an SU;

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

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

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

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

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

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

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

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

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

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

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

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

11. The system of claim 10,

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

wherein the SECD comprises

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

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

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

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

wherein the LCS comprises:

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

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

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

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

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

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

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

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

means receive a copy of the content data set;

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

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

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

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

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

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

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

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

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

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

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

a Local Content Server (LCS);

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

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

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

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

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

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

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

retrieving a copy of the requested content data set.

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

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

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

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

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

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

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

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

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

19 The Method of claim 17, further comprising

connecting a Satellite Unit (SU) to an LCS,

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

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

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

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

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

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

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

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

5 and

retrieving a copy of the requested content data set;

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

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

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

21. The Method of claim 20, further comprising:

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

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

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

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

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

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

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

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

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU).

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

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

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

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

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

26. The method of claim 24, further comprising:

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

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

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

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

re-saving the newly watermarked copy to the LCS.

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

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

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

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

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

-40-

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

receiving a copy of the content data set;

assessing whether the content data set is authenticated;

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

and

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

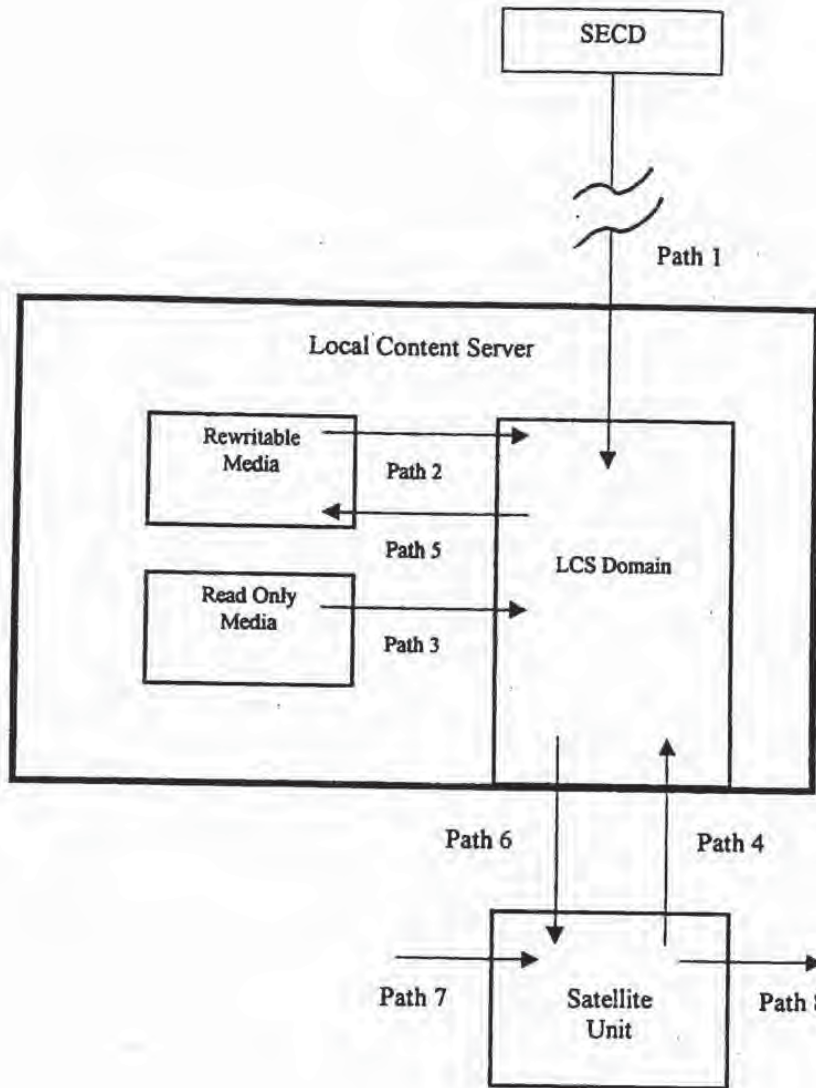


FIG. 1

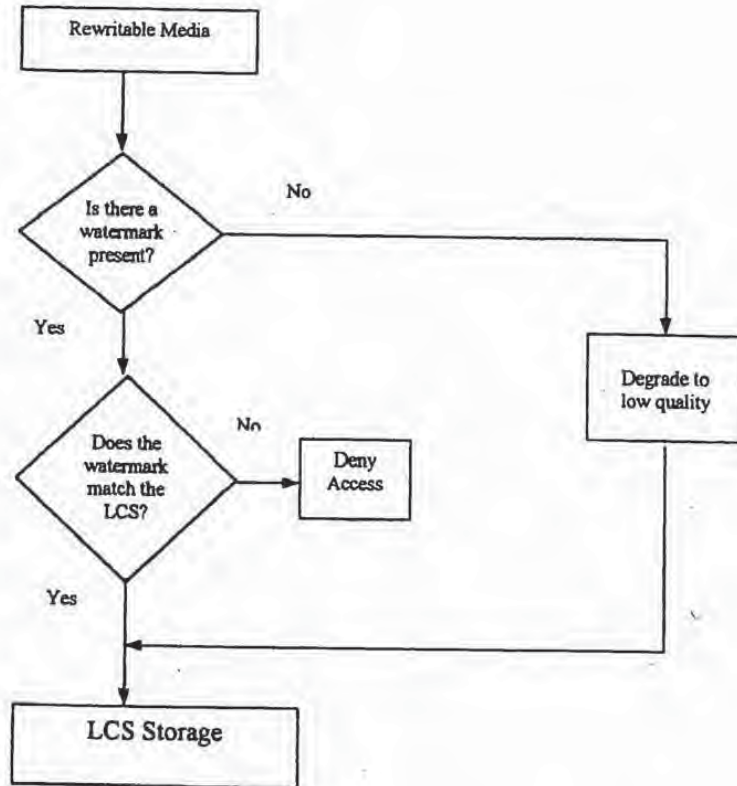


FIG. 2

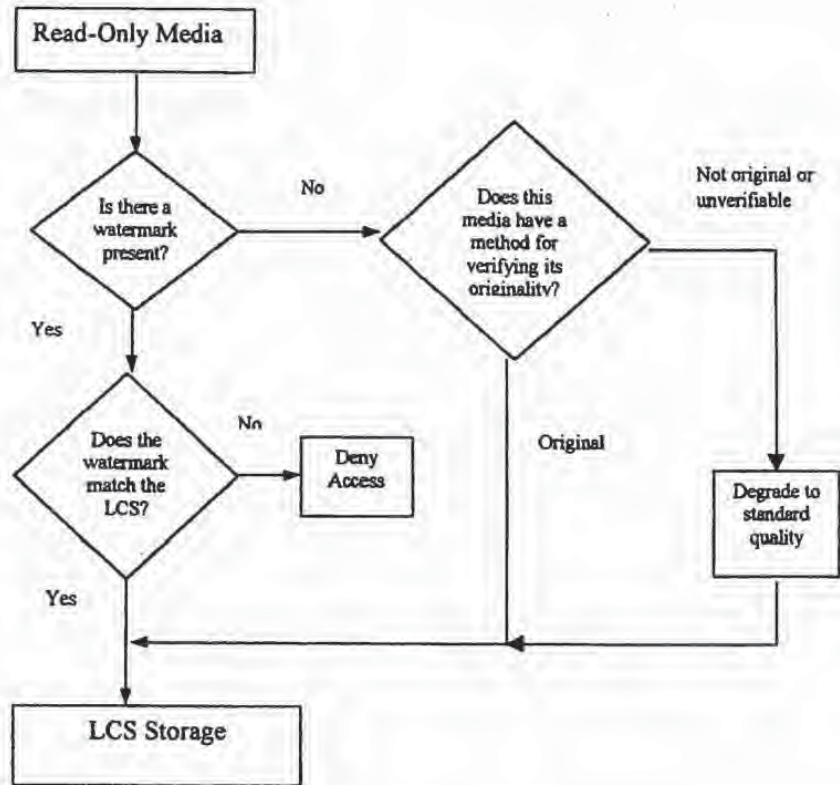


FIG. 3

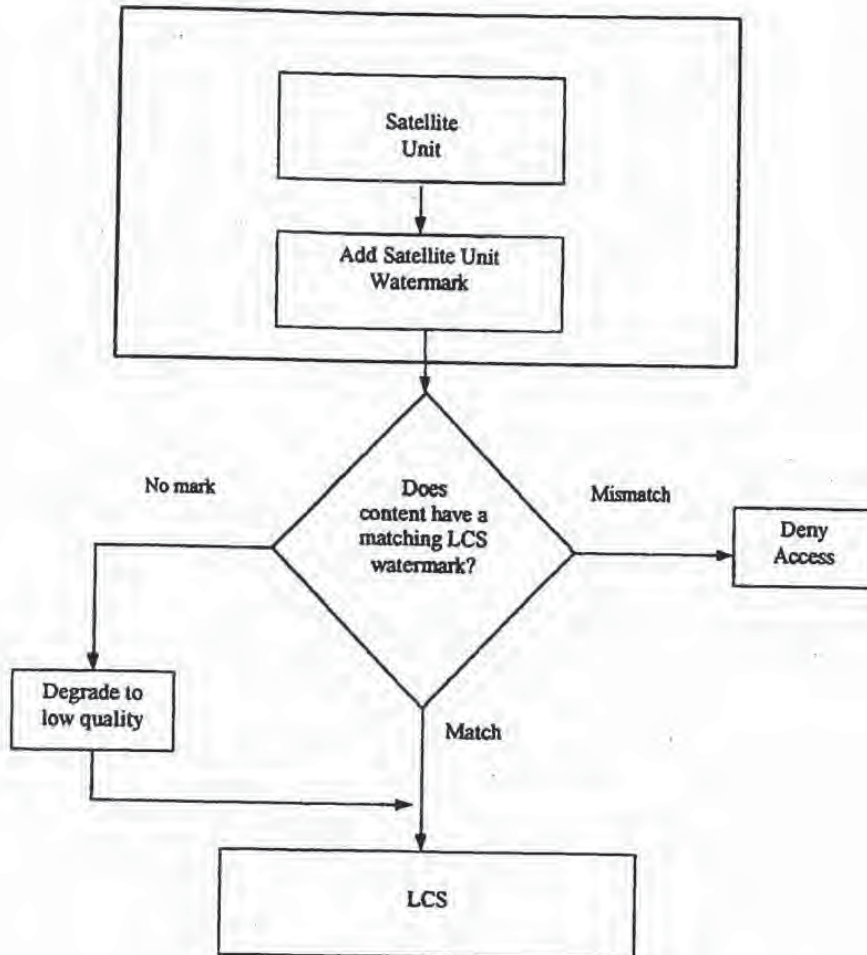


FIG. 4

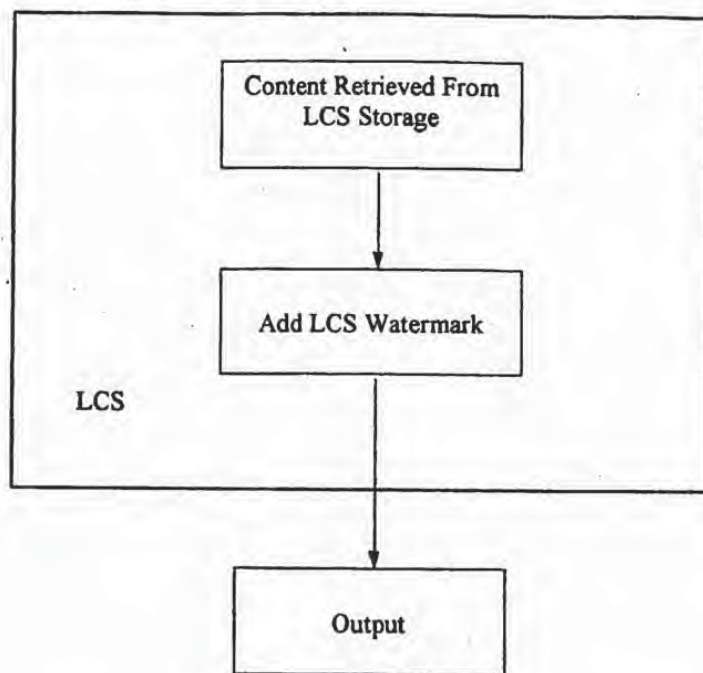


FIG. 5

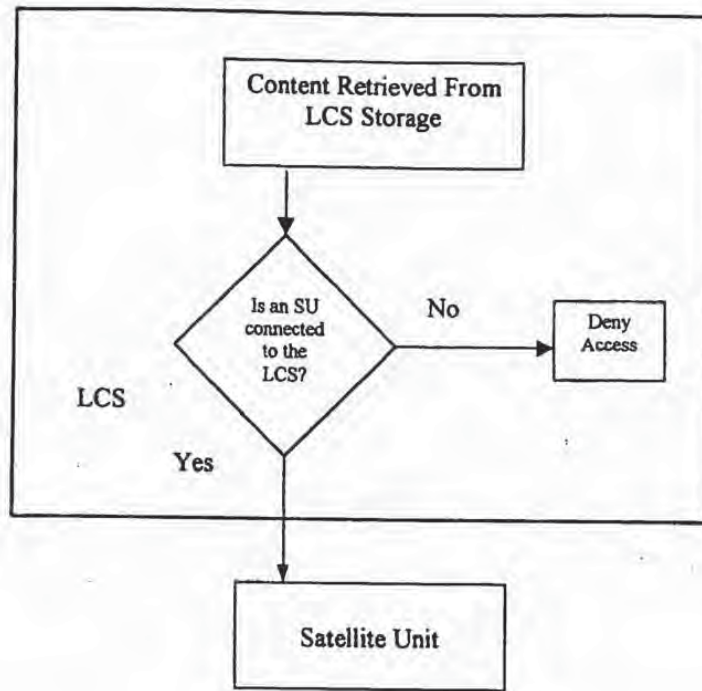


FIG. 6

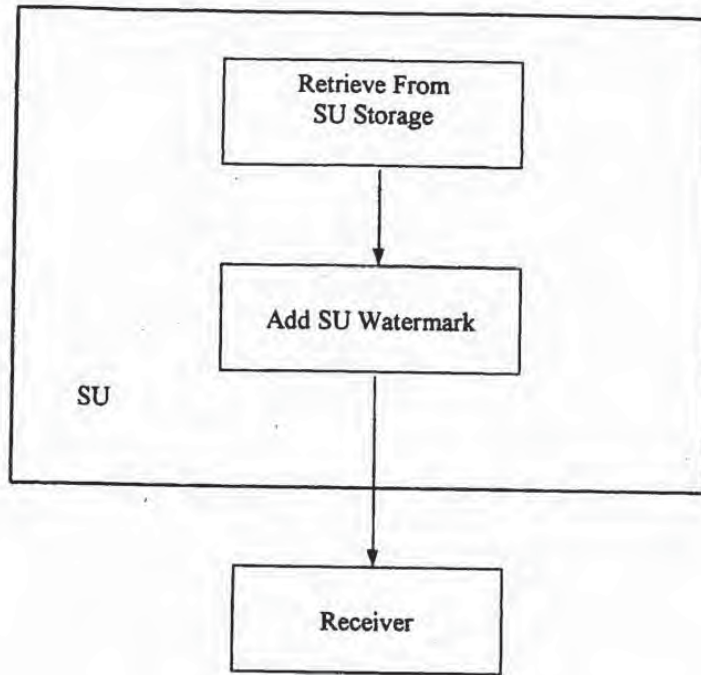


FIG. 7

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

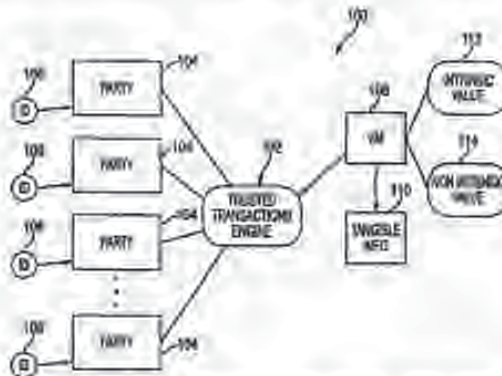
(18) International Publication Number
WO 01/43026 A1

- (51) International Patent Classification: G06F 17/60
- (72) Inventor: *aud*
- (21) International Application Number: PCT/US00/33126
- (75) Inventor/Applicant (for US only): MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue, #2505, Miami, FL 33160 (US).
- (22) International Filing Date: 7 December 2000 (07.12.2000)
- (74) Agents: CHAPMAN, Floyd, B. et al.; Intellectual Property Department, Brobeck, Phleger & Harrison LLP, Suite 800, 1333 H Street, N.W., Washington, DC 20005 (US).
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:

60/169,274	7 December 1999 (07.12.1999)	US
09/456,319	8 December 1999 (08.12.1999)	US
09/545,589	7 April 2000 (07.04.2000)	US
09/594,719	16 June 2000 (16.06.2000)	US
PCT/US00/21189	4 August 2000 (04.08.2000)	US
09/657,181	7 September 2000 (07.09.2000)	US
60/234,199	20 September 2000 (20.09.2000)	US
09/671,739	29 September 2000 (29.09.2000)	US
Not furnished	7 December 2000 (07.12.2000)	US
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue, #2505 Miami, FL 33160 (US).

{Continued on next page}

(54) Title: SYSTEMS, METHODS AND DEVICES FOR TRUSTED TRANSACTIONS



(57) Abstract: The invention discloses a system for enhancing trust in transactions, most particularly in remote transactions between a plurality of transactional parties, for instance a seller and buyer(s) of goods and/or services over a public computer network such as the Internet. Trust is disclosed to be a multivalent commodity, in that the trust that is to be enhanced relates to information about the subject matter of the transactions (e.g., the suitability of the goods and services sold), the bona fides of the supplier of the goods and services, the appropriateness of a pricing structure for a particular transaction or series of transactions, a quantum of additional transactional value that may be imparted to the transactional relationship, security of information exchange, etc. An important contributor to trust for such aspects of the transaction is disclosed to be the use of highly-secure steganographic computer processing means for data identification, authentication, and transmission, such that confidence in the transaction components is enhanced. By providing an integrated multivalent system for enhancing trust across a variety of categories (for a variety of transaction species, including those in which the need for trust is greater on the part of one party than of another, as well as those in which both require substantial trust enhancement), the invention reduces barriers to forming and optimizing transactional relationships.



WO 01/43026 A1



Published:

- *With international search report.*
- *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

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.

SYSTEMS, METHODS AND DEVICES FOR TRUSTED TRANSACTIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the transfer of information between parties; in particular, it relates to systems, methods, and devices for trusted transactions.

2. Description of the Related Art

Transactions are increasingly characterized by the amount and quality of information available to market participants. Whereas a seller seeks profit driven arrangements, which may vary over the course of a relationship with a particular buyer or consumer, buyers seek satisfaction of at least one of the following: price, selection or service. At any time the buyer or seeker of value-added information may lack recognition of the seller or provider of such information, even if coupled with a "manufactured" product or good. Sellers, or providers, similarly lack any information about individual buyers, buying groups or agents, and may only have information regarding potentially profitable transaction events defined by at least one of the following: existing market for goods or services, targeted projected market for new goods or services, or those consumers or buyers who currently engage in transactions with the provider. Transactions are the result of customer profiling, a form of recognizable pattern analysis for commerce.

Transactions conducted electronically, often in an online environment taking advantage of networks, such as the Internet and/or World Wide Web ("WWW"), form an increasingly-important subset of transactions. Most obviously, retail sales transactions in which individual customers purchase goods or services from a central web server using a WWW connection have become a prominent form of electronic transactions, though such transactions are by no means the only or even necessarily the predominant category of electronic transactions.

Electronic transactions pose special challenges for transaction parties. Some of these challenges relate to the difficulty of providing to a prospective acquirer (e.g., a purchaser) of goods or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics of the product in question. This is true in part, for instance, because the customer

cannot necessarily handle, sample, or evaluate at first hand the goods or services in question in an online transaction to the same extent to which he could evaluate them in an in-person transaction. It may also be true because of the fear of counterfeit, defective, or otherwise unsuitable products that may be viewed as more easily
5 "passed off" (assuming a certain non-zero incidence of deceit and/or inadequate suitability verification among suppliers of products) in an electronic transaction than in an in-person transaction.

Further challenges in online transactions revolve around the serious concerns regarding security of such transactions. Such security-related concerns arise from
10 the inherently-vulnerable nature of distributed public networks such as the internet, in which transaction parties cannot necessarily determine the path by which data travelling to and from them will take. Nor is it always possible to determine the identity of another transaction party, or to ensure that such other transaction party will take adequate precautions with sensitive data (for instance, data related to the
15 identity or financial details (e.g., credit card number) of the first transaction party) transmitted during the course of proposing, evaluating, negotiating, executing, or fulfilling a transaction. Thus, concerns are raised about interception, inadequate safeguarding, or other unauthorized or inappropriate use of data generated or transmitted between transaction parties. Such concerns have raised the perceived
20 need for security technologies adaptable for online transactions. Generically, these technologies have included encryption, scrambling, digital watermarking, and like methods of protecting transaction-related data.

Two conventional techniques for providing confidentiality and/or authentication currently in use involve reciprocal and non-reciprocal encrypting.
25 Both systems use non-secret algorithms to provide encryption and decryption, and keys that are used by the algorithm.

In reciprocal algorithm systems, such as DES, the same key and algorithm is used to encrypt and decrypt a message. To assure confidentiality and authenticity, the key is preferably known only to the sending and receiving computers, and were
30 traditionally provided to the systems by "secure" communication, such as courier.

In non-reciprocal systems, such as those described in U.S. Patent 4,218,582, a first party to a communication generates a numerical sequence and uses that -

sequence to generate non-reciprocal and different encrypting and decrypting keys. The encrypting key is then transferred to a second party in a non-secure communication. The second party uses the encrypting key (called a public key because it is no longer secure) to encrypt a message that can only be de-crypted by the decrypting key retained by the first party. The key generation algorithm is arranged such that the decrypting key cannot be derived from the public encrypting key. Similar methods are known for using non-reciprocal keys for authentication of a transmission. In the present invention, the non-secure "public" key is used to a message that has been encrypted using a secure "private" key known only to the originating party. In this method the receiving party has assurance that the origination of the message is the party who has supplied the "public" decrypting key.

SUMMARY OF THE INVENTION

Thus, a need has arisen for a system and method for enhancing trust on the part of participants in transaction. This may be with respect to all aspects of the transaction as to which trust may be an influential factor (or, viewed negatively, in which the lack of trust may be a potential bottleneck prohibiting consummation of the transaction, or of a more-optimal transaction, or of a series of transactions in a mutually-beneficial transactional relationship).

A need has also arisen for trust enhancement for transactions in connection with sophisticated security, scrambling, and encryption technology, for instance that provided by steganographic encryption, authentication, and security means.

A need has also arisen to provide these technologies in an integrated method and system, optimally requiring comparatively little processing resources so as to maximize its usefulness and minimize its cost.

The present invention represents a bridge between mathematically determinable security and analog or human measures of trust. These measures are typically perceptible or perceptual when evaluating value-added information. Additionally, a higher level of transparency between parties is assured, because information flow is recognizable and controllable by transacting parties at will.

According to one embodiment of the present invention, a method for trusted transactions is provided. The method includes the steps of (1) establishing an

agreement to exchange digitally-sampled information between a first and a second party; (2) exchanging the digitally-sampled information between the first and the second party; and (3) approving the digitally-sampled. The digitally-sampled information may be approved with an approval element, for example, a predetermined key, a predetermined message, or a predetermined cipher. The step of approving the digital information may include authorizing the digital information with the approval element, verifying the digital information with the approval element, or authenticating the digital information with the approval element. The predetermined cipher may be a steganographic cipher or a cryptographic cipher.

10 According to another embodiment of the present invention, a method for conducting a trusted transaction between two parties that have agreed to transact is provided. The method includes the steps of (1) establishing a secure transmission channel between the two parties; (2) verifying an identity of at least one of the parties; (3) determining an amount of value-added information to be exchanged
15 between the parties; (4) verifying the agreement to transact; and (5) transmitting the value-added information. The value-added information may include value-adding components.

According to another embodiment of the present invention, a method for conducting at least one trusted transaction between two parties is provided. The method includes the steps of (1) authenticating the parties; (2) agreeing to a security of a transmission channel; (3) exchanging secondary value-added information; (4) determining at least one term for a primary value-added information exchange; and (5) facilitating payment for the transaction based on the terms.

25 According to another embodiment of the present invention, a method for conducting a trusted transaction between two parties is provided. The method includes the steps of (1) establishing a steganographic cipher; (2) exchanging secondary value-added information between the parties; (3) agreeing to terms for the exchange of primary value-added information; and (4) facilitating payment for the transaction.

30 According to another embodiment of the present invention, a method for conducting a trusted transaction between parties is provided. The method includes the steps of (1) identifying a unique identification for each of the parties, a unique

identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; (2) applying a steganographic cipher; and (3) verifying an agreement to transact between the parties. Once the parties are identified by the unique identification, 5 transaction identification, or the unique identification of the value-added information, secondary terms and conditions may be offered for acceptance. The transaction may take several additional steps and may include additional value-adding components to reach a legal agreement.

The agreement may cause a secondary term to be enabled for one of the 10 parties. For example, the agreement may be related to the ability to choose ownership in the seller instead of some benefit in price, service or selection. This ownership may be priced according to traditional options pricing methodologies. Essentially the "discount" in cash value terms, may be the option price. So if there is a price, selection or service that can be equated to some cash equivalent amount, 15 that amount can be used by the buyer as a right, but not obligation to purchase equity in the seller. Alternatively, the cash equivalent may have a direct equivalence in equity prices.

According to another embodiment of the present invention, a method for bi-directionally exchanging value-added information between parties is provided. The 20 method includes the steps of (1) associating a plurality of unique identifiers with the value-added information, the value-added information including a digital watermark, a file header, a file attachment, and/or a file wrapper; (2) associating each of the parties with unique identifiers, the unique identifiers including a digital watermark, a file header, a file attachment, and/or a file wrapper; and (3) exchanging value-added 25 information between the parties.

According to another embodiment of the present invention, a method for exchanging value-added information between parties is provided. The method includes the steps of (1) providing a data transmission means; (2) verifying the 30 parties to the transaction; (3) negotiating a term such as a price, a service, and/or a selection; and (4) binding the term to the information using a digital watermark, a file header, metadata, and/or a file wrapper. The bound transaction terms may include value-added information.

According to another embodiment of the present invention, a method for trusted transactions is provided. The method includes the steps of (1) receiving data to be processed; (2) determining a structure of the data; (3) determining if the data is authentic; and (4) determining an associated usage of the data based on the data structure and the authenticity of the data.

According to another embodiment of the present invention, a method for secure transaction is provided. The method includes the steps of (1) receiving a request to process a transaction; (2) uniquely identifying the source of the request; (3) uniquely identifying at least one term of the request; and (4) storing identification information for transaction negotiation.

According to another embodiment of the present invention, a method for the facilitation of the exchange of information data between at least a first party and a second party is provided. The method includes the steps of (1) receiving a rule governing information data from a first party; (2) receiving a request for the information data from a second party; (3) matching the predetermined rule with the request; and (4) uniquely identifying the information data and the first and second parties. The information data may include unstructured data or structured data.

According to another embodiment of the present invention, a method for the management of rights is provided. The method includes the steps of (1) receiving information; (2) determining whether the information is structured information or unstructured information; (3) identifying the information with a steganographic cipher; (4) authenticating the information with a digital signature or a digital watermark check; and (5) associating the identification and authentication results with a predetermined record, a predetermined rule, or a predetermined function.

According to another embodiment of the present invention, a method for risk management is provided. The method includes the steps of (1) receiving information; (2) determining whether the information is structured or unstructured; (3) identifying information with a predetermined ciphered key; (4) authenticating information with a digital signature, a digital watermark check, or a predetermined ciphered key; (5) associating identification and authentication results with a predetermined rule; and (6) limiting access based on a predetermined exposure of a decision maker.

According to another embodiment of the present invention, a method for securely exchanging information data between parties is provided. The method includes the steps of (1) creating a private key; (2) deriving a corresponding public key corresponding to the information data sought and at least one of (a) verifiable data associated with different versions of the information data, (b) verifiable data associated with a transmitting device, and (c) verifiable data associated with an identity of the party seeking the information data; (3) establishing a set of one time signatures relating to the information data; (4) establishing a hierarchy of access to the set of one time signatures; (5) creating a public key signature, the public key signature being verifiable with the public key, including the hierarchy of access to the set of one time signatures; (6) providing the information to a certification authority for verification; and (7) verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

According to another embodiment of the present invention, a method for authenticating an exchange of a plurality of sets of information data between parties is provided. The method includes the steps of (1) creating a plurality of hierarchical classes based on a perceptual quality of the information data; (2) assigning each set of information data to a corresponding hierarchical class; (3) defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged; (4) predetermining access to the sets of information data by perceptually-based quality determinations; (5) establishing at least one connection between the exchanging parties; (6) perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; and (7) enabling a trusted transaction based on verification, and associated access, governing at least one of a set of information data sets.

According to another embodiment of the present invention, a method for authenticating the exchange of perceptual information data between parties over a networked system is provided. The method includes the steps of (1) creating a plurality of hierarchical classes based on a perceptual quality of the information data; (2) assigning each set of information data to a corresponding hierarchical class; (3) defining access to each hierarchical classes and to each set of information data

based on at least one recognizable feature of the information data to be exchanged; (4) perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; (5) enabling a trusted transaction of the information data based on verification of means of payment, and associated access, 5 governing at least one copy of the information data sought; (6) associating the transaction event with the information data prior to transmission of the information data; and (7) transmitting and confirming delivery of the information data

According to another embodiment of the present invention, a device for conducting a trusted transaction between parties who have agreed to transact is 10 provided. The device includes means for uniquely identifying unique identification information, such as a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; a steganographic cipher; and a means for verifying an agreement to transact between 15 the parties.

According to another embodiment of the present invention, a device for conducting a trusted transaction between parties who have agreed to transact is provided. The device includes means for uniquely identifying unique identification information such as a unique identification of one of the parties, a unique 20 identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; and means for enabling a subsequent mutually agreed to at least one term.

According to another embodiment of the present invention, a device for conducting trusted transactions between parties is provided. The device includes a 25 steganographic cipher; a controller for receiving input data or outputting output data; and an input/output connection. The device may have a unique identification code.

According to another embodiment of the present invention, a trusted transaction device for transmitting authentic value-added information data between parties is provided. The device includes a display; a unique identifier; means for 30 ciphering information that is input and output; means for interacting with other similarly functional devices; and means for storing or retrieving value-added information and a value-adding component.

According to another embodiment of the present invention, a device for securely exchanging information data is provided. The device includes means for creating a private key by the party seeking information; means for deriving a corresponding public key based on the predetermined data and verifiable data associated with different versions of the information, verifiable data associated with a transmitting device, or verifiable data associated with the identity of the party seeking information; means for creating a set of one-time signatures relating to the predetermined data; means for validating a predetermined hierarchy of access of the set of one-time signatures; means for creating a public key signature, verifiable with the public key, including the access hierarchy of one time signatures; means for securely transacting predetermined data by providing information relating to a proposed transaction; and means for verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

According to one embodiment of the present invention, a system for the secure exchange of predetermined, verifiable information data between parties is provided. The system includes at least one condition for the use of the information; means for differentiating between predetermined information and other seemingly identical information based on an authentication protocol; means for associating authenticity of verifiable information data with at least one condition for use; a storage unit for storing the predetermined, verifiable information; and means for communicating with the predetermined, verifiable information storage.

According to one embodiment of the present invention, a system for the exchange of information is provided. The system includes at least one sender; at least a receiver; a verifiable message; and a verification of the message by at least one of the senders and the receivers. A verification of the message may enable a decision over receiving additional related information.

According to one embodiment of the present invention, a system for computer based decision protocol is provided. The system includes a means for identifying between structured and unstructured information; a means for authenticating structured information; and a means for enabling a decision rule based on the identity and authenticity of the information.

According to one embodiment of the present invention, a system for computer-based decision protocol is provided. The system includes means for identifying between structured and unstructured information; means for identifying structured information; and means for enabling a predetermined decision rule based on the identity of the information.

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 is a block diagram of a system for trusted transactions according to one embodiment of the present invention;

Fig. 2 is a schematic of a local content server environment according to one embodiment of the present invention;

Fig. 3 is a flowchart depicting an example of an authentication according to one embodiment of the present invention;

Fig. 4 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 5 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 6 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 7 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 8 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 9 is a flowchart of a method for trusted transactions according to one embodiment of the present invention;

Fig. 10 depicts a device for trusted transactions according to one embodiment of the present invention.

Fig. 11 is a block diagram of a person information device according to one embodiment of the present invention;

Fig. 12 is a block diagram of an authentication device according to one embodiment of the present invention; and

Fig. 13 is a flowchart depicting an authentication process according to one embodiment of the present invention.

5 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In order to assist in the understanding of the present invention, the following definitions are provided and are intended to supplement the ordinary and customary meaning of the terms:

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

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: Encryption is a method of securitizing data. For example, encryption may be data scrambling using keys. For value-added or information rich
20 data with content characteristics, encryption is typically slow or inefficient because content file sizes tend to be generally large. Encrypted data is sometimes referred to as "ciphertext."

High Quality: A transfer path into the LCS Domain that allows digital content of any quality level to pass unaltered. "High Quality" can also mean
25 unfettered access to all VACs.

Local Content Server (LCS): A device or software application that can securely store a collection of value-added digital information, such as entertainment media. The LCS has a unique ID.

LCS Domain: A secure medium or area where digital content can be stored,
30 with an accompanying rule system for transfer into and out of itself.

Low Quality: A transfer path into the LCS Domain that degrades the digital content to a sub-reference level. In an audio implementation, this might be defined

as below CD Quality. Low Quality can also mean no VACs are allowed in to the system.

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.

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

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

Satellite Unit: A portable medium or device that can accept secure digital content from a LCS through a physical, local connection and that can either play or make playable the digital content. The satellite unit may have other functionality as it relates to manipulating the content, such as recording. The satellite unit has a Unique ID.

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the data. Value-added or information rich data may be manipulated at the inherent granularity of the file format, essentially through the use of a transfer function. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. The manipulation may be associated with a predetermined key, which may be made cryptographically secure or made into asymmetric 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, generally alters the data such 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.

Secure Electronic Content Distributor (SECD): An entity that can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. This may be referred to as a "certification authority." SECDs may have differing arrangements with consumers and providers of value-added information or other parties that may conduct transactions, such as business to business relationships. The level of trust place into an SECD can be dynamically adjusted as transactions warrant or parties agree.

Standard Quality: A transfer path into the LCS Domain that 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. Standard Quality may also refer to a particular set of VACs that are allowed into the system.

Unique Identification, or 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-Adding Component (VAC): An attachment to the content that enhances the user's experience of the content. VACs may be metadata, headers, usage rules, etc. For music, some examples are: album art, lyrics, promotional material, specialized playback instructions. For other embodiments, the value-adding component may relate to the consumer's personal information, preferences, payment options, membership, or expectations over a transaction.

The agglomeration of value-adding components is "value-added information." In the aggregate, value creation on an informational level can be observed and measured.

Value-added Information: Value-added information is generally 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.

Verification: Called "integrity," in cryptography, an intruder preferably cannot substitute false messages for legitimate ones; the receiver of the message (embedded or otherwise within the value-added information) preferably is assured that the message (or by effects, the origin of the carrier within which the message is stored) that the message was not modified or altered in transit.

Note: The above definitions may be interchanged in different embodiments of the present invention and serve as parameters in breaking down value-added information exchange and trusted transactions.

Embodiments of the present invention and their technical advantages may be better understood by referring to Figs. 1 through 13, like numerals referring to like and corresponding parts of the various drawings.

Increasingly, a premium is being placed on both recognition and trust. These intangible elements are both expensive to create and to maintain given the ever-decreasing amount of human contact during transactions. To the extent that many transactions are now possible without any human contact, the present invention is a unique improvement over the art in enabling bi-directional authentication of information between parties to enable "trusted transactions" between those parties

For anonymous market exchanges, transparency and data integrity, as well as confidence, serve to promote confidence and growth in product, goods and service offerings. Perception is an expensive trigger to trusted transactions reinforced by the experience of market participants.

Confidence as well as experience enable trust: in an anonymous marketplace, it is desirable for the authenticity of value-added information and value-added components to be made more transparent and independently verifiable by all concerned parties. Transparency is valued in education and experience.

A purchase decision between a buyer and a seller is equivalent to the temporal establishment of a mutually agreed "abstraction of value" in the information sought or exchanged, which may be represented in both tangible and intangible forms. Perception is the natural limit of "fair pricing," and drives value determination of a particular good or service. Perception may be structured by context, history, and/or condition. The "value" of a particular transaction has an intrinsic meaning (financial, economic, legal, political, social, statistical or actuarial meaning), temporally (at the instant of the transaction), for both the buyer and seller (reached an agreement including offer acceptance and consideration), with any inclusive terms and conditions (hereinafter, "terms") governing the transaction (price, credit terms, delivery options, and other parameters concerning the good or service with respect to which the transaction takes place). As a result of such trusted

transactions, the parties gain confidence. Even parties who may be anonymous benefit from the contemplated improvements over the art.

Referring to Fig. 1, a block diagram of a system for trusted transactions is provided. System 100 includes trusted transaction engine 102, which interacts with a plurality of parties 104. Each party 104 has a unique identity 106.

Value-added information 108, as defined above, includes both intrinsic value 112 and nonintrinsic value 114. A vendor (who may be a party 104) may decide what information has value (i.e., should be considered to have intrinsic value or not), and this decision may be made on a per transaction basis.

The present invention may provide advantages to all parties involved, including pricing flexibility, a reduction (or optimization) of transaction costs, a recognition of value-adding components, and the ability to provide provable security and trust among parties. Each will be discussed in greater detail, below.

1. Pricing flexibility for parties

Because buyers and sellers have complementary but competitive goals in consummating a transaction, variable pricing in the present invention is supported without any detrimental affect on the potential relationship between the buyer and the seller, or their agents. Known systems depend primarily on securing payment; payment alone, however, does not ensure the buyer and the seller of lasting protection of their respective "intangible assets," especially those that are increasingly based on value-adding information (e.g., trademarks, copyright, patents, credit history, health condition, etc.). The buyer fears identity theft ("first party," or "sentimental" piracy), while the seller fears piracy of valuable information assets ("third party," or "positional" piracy). The separation of authentication of perceptually-represented goods and services and value-adding information, from payment security, is an important novel feature of the present invention.

Known systems specify a number of methods for ensuring "security." However, the primary feature of these approaches is access control based solely on proof that a purchase has been completed. This means that if a purchase can be enabled only by determinations that a transaction was successful, the ability to entice more transactions or otherwise increase the development of maintainable trusted transactions is undermined. Simply, the fact that a purchase was completed does not

mean that a trusted transaction has, in fact, been enabled. No provision for establishing a trusted relationship between the buyer and the seller takes place absent some authenticable exchange of additional value-adding information. The present invention increases the likelihood of a successful trusted transaction and extends beyond the ability to pay (assuming no "identity theft" has occurred). The present invention provides additional means for verifiable information exchange that enhance the experience of the buyer and the seller in seeking trusted transactions.

Because many manufactured goods are likely to have similar costs from a strict manufacturing standpoint, the value-added service, or services, that are provided to the buyer are likely to encourage additional opportunities for trusted transaction. The seller can benefit by leveraging a single purchase into a profitable relationship. Even distribution costs may be commoditized for all similar tangible goods. A series of non-contiguous or non-temporal transactions alone would constitute a profitable relationship if the buyer is satisfied and the seller is profiting. That pricing, and its terms, may be varied dynamically or supported flexibly (based on information exchange at the time or leading to a transaction), is another improvement over the art. The incorporation of micropayments becomes more feasible as the cost of trust has been reduced and thus smaller discrete increments of monetary consideration are easier to support to the benefit of buyers and sellers seeking higher granularity or discreteness over the information or tangible goods they transact. Simply put, identification and authentication of specific information and value-added components is inherently important to further segmentation of units of payment (e.g., micropayments). Micropayments may be interpreted as a value-added component in facilitating transactions.

Pricing may also be bi-directional and asymmetric, and is preferably determined by the seller in order to define "profitability." Some sellers may choose to maintain fixed pricing for their goods or services, but may incorporate variable pricing in the value-added component. For instance, while the price of a given good or service may be fixed, the value-added component may be the terms of the pricing as it effects the buyer. The seller may also entice the buyer to provide demographic value-added components, or related data, which has intrinsic, sentimental value to the buyer. To the seller, the pattern, or structure, of demographic datum serves as a

valuable filter in which to position its offerings. Simply put, while barter is relatively inefficient, cash, being anonymous, may not reveal enough information to provide an incentive for the seller to vary credit terms or offer a greater variety of goods and services, even if there is a single underlying value-added information good (the seller can still offer perceptually similar but nonequivalent versions of the information without threatening secure, higher quality, limited, or more expensive versions).

The ability to offer both secure and unsecure, or legacy, versions of the same information based on a mutual disclosure and mutual understanding of both the buyer and the seller is particularly novel in the art. Moreover, privacy can be enhanced and new, unproven and yet unsecure information can be offered without jeopardizing the security of any pre-existing primary value-added information whether it be music, images, currency, electronic documents, chip designs, source code, legacy versions, prior art, etc.

The period of payment, like the discreteness of the actual payment, interest rate relating to a payment period, grace periods, early payment benefits, variable interest rate based on the seller's ability to assess the credit risk/worthiness of the buyer or its agent, etc. is an element or component (a value-added component) that may be changed to affect a transaction. Making these components more transparent to buyers improves the opportunity for enhancing and maintaining trust. It also enables buyers and sellers to make mutually beneficial decisions based on transparent, verifiable information or value-added components. Moreover, buyer-driven pricing, as with Dutch auctions, or market-based pricing, are not possible without compromising the access-based security in known systems. With the present invention, goods and services are better able to realize full market value because access to the good or service is not restricted (such as with new music or new endeavors by "unknown" or "unrecognized" artists, designers, creators or engineers). The market participants are better able to assess the good or service in question, and/or the related value-adding information/component, when experience and information sharing is encouraged. The prior art is restrictive by necessity in information sharing precisely because security cannot be maintained by prior art systems with such open access to information.

For goods or services that are difficult to value (e.g., media content, legal advice, design, non-commodity items, etc.) and decision-intensive, pricing becomes a barrier to entry in a marketplace that puts a premium on recognition. Highly recognized artists, lawyers, designers, retailers, etc. have a competitive advantage
5 over their unrecognized competitors. One approach to gaining recognition is freely distributing or providing goods or services. Ultimately, the seller still needs to profit from this initial positioning to the extent that financing of operations is available (the seller can stay in business as long as investors or financing is available to enable such operations). The same goods or services may be offered in a "tiered" manner,
10 which relates to the purchase price or to the quality of the underlying good or service to be exchanged. Examples of this include providing music in MP3 quality audio instead of CD quality; providing 10 hours of customer support instead of charging per hour; charging service charges instead of free checking or ATM access; charging a price per bit or bandwidth; etc.

15 Segmenting also plays a role in the "freshness" or "newness" of the information good or service. Live concerts or lectures may be worth more to the buyer than pre-recorded versions offered later or separately. The performer or creator of the information to be performed, or conveyed live, can only be at one place at a time, and may be a premium for that time. Live broadcasts may similarly
20 have a higher value. Physical advice may be worth more than printed literature to the buyer as well. These dynamics create an impetus for flexible and dynamic pricing that does not undercut the security of the overall "trusted transaction" methods and systems envisioned in the present invention.

In known systems, legacy information, relationships, etc. systemically
25 undermine the ability to ensure a "trusted system." The buyer and the seller in the art have no means for differentiating between the secure and insecure versions of a good, service, or value-adding component. The present invention provides such protocols by incorporating additional bits of data, which do not necessarily represent added data, but imperceptibly replace data with identifying or authenticating data,
30 enabling market participants to determine whether a value-added information "package" is secure. This also enables uniqueness of information packages to be consistently created and checked or maintained for later reference. The prior art

relies on the denial of access or access restriction, a clear disadvantage in increasing the availability of value-added information. With trusted transactions market participants are able to verify, identify, and price information and then decide which versions are appropriate for a given or existing demand.

5 Pricing may be better understood if the cost or time of computation is measured as a tangible asset. Similarly, the natural limit to theft of tangible assets has always been in the cost of the tangible assets. As information can increasingly be traded for value in excess of the cost of its storage or transmission, pricing becomes less tangible and more subjective. Delivery of information accurately and
10 quickly becomes a valued service. Measuring such value is based on the same principles that allow cost estimates of the delivery of fixed weight parcel packages. The existence of hackers indicates a lowered economic barrier to entry for informational crime, including identity theft and piracy. Dissemination of binary code, which is similarly detrimental, at little or no cost to the originator of the
15 valuable information, introduces novel concepts to the approaches of information pricing. Tangible goods become substitutes for cash payment.

An example of pricing based on effort is illustrated by a watchmaker who takes six months to finish a watch that he prices at \$70,000. This includes a "reasonable" profit and the cost of materials. The buyer is a watch fanatic and earns
20 \$140,000 a year. The exchange of a tangible good that has intrinsic value, which is converted into monetary terms for negotiation, as agreed by the parties in the exchange, becomes more prominent if information concerning value is transparent or fluid for all market participants. Transparency is inherently favored by markets seeking to appropriately price goods or services based on all available information at
25 the moment of pricing. Conversely, risk can be priced based on the financial context or structure of an organization. Those who earn \$20,000 should have to have confirmation by others with additional financial or fiduciary responsibilities before validating or approving transactions that exceed an individual's earnings for the period in question. At any time responsibility can be linked to authority, as a pricing
30 mechanism for decisions concerning similar amounts of monetary consideration. With pricing mechanisms and use rules, trusted transactions offer flexible pricing not possible with current systems.

Value-adding components, which may include pricing, is preferably viewed as a separate and distinct means for the buyer and the seller to separate information that may or may not be essential to any given transaction and may also be viewed as nonessential unless both parties can stipulate such information exchange. This is
5 invaluable as multiple channel distribution of the "same" goods (e.g., download music over the Internet versus purchasing a CD from a store) or services (obtaining a mortgage online versus processing physical loan documents) can be offered by the seller. Determinations of which channel, or channels, are profitable requires verification of unsecure and secure versions of these "same" goods.

10 Value-adding components may also include an offer, an acceptance, a bid, a purchase, and a sale of a securities instrument, including an option, a warrant, or equity.

Security is inherently intended for the party seeking value or authentication over the information or transaction and conversely protecting sentimental
15 information or identity from being stolen or defrauded. For the long term, buyers are able to differentiate that personal information value-added components are appropriate for dissemination to a seller to affect a transaction, or to get better terms. Either the buyer or the seller, or both, are better able to determine that transactions or relationships are favorable on a transaction to transaction basis, and thus
20 "transact" accordingly.

Pricing of the value-added information may include a value-adding component relating to the present value of recognition/non-cash equivalent cost/service that is handled in a separate negotiation or transaction, or a subsequent negotiation or transaction

25 The present invention may include limits of liability, or may consider the time value of money when determining a limit of liability threshold. The present invention may enable rules/access/authorization based on the result of that operation. In one embodiment, an actuarial estimate of liability (future time) or cost (present time) may serve as a rule for enabling another rule.

30 2. Reduction or optimization of transaction costs

In instances where the buyer and the seller, or their agents, seek to transact products or services that include value-added information, the seller generally seeks

to maximize profit, but may forego profit in the short term to ensure recognition or market share in the short term. The buyer seeks "satisfaction," which is dependent on one or more of the following product/service determinants: 1) price; 2) service; and 3) selection. These determinants may be quantitatively or qualitatively assessed
5 and may be based on available bandwidth, time of transaction, and transaction event conditions.

A priori, the buyer may not recognize the seller. In an information economy, such events are not a disincentive to pursuing a trusted transaction, but instead present market opportunities for valuing, authenticating, and verifying information
10 (all may be value-added components) concerning potential transactions are inefficient. Conversely, the seller may not have enough information about the buyer to determine what type of potential transaction can be enabled, based on the buyer's ability to purchase now, or at any point in the future. The seller may be inclined to make a sale with the buyer (or the buyer's agents) with or without confidence that
15 the initial transaction will lead to further transactions or trusted relationships that are profitable for the seller. The seller may use purchasing options (e.g., barter, cash or its equivalent, or credit) to enable a purchase by the buyer. According to one embodiment of the present invention, because value-adding information and its components may be bi-directional, both the buyer and the seller may chose to
20 negotiate the transaction, including variable terms for payment, as one form of value-added component or service and support for the information to be transacted.

Transactions, as defined by a purchase event (payment can be preliminarily assured), may happen before or after the buyer and the seller have "agreed" to transact. When the seller requires value-adding components/information about the
25 buyer before entering the transaction, the seller generally has higher risks than the buyer, which may affect its profitability. Where there is a high risk for piracy, such as the digital copy problem (that can render individual copies of value-added information worthless), the seller may not be able to establish trust with an unknown
30 buyer. The seller is not assured of any potential profitable transactions or long-term relationship with the buyer, which poses a significant risk to the seller if the buyer pirates information goods or services. A lack of dynamic authentication, even in

real time, at least initially, and adjusted as needs arise over time, and flexibility in negotiable terms, may cause the seller's assets to be economically undervalued.

Conversely, in those events where the buyer requires value-adding components/information about the seller in advance of entering a transaction, the
5 buyer generally has higher risks than the seller with regard to its ability to enter into transactions. "Identity theft" is an example of a risk that is higher for the buyer than the seller in these types of transactions. Additional transactions include on-line brokering, auctions, searches, bots, webcrawlers, recognition, and determination of goods or services absent proof of privacy guarantees. This applies to
10 noncommercial information as well (e.g. the FDIC logo, currency, driver's license, etc.)

The establishment of mutual trust may be asymmetric depending on the risk profile of the buyer and the seller. Risk/reward tradeoffs are implicit to some transactions, while the time required to establish a trusted transaction or eventual
15 profitable relationship may not be contiguous. In many on-line transactions, the per transaction risk is generally higher to the buyer, who may suffer fraud and may need to be more diligent about what value-adding information it chooses to exchange in the interests of enabling a trusted transaction. It is true, however, that in business to business transactions ("B2B"), or in financial information exchange, the relative
20 risks to each party are relatively equivalent, and requiring a more symmetric exchange of value-adding components relating to verification and purchasing power (in the form of barter, cash, cash equivalents or financing that would also constitute value-adding components) is not as necessary. Reducing the cost of creating and maintaining trust is an advantage of the present invention over known systems.

25 3. "Reintermediation": recognition as a Value-added Component

Asymmetry exists in recognition as well. Where word-of-mouth may constitute an acceptable means for creating recognition for a particular good or service, the buyer and the seller may wish to expand their respective abilities to capture more of the increasingly available goods and services, or value-adding
30 information (about themselves, or terms for a trusted transaction). With advertising and other forms of marketing, the push and pull of value-adding information between the buyer and the seller also contributes to potential purchase decisions by

both parties or their agents. The buyer may control certain criteria it seeks, such as price, selection, and/or service. The seller, conversely, seeks the highest profits from a given potential buyer or his agents, which may not be quantifiable from the first transaction or may not be the primary focus of the seller (such as seeking a valuable, marquis client). Both the buyer and seller may compare patterns or structure that, when recognized, help in forming opinions about the history, condition or context of the information.

In general, recognition serves to encourage more recognition. The seller will likely seek trusted transactions in the interests of profitably leveraging the time, cost and expense of generating the initial exchange of goods and services with the buyer. Over the longer term (defined as any additional transactions beyond the initial transaction), a profitable relationship is sought by the seller. The buyer and the seller may still maintain flexibility as expectations or needs concerning the relationship change. The present invention allows for such variability and flexibility by enabling real time adjustments to the terms that prevail between market participants. While terms and conditions are negotiable, security of the overall system is not jeopardized because secure and unsecure versions of the "same" value-added information and value-added components can be adjusted bi-directionally. In an information-based transaction, there is value in reintermediation by sellers seeking to ensure that their information is provably identifiable and verifiable.

The buyer and the seller may seek recognition or use means for increasing visibility of their respective interests. The buyer ultimately seeks to satisfy itself through a trusted transaction preserving private or financial information for select transactions requiring higher amounts of information exchange or verification (real time references, "membership reward programs" such as frequent flier airline points, or financing options that can be dynamically offered, are two incentives to the buyer and are likely to differentiate vendors, large and small, really or perceptually); the seller ultimately seeks to profit from the trusted transaction. Recognition of this potential exchange between the parties is not assumed to be high enough to enable a transaction, but high enough to create exposure for the buyer or the seller. Trust is assumed to not be pre-existing, or it may be variable between the buyer and/or the seller, requiring additional exchanges of value-adding information to enable a

trusted transaction. The seller, in the extreme, seeks the highest profit for each transaction. The buyer, in the extreme, seeks the highest satisfaction for each transaction. As discussed above, both goals are complementary and competitive, thereby increasing the need for dynamic exchange of value-adding information.

- 5 Recognition can enhance the potential for a successful trusted transactions and serves as a form of abstract experience for both parties to efficiently make decisions. With experience, value assessments become possible. Abstractions of value become experience as trusted transactions beget more trusted transactions.

4. Provable security and trust

- 10 Trusted transactions are characterized primarily by bridging the gap between "provable security" and the imprecise nature of trust. Encryption, cryptographic containers, digital watermarks and other forms of electronic data security can be mathematically demonstrated – discrete algorithms can be designed to meet certain pre-defined specifications or pre-defined expectations.

- 15 Encryption and secure digital watermarking (e.g., steganographic ciphering) offer tools for determining data integrity, authenticity and confidence. Transactions, however, still require human decision-making. Known systems describe a number of approaches for ensuring transactional security based solely on transmission security and fail to differentiate between what could be called "positional piracy" (e.g., the fraud or theft of universally recognized goods, products, and services) and
20 "sentimental piracy" (e.g., the fraud or theft of personal, private or financial information).

- For the purposes of this disclosure, the extreme case of sentimental piracy is identity theft. So long as information can be represented in binary digits (0s and 1s),
25 and can be easily copied, stored or transferred, identity fraud becomes an increasingly insidious problem. There is a temporal limit whereby the actual person is able to "reclaim" their identity at some point in time. The extreme case of positional piracy is zero returns on an intangible asset that has been pirated. As well, the present invention offers advantages over known systems for positional
30 piracy that enable the continuation of legacy business, customer relations and existing information formats, without sufficiently weakening any overall system security for trusted transactions. Simply, unlike known systems, access restriction is

not an adequate or appropriate means for ensuring the security of information data for a wide variety of applications.

To the extent that "security by obscurity" is typically representative of weak security to those skilled in the art of cryptography, more transparency for parties to a transaction over security protocols and information transfer are inherently necessary to ensure trusted transactions. Although information between parties may be asymmetrically exchanged (i.e., the value-added information or value-adding components is not equivalent in quality or quantity between parties, such as a difference in the amount of information exchanged, the identification of the parties, etc.), the level and degree of authenticity or verification only differs among the goods, products or services to be transacted, as well as the demands of the market participants. For the purposes of this disclosure, the value-added information is the fundamental good to be transacted between parties, while value-added components represent an atomic unit of data that is defined as the least amount of data that can either add functionality or be perceptibly recognized to a system for trusted transactions. Data may be represented in analog or binary terms in order to establish uniqueness and assist in identification and authentication. Value-added components may be added, subtracted, or changed to vary the underlying value-added information sought.

Because humans have difficulty remembering passwords, personal identification numbers (PINs), and the like, dependence on such data is increasingly problematic as more anonymous transactions are enabled between parties over electronic networks, such as the Internet, or between businesses in private networks. While passwords, or PINs, are commonly thought to be secure, the ability to check all combinations of numbers or crack passwords becomes less computationally expensive with increases in both processing speed and availability of bandwidth. Cost is reduced to the detriment of security if any individual has the means for high order computation or network-based bandwidth in discovering or hacking any given secret. Quantum computing speeds up the ability to test and discover such data at even greater speeds, and presents unique problems to security systems described in the art. Quantum computing also enables the definition or predetermination of the physical limitations of communicating or securing

information. Where difference between binary or digital signal processing and quantum mechanical limits is higher, better security is enabled.

Biometrics have been suggested to remedy this problem, but do not offer any way to create truly cryptographic secrets to be shared between parties. Iris scans, fingerprints, and the like, are easily stolen because they are easily perceptible to those seeking to defraud. Once stored electronically, biometrics be stolen for unauthorized use. Combining a biometric with a digital signature may provide a means to ensure that a given representation of a fingerprint or iris is fixed, temporally at the time the certificate is created, but does not prevent dedicated attacks at determining the fingerprint or iris to be used at some subsequent time. Real time authentication and verification are improvements envisioned with the present invention. Assuring that a particular fingerprint, signature or iris "data set" is that of the intended user, is fundamentally important to embodiments described herein. This becomes especially invaluable with increasing number of anonymous transactions. Although uniqueness may be enhanced with digital signatures and digital iris or fingerprint records, the advantage with the present invention is that more secure forms of uniqueness based on a predetermination of the discreteness of time and a predetermination of the limits of information conversion and transfer are absent in the art.

Moreover, real time authentication is not enhanced with systems described in the art, since such biometric data is easily stored or transferred, and thus suffers the same pitfalls for any binary data that is sought by a party seeking to defraud. Biometrics may be great for forensics (e.g., to determine after the fact who is responsible for a particular act), but they do not effectively address an inherent problem in enabling trusted transactions; that is, real time verification of parties or real time association of parties with information being transacted (in an auction, for instance). They are also not representative of a cryptographic key, which, as is well-known in the art, requires secrecy, randomness, and an ability to update or destroy the cryptographic key.

Another advantage of the present invention is the ability to serialize or individualize "personal secrets" that are shared between parties to boost confidence and transparency of transactions. That control, and the inherent uniqueness of

personal entropy, constructed from such information as a hometown, favorite restaurant, or high school sweetheart, is a means for perceptible representations of "secret data" that enhances the ease-of-use and application of appropriate shared secrets to be exchanged in conducting trusted transactions. Associating such secrets
5 with primary value-added information or value-added components being transacted is an additional novel feature of the present invention. Essentially, the present invention provides the ability to personalize or serialize, informationally, an actual "transaction event," including: the buyer; the seller; primary information; value-added components and tangible assets created, manufactured, or manipulated; and
10 any additional reference that can be made perceptible and secure to any observer. Bridging cryptographic with real world perception is a benefit over the prior art.

Essentially, randomness alone, whether pre-determined or not, is not sufficient for the creation of a "secret" that may be used with high levels of confidence repeatedly in assuring the validity of information or verify the identity of
15 a party. Encryption systems cipher the randomness according to available data capacity; digital watermarking ciphers the randomness according to perceptible features or characteristics of the carrier signal (a humanly-perceptible measure of data capacity, which distinguishes applications for encryption from secure watermarking). That such information can be made more computationally difficult
20 to discover, even by brute force attacks (since such experience is only limited by the experience of individuals) is of particular benefit to the art. The computational complexity added by use of a steganographic cipher is discussed in the U.S. Patent No. 5,613,004, the disclosure of which is incorporated by reference in its entirety, and offers a means for human observers to see the actual tampering of information
25 represented perceptibly. This proof is self-similar to that which is obvious in the real world, i.e., the ease at which one can observe that a watermark is missing from currency. Handling information as contemplated by the present invention for trusted transactions is unique in bridging computational benefits from both digital signal processing and cryptography to the benefits of all parties to a transaction. The
30 present invention is the enhancement of transactions through bi-directional verification of parties and verification of primary or secondary information exchanged.

An additional advantage of the present invention is the ability to continue to offer legacy business relationships, legacy products, legacy services and other means that will not reduce the overall security maintained by a system for trusted transactions. Known applications lack this feature, and instead rely on denial of access or authorized access to information. Information need not be restricted, and is preferably freely exchanged to widen the opportunities for transactions with a greater potential number of parties. The present invention is an improvement, in that the elements necessary for generating trusted transactions may be made more flexible, and those elements that are "secret," those elements that will be available at predetermined times, as well as those elements that are made more obscure to unintended parties, increase the overall computational difficulties in defeating a system for trusted transactions.

An additional consequence is improvements in enterprise resource planning and data mining. To the extent that transactions are made unique and may be atomized into data, functions, value-added components and any associated information, the cost of maintaining or referencing stored data, a goal in data mining technologies, can be made more efficient and effective in assisting with an optimized appropriation of resources, individual or corporate. Without such uniqueness, serialization, authentication, verification or identification, particular transaction events cannot be analyzed, manipulated or optimally used to create additional trusted transaction opportunities. Caching technologies are similarly affected by the present invention. The choice about what information should be maintained locally based on identification or authentication of that information available on a network, such as the World Wide Web, enables higher efficiency in sorting and referencing data for repeated use without increased demands on the network.

The ability to serialize individual transactions by particularizing trusted transaction elements between parties is handled more consistently than in known systems. Access is not denied, and rules for access are not pre-determined for goods or services that require exposure, testing or additional information for consummating a transaction. Ease-of-use, maintenance of more human-like and physical world expectations of trust are made more transparent. Identity and authentication risk is

reduced, and confidence is increased. Overall expectations are handled according to the needs of individual parties to any number of transactions. What results from trusted transactions is a more vibrant and competitive marketplace for information, value-added or not. Anonymity and legacy relationships may be maintained, unlike
5 requirements in known systems.

The application of steganographic ciphers enables an "optimized envelope" for securely inserting, detecting, and protecting informational signals, or data, or digital watermarks (predetermined messages) in a given digitized sample stream (e.g., a predetermined carrier signal, such as audio, video, image, multimedia, virtual
10 reality, etc.). As the perceptible qualities of the content stream have a basis as analog waveforms, steganographic ciphering increases the computational difficulty of crypto-analysis and makes unauthorized removal or tampering of the watermark a costly operation. With perceptible damage to a carrier signal a result of such tampering, tampering is more easily observable by parties, including those who are
15 involved in a particular transaction event. Moreover, such tampering enables higher transparency and verification of carrier signals of datum that are marked for secure exchange, even if over unsecure transmission channels. The prior art relies overly on secure transmission channels while ignoring the potential benefits of securing datum (with secure watermarking, scrambling, or chaffing, for instance) over any
20 available transmission channel. Such tampering is also transparent to vendors handling or accepting the information that enables less costly validation of claims made after some event must be confirmed and verified to the satisfaction of transacting parties. These unique features are an improvement over the art.

What differentiates the "digital marketplace" from the physical marketplace
25 is the absence of any scheme that establishes rights and responsibility, or trust, in the authenticity of digitized goods, services or value-added information. For physical products, corporations and governments watermark "goods" and monitor manufacturing capacity and sales to estimate loss from piracy. Reinforcement mechanisms, including legal, electronic, and informational campaigns also exist to
30 better educate consumers. Evidentiary levels of confidence must exist to support claims that are typically competitive between parties to a transaction.

Currently, security parameters may be coded into the actual physical transaction system or instrument. Similar to the security inherent in the randomness of the magnetic strip on most credit cards, these security parameters are designed to be tamper-resistant. Cracking such codes would not present insurmountable barriers to a dedicated effort at cracking a PIN. Access authorization is easily compromised by fraudulent reconstruction of an instrument, such as a credit card. Although storage of the security parameters in volatile, or nonpermanent, memory appears to offer advantages, including higher security required for many transactions, absent this higher level of security, real time authentication becomes a crucial benefit to parties in ensuring the validity of many forms of transactions. Insurance, identity, and purchases of expensive items or services are not generally confidently handled. Use of trusted transactions to process value-added information is unique and beneficial.

Several components may be used for separation of "trusted elements" for a given device or method for ensuring "trust" according to one embodiment of the present invention. First, a general purpose computing device is comprised of a CPU, a memory or storage, input and output devices, and a power supply. A device or card holder decides whether and when to use the device. For additional benefits described herein, personal information or privacy data may be controlled by the user in sample embodiments envisioned, unlike other pre-determinations of data in non-trusted transaction smart cards (e.g., a credit card).

A data owner, who may or may not be the device holder, is provided. Where the device holder and data owner are the same, as contemplated by some embodiments of the present invention, such data as digital certificates, time stamps, Unique IDs of data coming into and out of the device (personal or financial information being a large class of such data), etc. can be authenticated in a humanly-perceptible manner. This may be accomplished by a transducer, or a screen, that can transfer analog-based information of device holder, or be inputted and transmitted by the device holder for secure watermarking, or hashing of data to be exchanged.

A terminal, controlling input and output to and from the device (e.g., phone cards are controlled by the phone service provider's terminals, ATMs are controlled by financial institutions, set-top boxes controlled or owned by entertainment

distribution providers, etc. that may be made physically secure by separate means) or a system that may interact with a device, such as that contemplated in embodiments herein, to enable real time authentication or verification where such checks may fail from time-to-time with existing pre-defined trust arrangements or pre-determined protocols that require inefficient updating by one or both parties. In lieu of a physical visit to a vendor, the present invention anticipates more convenient anonymous updates, in those markets where it is possible to the benefit of both buyers and seller -- both parties have a market demand or need and are able to agree to such arrangements.

Embodiments of the present invention may include a simple Internet browser plug-in, with complementary system software for the provider of "information goods or services," that would identify, verify, authenticate, enable transfer, enable copying or other manipulations of the various primary value-added information and value-added components. Some of the functionality may strictly indicate what, if any, security exists within a particular primary value-added information set. This need not be settled within a system of trust, but be inherently imperceptible to any casual observer or market participant interested in the information or the transaction events that can be observed. Essentially, encouragement of provable differentiation between different classes of primary value-added information (secure, insecure, legacy, etc.), value-added components (not the primary information but value-adding to the transaction event, and any information concerning market participants (private, history, condition, or financial) is enabled, using simple steganographic ciphers with mapping and transfer functions without compromising the underlying security.

A device issuer controls the operation of the device according to mutually agreed to terms between parties. The device issuer may limit the use or functionality of the device.

For the device hardware manufacturer, fraud may be attempted by the various parties, subcontractors, etc, who are involved in the manufacture of the devices. The device issuer requires protocols that cannot be defeated by typical "rogue engineer" attacks, where security is dependent on an understanding of the methodologies, device, or system design. In fact, the ability to transparently and

provably manufacture secure smart devices may be accomplished with such protocols as digital time stamping (using successive temporally related hashes that seed other hashes to create a universally acceptable means for establishing the time of manufacturer, with time being the universal constant), or digital watermarking (where instead of time, other predetermined data is concatenated with data for provably establishing ownership, over the device). Tampering must be provably perceptibly evident upon tamper detection of the device (as with device used for limiting theft of clothing or physical items in retail stores). Prevention of the rogue engineer problem is not anticipated by known systems.

10 A software manufacturer usually requires clear specifications or transparency such as open source code, providing the underlying ciphering algorithms and other specifications for analysis. Similar trust issues as with device hardware manufacturing exist. Stega-ciphering the operating system, the simple system or engine for determining authenticity and identification of available data, to prevent memory capture, cloning, write once memory specific to the device holder provide additional benefits of security. A discussion of such is provided in U.S. Patent No. 5,745,569, the disclosure of which is incorporated by reference in its entirety. As well, using transfer functions with associated predetermined keys is also a means for accomplishing confidence and authenticity in transaction. This is described in U.S. Patent Application Serial No. 09/046,627, entitled "Method for Combining Transfer Functions with Predetermined Key Creation," the disclosure of which is incorporated by reference in its entirety.

25 In general, security requires: fewer splits of trust (poor tying arrangements that may encourage fraud or piracy), better transparency of data (it should be perceptibly apparent, or mathematically, or actuarially possible to observe risks and quantify them to enable security design with a clear understanding of potential threats for each system, method or device), and use of cryptographically strong protocols, where security is both provable and perceptible such that market-driven features are both fundamental at the earliest development and design of appropriate systems and devices, in order to build confidence and trust that is acceptable and transparent to all parties to a transaction.

Application of a steganographic cipher to the operating system or operation of the contemplated systems and devices ensures further security from tampering. Such methods are disclosed in U.S. Patent No. 5,745,569, and offer additional benefits when coupled with the embodiments disclosed herein. System or device operations may be controlled with minimum functionality, objects or executable code. As value-added information is checked for authenticity, decoding any embedded operation objects or code, executing the operation of the system, and deleting the object or code from memory, or randomizing it in memory to avoid capture, would greatly increase the security of both value-added information and the systems or devices intended for manipulation of the value-added information. Alternatively, certain base functions, such as play, record, copy, manipulate, and transfer data, may be problematic. These functions may be atomized into objects that must be first authenticated by the trusted transaction device before they are operable for the given format, or before they provide additional information.

Time of use has traditionally been a typical constraint for securing smart cards and similar devices, but may become ineffective and inconvenient to users. Enabling a smart card to capture or transduce information (even converting analog information or input into secure digitally-sampled representations of the analog information for analysis and authorization, as with a stega-ciphered digital watermark) about the time, location, identity or any number of specific datum greatly enhances smart card and similar device security, trust and confidence. Such benefits over known systems are valuable contemplated with the present invention.

Valuations of trust also enables the described sample embodiment of a trusted transaction system or device to compare private information with financial information, essentially bridging determinations of risk in financial transactions and insurability. Private, or sentimental, information disclosure is more highly sought in determining insurance risk. The ability to pay, and other financial information, are being commoditized. Insofar as the described method and device for such deployment of trusted transaction technology can be assessed for different products and markets, the example of an insurance device could easily be called a trusted transaction privacy/financial information device or card. Users can control what information they disclose given the risk coverage or credit they seek, and providers

being able to decide, with more current and transparent information disclosure possible, what to underwrite or what to finance.

For the authentication or identification device, there is a risk of identity theft to both buyers and sellers, or information that is limited by law. Examples include Medicare-covered drugs, local legal constraints, etc. Risk may be predetermined or limited by a government agency (FDIC, FBI, Social Security, IRS, DMV, Federal Reserve, etc.), a similarly outfitted organization (trust is held in perceived and observable representations of the organization, food stamps, stamps), or an equivalent transaction event enabler (traveler's check provider, medication, etc.). In these cases, systemic risk is limited by enforcement agencies held in trust by a government or body politic. The restrictions are predetermined and dependent on successful authentication or identification of a product, label, or other similar item. Laws may differ between localities and may be dependent on some form of identification, proof of age, or proof of residency. To properly serve local residents becomes a data security issue. This embodiment offers advantages over the art in its flexibility and real time, perceptible authentication properties.

Both the provider and the agency involved may have higher levels of risk, because the nature of the information is characterized by high value, general or universal recognizability, and a genuine threat of fraud. Most people casually accept that \$10 and \$20 bills are real even if they prove not to be later. Governments try to limit such liability without damaging the overall trust in the currency. As abstractions of value are exchanged, a smart identifying device, instead of value replacement device (predetermined, fixed spending or authorization in a device), is necessary to capture "personal entropy," or information about oneself that can be more closely guarded and less open to theft versus a password or pass phrase. Secrets must differ from identification. The larger body of data to search to discover these secrets act as a higher form of secrecy. These datum may be converted to readable text in some embodiments or maintained in digitally-sampled but humanly perceptible form in other embodiments (favorite restaurant is represented as an actual image of the restaurant, mother's maiden name is actually the voice of an individual's maternal grandparents, highly specialized forms of personal information

that may be dynamically changed or checked quickly and conveniently without undue risk exposure to the system).

For governments and individuals, piracy of identity is the most insidious risk exposure. Identity theft may be curtailed with devices that can transduce, in real time, an iris scan, fingerprint or other biometric and compare securely transmitted results with a secured stored record at the time of initialization. Alternatively, this may be accomplished with an unrelated Unique ID that confirms the identity of the user, and may be created and stored on the device. Because governments are arbiters of trust in markets (their actions in the collective affect trust and confidence in products and markets), these devices are able to alert consumers to potential risk for a given product or service (represented by some ruling or law that is important to convey to the consumer, such as with alcohol, medications, or tobacco). These devices could, at the discretion of the user, indicate related warnings for which the government has an interest in safety. In one embodiment, by checking an actual cigarette carton, or drug packaging, with the enabled device, counterfeit packaging may also be detected. In one embodiment of the present invention, bar code scanners may be "required" to also check for embedded or associated signals indicating authenticity. The devices may also check if supposedly "real" prescription drugs are authentic. Such a check may occur when using the device to communicate with a vendor and check to see if any complaints or problems exist in stored records; again the packaging may be checked for authenticity in cases where counterfeits are high and difficult to check without some form of secure watermarking or perception-based authentication that can be efficiently handled by an enabled device.

According to one embodiment of the present invention, digital content may be distributed through a local content sever, or LCS. In general, the LCS environment is a logical area inside which a set of rules governing content use may be strictly enforced. The exact rules may vary between implementations, but in general, unrestricted access to the content inside the LCS environment is disallowed. The LCS environment has a set of paths, or paths that allow content to enter the domain under different circumstances. The LCS environment also has paths that allow the content to exit the domain.

The act of entering the LCS environment may include a verification of the content (an authentication check). Depending upon the source of the content, such verification may be easy or hard. Invalidatable content may be subjected to a quality degradation. This degradation may be to the content itself, or it may be removal of value-added components. Content that can be validated, but that belongs to a different LCS environment may be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between environments.

When content leaves the LCS environment, it may be watermarked as belonging to that environment. It is allowed to leave the LCS environment at the quality level at which it was stored (i.e., the quality level determined by the path). The watermark on the exiting content may be both an embedded digital watermark and an attached hash or digital signature (it may also include a secure time stamp). Content cannot return into the environment unless both the watermark and hash can be verified as belonging to this environment. The presence of one or the other is generally sufficient to allow re-entry.

This system may allow a certifiable level of security for high-quality content, and may allow the use of unsecure content at a degraded quality level. The security measures are such that a removal of the watermark constitutes only a partial failure of the system. The "wiped" content may be allowed back into the LCS environment, 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 U.S. Patent No. 5,613,004; U.S. Patent No. 5,687,236; U.S. Patent No. 5,745,569; U.S. Patent No. 5,822,432; U.S. Patent No. 5,889,868; U.S. Patent No. 5,905,800, U.S. Patent No. 6,078,664, U.S. Patent Application No. 09/046,627 U.S. Patent Application No. 09/053,628, and U.S. Patent Application No. 09/594,719

Provable security protocols may minimize this risk. Thus, the embedding system that embeds 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 and commercial interests in the content than to consumers). Ideally, as previously disclosed, security preferably does not obscure the content, nor prevent market participants from accessing information contained therein, and for the longer term, developing trust or creating relationships.

5 The system can flexibly support "robust" watermarks as a method for screening content to speed processing. Final validation, however, is relied upon the fragile, secure watermark and its hash or digital signature (a secure time stamp may also be incorporated).

10 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 is preferably stored as ciphertext (encrypted or scrambled), not plain text, to prevent system-level extraction of the content. This is in contrast to known systems, which affix or otherwise attach meta-

15 The LCS may be able to receive content from a secure electronic content distributor, or SECD, and may be able to authenticate content received via any of the plurality of implemented paths. The LCS may monitor and enforce any rules that accompany received content, such as number of available copies. Finally, unless being transmitted to a satellite unit, the LCS may watermark all exported material
20 and supply a hash made from the Unique ID and the content characteristics (so as to be maintained perceptually within the information and increase the level of security of the watermark).

25 The satellite unit enables the content to be usable apart from the LCS. The satellite unit is partially within the LCS environment. A protocol may exist for the satellite unit and LCS to authenticate any path made between them. This path may have various levels of confidence set by the level of security between the satellite unit and LCS, and determinable by a certification authority or its equivalent, such as an authorized site for the content. The transfer of content from the satellite unit to the LCS without watermarking may be allowed. However, all content leaving the
30 satellite unit is preferably watermarked. The satellite unit watermark may contain a hash generated from the satellite unit Unique ID and the content characteristics. If the content came from a LCS, the satellite unit may also add the hash received from

the LCS to the watermark. The LCS and satellite unit watermarking procedures do not need to be the same. However, the LCS is preferably able to read the satellite unit watermarks for all different types of satellite units with which it can connect. The satellite unit does not need to be able to read any LCS watermarks. Each LCS and satellite unit preferably has a separate Unique ID.

Referring to Fig. 2, a schematic of a local content server environment according to one embodiment of the present invention is provided. LCS 202 may be a software device running on a general purpose computing device, such as a personal computer (including, in general, a central processing unit, an input, an output, a memory, and a power supply). LCS 202 may include local content server domain 204, rewritable media 206 (such as a hard disk drive, a CD-R/W, etc), and read-only media 208 (such as a CD-ROM). LCS 202 may communicate with at least one satellite unit 210 via an interface.

In one embodiment, LCS 202 may have a Unique ID. Similarly, in one embodiment, satellite unit 210 may have a Unique ID.

LCS 202 may communicate with SECD 212 via a network, including a local area network, a wide area network, an intranet, and the internet. This communication may also be established by a telephone link, a cable connection, a satellite connection, a wireless connection, etc.

In one embodiment, a single LCS 202 may interface with more than one SECD 212.

A plurality of paths 220, 222, 224, 226, 228, 230, 232, and 234 may exist among LCS 202, SECD 212, Satellite unit 210, LCS domain 204, rewritable media 206, and read-only media 208. Each will be discussed in greater detail, below.

Digital content may be securely distributed to LCS 202 from SECD via path 220. The content may be secured during the transmission using one or more security protocols (e.g., encryption or scrambling of the content). In one embodiment, if LCS 202 interfaces with multiple SECDs 212, each path may use a different security protocol.

The security protocol may use an asymmetric cryptographic system. An example of such a system includes a public key cryptography system. The private and public key pairs allow LCS 202 to authenticate and accept the received content.

Referring to Fig. 3, a flowchart depicting an example of an authentication by LCS 202 is provided. In step 302, the user connects to the SECD, makes a selection, and completes a sale.

In step 304, the LCS provides its public key to the SECD.

5 In step 306, the SECD uses the LCS public key to initiate transmission security.

In step 308, the SECD transmits the secured digital content to the LCS.

In step 310, the LCS receives the digital content, authenticates that the digital content was unchanged during transmission, and unpacks it from its security wrapper (that may include a secured transmission line, such as SSL). In one embodiment, the digital content may be authenticated by a watermark and hash check. If the content can be authenticated, the content is accepted into the LCS domain. If the content cannot be authenticated, it is rejected.

15 Referring again to Fig. 2, path 222 connects LCS domain 204 with rewritable media 206. Referring to Fig. 4, a flowchart depicting the process for content entering LCS domain 204 from rewritable media 206 is provided. In step 402, the content is provided. In step 404, the content is checked for the presence of a watermark, such as a watermark for the particular LCS. If there is not a watermark, in step 406, the content is degraded to Low Quality and, in step 408, the content is stored in the LCS domain.

20 If, in step 404, a watermark is present, in step 410, the watermark is checked to determine if it matches the LCS. This may be achieved by a hash. If the watermark is verified, in step 408, the content is stored in the LCS. If the hash does not match, the content is rejected.

25 Referring again to Fig. 2, LCS domain 204 may export content to any receiver (other than satellite unit 210) through path 224. This may include copying content to a rewritable media, creating a read-only media, rendering the content for use (e.g., playing, viewing, etc), etc.

30 Referring to Fig. 5, a flowchart depicting the process for content leaving LCS domain 204 is provided. In step 502, the content is retrieved from storage within the LCS. In step 504, the content is embedded with a watermark. In one embodiment, the watermark may be unique to the particular LCS, as determined by

the LCS Unique ID. The watermark may contain a hash that is created from the combination of the content characteristics (such as signal features, etc.) and the Unique ID. The watermark may optionally contain other data, such as a timestamp, a number of allowable copies, etc. This would be described as parameters of use, usage data, etc. which could be referenced when content is exported. If the export is to a storage medium, the LCS optionally can add a second hash to the file, external to the content, which can be used for further authentication. For security purposes, in one embodiment, the external hash may be created in a different manner from the embedded, watermark hash.

10 In step 506, the content is output from the LCS to the receiver.

Referring again to Fig. 2, path 226 connects LCS domain 204 with read-only media 208. Referring to Fig. 6, a flowchart depicting the process for content entering LCS domain 204 from read-only media 208 is provided. In step 602, the content is provided. In step 604, the content is checked for the presence of a watermark, such as a watermark for the particular LCS. If there is no watermark, a check is made in step 610 to see if the originality of the content can be determined. An example of such includes a media-based identifier that identifies the content as original.

20 If the content can be verified as an original, in step 608, it is stored as High Quality in the LCS domain. If the originality cannot be verified, in step 610, the quality is degraded to Standard Quality, and, in step 608, the content is stored in the LCS domain.

If a watermark is identified in step 604, in step 612, the hash is checked to verify that the content matches this LCS. If it matches, in step 608, the content is stored in LCS domain at High Quality. If it does not match, in step 614, the content is rejected.

Referring again to Fig. 2, path 228 connects LCS 202 with satellite unit 210. Referring to Fig. 7, a flowchart depicting the process for content entering LCS 202 from satellite unit 210 is provided. In step 702, the content may be watermarked before it is transmitted to the LCS. In step 704, the content is transmitted to the LCS.

In step 706, the content is checked by the LCS. This may include checking the LCS hash. If the hash matches, in step 708, the content is stored in the LCS domain as High Quality. If there is no hash, in step 710, the content is degraded to Low Quality, and in step 708, the content is stored in the LCS domain. If the hash
5 does not match, in step 712, the content is rejected.

Referring again to Fig. 2, path 230 connects LCS 202 with satellite unit 210. Referring to Fig. 8, a flowchart depicting the process for exporting data from the LCS 202 to satellite unit 210 is provided. In step 802, the content is retrieved from storage within the LCS. In step 804, the security of the path between the LCS and
10 the satellite unit is verified. Once the security is verified, in step 806, the content is exported to the satellite unit without a watermark.

If the security of the path cannot be verified, the export process mirrors that of an export to a receiver, depicted in Fig. 5.

Referring again to Fig. 2, path 232 is a path for content to be stored in
15 satellite unit 210. In one embodiment, all content may be allowed to be imported into satellite unit 210, but may be automatically degraded to Low Quality when it is stored.

Path 234 is an export path for content rendered by satellite unit 210. In one
20 embodiment, this content may be marked with a satellite unit watermark that contains a hash from the satellite unit Unique ID and any hash that is associated with the content from an LCS .

It should be noted that a hash function may be converted into a digital
25 signature by performing a hash and encrypting the result of the hash. The uniqueness of the hash can vary with the hash function, while the digital signature adds a layer of confidence to the integrity of the data.

Other types of encryption, including transfer functions, may also be used.

Referring to Fig. 9, a flowchart of a method for trusted transactions
30 according to one embodiment of the present invention is provided. In step 902, value-added information, or its tangible equivalent, is provided. This may be provided by a user that wishes to verify the value-added information.

In step 904, the perceptible data for verification may be maintained by a vendor or provider, and may be updated by a public-key secure digital watermark in

the observable packaging (if applicable). In those cases where security must be high, real time, or simply faster, key generation or signature generation functions may be enabled with embodiments of the present invention.

In step 906, the user provides a public key based on the identify held in the device to enable an authentication check.

In step 908, a response may be sent to the user.

Steps 906 and 908 may be repeated with further prompting for higher levels of authentication, or for additional checks. If the remote location provides the confirmation, or if a certification authority is involved, the response may be sent via secure transmission lines (e.g., encrypted transmission that can only be decrypted with the user's device and access to the user's stored private key). Alternatively, information may not need to be sent in a secure manner and may be checked upon delivery to the device to limit any remote communications breaches by unintended third parties.

Referring to Fig. 10, a device for trusted transactions according to one embodiment of the present invention is provided. Device 1000 may include steganographic cipher 1002. Steganographic cipher 1002 may be governed by at least the following elements: (1) a predetermined message; (2) a predetermined key/key pair; and (3) a predetermined carrier signal (image data, so images will be the primary data represented and ciphered).

Transducer 1004 may be provided. Transducer 1004 may include a charged coupled device (CCD), a personal entropy capture device (e.g., a retinal scanner, a thumbprint scanner, etc.), a touch pad (e.g., a pad for receiving a signature), an image capture device, a bar code reader, a magnetic card reader, etc. Transducer 904 receives the data in a physical format and converts it to an analog or digital format.

In one embodiment, the data from transducer 1004 may be marked with a timestamp for time-critical input.

Analog/digital converter 1006 may be provided. A/D converter 1004 may be used to convert analog information from transducer 1004 into predetermined digital format. In one embodiment, signatures may be converted in one format, images that

are captured in another format, and fingerprint/iris scans may be converted in another format.

A memory may be provided. The memory may include both volatile memory, and re-writable memory, such as DataSlim™.

5 A volatile device may be provided, such as a one time pad (private key of card holder/user), a one time memory or floating in the volatile memory to evade capture (stega-cipher computer code). This may be provided in a tamperproof casing.

10 Device 1000 may also include output 1020. Output 1020 may be any suitable output, including a connection port, a wireless port, a radio transmitter, etc. Before information is output from device 1000, it may be encrypted. In one embodiment, the information may be digitally watermarked. In another embodiment, the information may be digitally signed. In another embodiment, the information is not encrypted, and instead is transmitted over a secure transmission
15 channel. Number generator 1008 may be provided. Number generator may be a random number generator, or it may be a pseudo-random number generator.

In addition, the device may include a controller, a power source, and an input and an output.

20 Information may be converted into a humanly perceptible form (chemical/electrical/magnetic such as a humanly visible chemical test result, as with a pregnancy tests, an EKG, an MRI or CatScan image, are all converted into "humanly perceptible form for "human" analysis) prior to authorization of a transaction/decision event.

EXAMPLES

25 In order to better understand the present invention, several examples are provided. These example do not limit the present invention in any way, and are intended to illustrate embodiments of the present invention.

1. Smart Telecommunications

30 At present, large volumes of commerce and commerce-related activities are performed using telephone connections. Authentication of identity is an ongoing concern in such transactions. Present technology allows the verification of the

origin of a landline phone call (POT), but offers no assurances as to the identity of the user. Furthermore, simple identification of the origin of the call is only useful insofar as that phone number can be used to index a database of callers. The present invention allows for bi-directional verification of identity during a phone call, with the option of partial or full concealment of identity.

A consumer may wish to make a purchase on the phone. Presently, the consumer's identity is established by the seller using personal information from the consumer, such as a credit card number, an address, a phone number, etc. However, all of this information may be known by an imposter. A smart phone transmits identity information (perhaps embedded as a watermark in the audio connection), in response to a query from the seller. The receiver verifies the buyer's identity with a certification authority. Furthermore, the consumer may also verify the authenticity of the seller's identity at the same time, by the same method. The consumer may choose not to respond to certain queries in real time.

The smart phone may require a level of identity disclosure before it accepts an incoming call. For instance, telemarketers may be required to reveal the name of their company before the call is accepted by the smart phone. Consumers may protect themselves from fraudulent sellers by requiring such identification. Further, legitimate sellers may be assured that their customers know that they are legitimate. The certification authority assures the consumer and seller that they are receiving authentic identifications.

2. Equity Programs As A Value-added Component

Another embodiment of the present invention relates to methods and means of payment includes a novel means for encouraging alignment of buyer and seller interests. Similar to cooperatives, membership programs (in proprietary form, co-branded with a financial institution, or implemented as a specialty device that can handle these equity transactions) may be enhanced to offer buyers the opportunity to purchase options in equity of the seller's company or related institution. Instead of being given cash or points, at some fixed point in time, consumers and sellers may be provided with the opportunity to purchase equity as available on some public or private market or exchange.

These options may be built into the functionality of the actual transaction device and may be coupled with both trusted transactions or general transaction systems. Settlement of the option may be based on any known option pricing mechanism (such as the well-known Black-Scholes model) and predetermination of terms for settlement and conversion of the option. This approach incentivizes and encourages clearer alignment of all market participants in the value and condition of the equity of the entity with which transactions are being handled or negotiated. Independent certification authorities, or intermediaries that are able to ensure or verify a transaction or related information, may be used to ensure that such equity programs can be trusted. Any relevant disclosures concerning legal or financial restrictions are simply additional value-added components for consideration.

3. More security - body movements for entropy and pharmaceutical use control

A related embodiment according to another embodiment of the present invention includes an interface for detection of body movements (eye movements, blinks, voice pass phrases, etc.). These movements may include predetermined sequences of movements that may be ciphered in a manner similar to encrypting ASCII pass phrases. This is a novel implementation of human movement in generating symmetric or asymmetric cryptographic keys. The transducer may include any number of means of capturing human-based body movements in real time for instantaneous verification of an authorized user. Moreover, unlike simple biometrics, a series of body movements (similar to the act of signing in writing, but likely to be more difficult to capture for unauthorized misuse -- a signature, like a fingerprint, is able to be observed and copied without permission or knowledge of the signature author) is difficult to copy.

The movements or similar biological entropy (transduced from biomedical, bioengineered, biochemical or biophysical information that may be made perceptible and encrypted or securely watermarked for later comparison or real time verification) may be captured by a transducer of analog signals and converted into digital binary information used for comparison with any number of stored corresponding instructions or messages to be decrypted. These signals may be multidimensional (2D, 3D, 4D- with a time component, etc.) to increase the information space and make discovery of hidden secrets more computationally

difficult. Images, medical or human-condition based, audio signals, video, virtual reality, multimedia, etc. all provide rich media information in which to enhance the security of any embodiment contemplated by the present invention. Combinations of multidimensional media for varying ciphering options as well as steganographic embedding are also contemplated as a means for furthering ensuring computational 5 complexity to any unauthorized user. Steganographic-mapping (watermarking) or transfer functions (scrambling or "chaffing") may be combined with encryption ciphers as a means for making each unique implementation or tangible device – serialization or personalization of a method for engaging in trusted transactions, high 10 risk, information-intensive or sensitive decision (military use, security use, restricted government use, privacy use, or any number similar commercial or noncommercial decision or transaction events).

Additional embodiments include actual control over the use or access to pharmaceuticals based on medical risk, condition or personalized advice to the user. 15 Tangible methods for transfer of chemical, biological or physical agents intended for medical use or individualized control based on third party conditions (legal, medical, governmental, etc.) are governed by manipulation of the apparatus, device or system used to introduce foreign agents (informational, intangible or tangible) into patients (the intended, authorized or verified user).

20 Highly secure and artificial environments, such as aircraft flying simulations or visual financial trading information, may be representative of more risk to owners of actual tangible planes or tangible assets related to any financial information. Recognition of a digitized iris does not enable movement based confirmation of future secrets (the movements) that may be changed, destroyed or updated to ensure 25 consistent or higher degrees of security maintenance. For some body movements, it may be possible to maintain better security than with written information. In other words, certain body movements may be prevented, or made difficult to perform even under rigorous demand by unauthorized agents. Blinking or other facial movements may be made impossible to verify the real time identity of the user. This adds a 30 layer of security and increases the difficulty of defeating a cipher or a series of related ciphers (encryption-based or steganographically-based, where the digitized signal has humanly-perceptible fidelity or characteristics) depending on access or

sensitivity of information. It also maybe psychologically or human-rule driven. Certain humanly observable body movements, or detectable "telemetry-type" data (brain activity, heart beat, pulse, or any other medically observable information) may be either unique to an individual or simply general to certain behavior. This data may be important to use as a means of preventing poor decision-making, or requiring higher diligence before transacting or executing a given operation. At the least, the movements are a means for predetermining and assisting the generation of a binary key or seeding the generation of a cryptographic key, message or signature.

Any particular instance may be successively stored in subsets of any primary value information or value-added components (single key or key pair associated with a single message or signature to further serialize data that may have steganographic capacity for imperceptible embedding in the carrier signal, primary or value-added components data). The operation may be highly demanding, or may require human-based or driven or initiated decisions. The instructor, or the user, may have predetermined the conditions that indicate confidence or lack thereof at the time of the verification or authentication of the user. This may be for security reasons, or simply risk management, as information is increasingly processed at higher speeds and may require greater care in ensuring information data integrity. As well, humanly-observable (and convertible into binary data for deciphering) movements enable a form of bridging analog, human trust with digital or mathematically provable, actuarially, statistically, deterministically known or predictable measures of risk and trust. This novel feature is an additional benefit over the prior art and ensures future human-like characteristics in "digital" (underlying, "measurable" or "estimable" data integrity, authentication and confidence), electronic (analog transducers and transmitters), or binary transaction systems. Further security or serialization of transaction event information (human movement or observable condition used for secret key or equivalent generation) enable additional forms of trusted transactions.

Additional security may be assured with temporal-based limits on human body movement or biologically observable human condition (by use of a medical or human directed transducer). Interlocking keys and messages with blind signatures, or onion routing transmission techniques to obscure the identity of the user, are

further enhancements that may guarantee a high level of privacy to the user of the system or device. Information formats may be encrypted or have stored primary or value-added component information that has to arrive to the user without any digitally evident tampering for the user to make the best possible decision regarding the observed information.

Unlike the prior art, embodiments of the present invention consider the perceptibility of information to bridge human trust and confidence with cryptographic or "mathematical" measures or estimates of "security," "data integrity" or "trust." This is novel to the art of data security and secured transaction or transmission technologies.

4. Algorithmic Information Theory (AIT) for additional security

By implementing predetermined indications of mathematically provable randomness, the ability to discover secrets and human choice, based on unprovability or incompleteness, as discussed and is well-known in the art as originating with Godel (incompleteness theorem) and Turing (halting problem, uncomputability). Chaitin "discovered" randomness, stating essentially that randomness can be described mathematically, and thus differentiations between discrete and infinite randomness are logically observable. Because truth is relative in a quantum mechanical sense, degrees of credibility concern the level of trust that may be offered in any trusted transaction system. While the primary value that concerns us is information, the ability to describe programming size complexity (that is optimized functional data) enables self-limiting software to be programmed. To the extent that trusted transactions can never be physically perfect operations, uniqueness of information, as both data and code, is particularly important to providing higher security when computational cost and bandwidth is extraordinarily cheap.

Essentially, choice over answers to questions that cannot be characterized as "True" or "False," such as "This statement is false," have inherent randomness and are thus ripe for paradoxical response. More intricate paradoxes, Berry's Paradox, Turing's halting problem, as well as Chaitin's definition of "randomness," are sure to enable predictable infinite and finite (discrete) randomness with which to seed and cryptographic secret or generation of a symmetric, asymmetric key or digital

signature. Human perception as a means for enabling analog trust may be made inherently more secure by choosing responses to paradoxes that have no computable value. That Chaitin can describe "randomness" with logically structured instructions for the halting problem, in LISP or C programming languages, including the computer programming language of Mathematica, enabled the development of a randomness constant.

The equations of randomness may be implemented in software and offer a unique and novel means for further securing the generation of cryptographic or steganographic seeds, secrets, keys or messages. Of course, differences between any of these information elements as to the means for securing or authenticating data would enable flexible architectures combining various ciphers and methods for arriving at a rule for validation, authenticity, data integrity, confidence or enabling any subsequent manipulation of the associated data (primary value-added or value-added components).

5. Entertainment media exchange

According to one embodiment of the present invention, the device may be used for the exchange of entertainment media. This may include audio, video, multimedia, etc. In such an exchange, the perceived risk of value-added information piracy is relatively high for the seller or provider, while the perceived risk is relatively low for the purchaser. The obvious risk is that all potential "consumers" of the media access and copy the entertainment media for free. For music or video, or similar entertainment good, according the present invention provides the following structure may be used.

a) Fragile watermark structure

The fragile watermark, according to one embodiment of the present invention, can actually hold an entire value-added component, encoded in the least significant bit (LSB) of each 16-bit sample. This gives a data rate of 88200 bits per second in a stereo CD file, or a capacity of 1.89 M in a 3 minute song. This is an immense capacity relative to the expected size of the value-added component (100 - 200 K).

The fragile watermark is preferably bound to a specific copy (Unique ID) of a specific song (Unique ID), so that it cannot be transferred to other songs. This binding can be achieved through use of a hash in the following sequence:

- 5 (1) A block of value-added component is encoded into a block of samples.
- (2) A hash of the value-added component block and a random number seeded by the owner's identity (Device or system Unique ID) is generated and encoded into the subsequent block of samples.
- 10 (3) A hash of the first two blocks of samples and a random number seeded by the owner's identity is generated and encoded into a third block of samples.
- (4) Repeat steps 1-3 as necessary.

15 Each value-added component block may 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
20 BlockLength
    char  IdentityHash[hashSize];
    char  InsertionHash[hashSize];
}

```

25 An application can read the block identifier and determine if it recognizes the block type. If it does not recognize the block type, it can use the BlockLength to skip this block.

Certain Block Types are required to be present if the value-added component is to be accepted. These may include an identity block and a value-added component Hash block. The Block Data may or may not be encrypted, depending on whether the data is transfer-restricted (value-adding) or simply informative. For instance, user-added value-added component data would not need to be encrypted. The BlockIdentifier would indicate whether the block data was encrypted or not.

b) Robust open watermark

This is the mark that may indicate non-legacy content. In one embodiment, there may be two possible settings. "1" indicates non-legacy content that must be accompanied by a authenticable value-added component for entry into the domain
5 (e.g., EMD or Electronic Media Distribution media content). "0", on the other hand, indicates non-legacy media that was distributed in a pre-packaged form (e.g., CDs, DVDs, game software, etc.). "0" content may or may not have a value-added component. "0" content may only be admitted from a read-only medium in its original file format (e.g., a "0" CD may only be admitted if it is present on a Red
10 Book CD Specification medium).

c) Robust forensic watermark

This watermark may not be accessible to the consumer in any way. It may be secured by a symmetric key held only by the seller (or an asymmetric key pair that may be desired for some embodiments). A transaction ID may be embedded at
15 the time of purchase with a hash matching the symmetric key (or key pair). The watermark may then be embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of this watermark is not limited by real-time/low cost constraints. The recovery will only be attempted on pirated material. A recovery time of 2 hours on a 400 MHz PC is
20 reasonable.

6. Additional parameters for value-adding components

Physical shipment of packaged goods or services (value-added information) is anticipated as being a potential option to consumers or purchasers as well as sellers and providers. That the value-adding information may be packaged or
25 represented tangibly does not obviate the need for trusted transactions to ensure payment and the appropriate division of rights and responsibilities for various goods (a DVD for music or video), services (smart credit card or insurance card) or markets (trusted telephone system, government identification schemes). This type of transaction represents additional benefits over embodiments in the existing art --
30 on-demand trusted transactions and physical manufacture/delivery of goods is enabled, without risk to the overall system and its value-added information security. This amounts essentially to serializing or personalizing, depending on the

perspective in the transaction, each and every transaction, while building trusted transactions for the benefit of the marketplace for goods services and information.

7. Financial Or Insurance Device

The present invention enables systems and supported devices that are useful
5 in situations where parties need to have pre-defined limits to risk exposure, such as
an insurance policy or a claim. These systems are generally characterized by an
emphasis on transmission and data security, which reduces the perceived risk of the
insurer (a seller of risk coverage for pre-determined events). To the extent that
10 insurance takes into account the history and existing condition of an asset, a measure
of context or structure (tangible as well as intangible) to be covered, as well as an
economically-based replacement value (though to confuse matters, there are also
issues concerning such items as after market versus brand new, brand versus
generic, etc.), there exist differences with more transparent financial devices.
15 Financial devices (essentially a "credit agreement" or credit facility based on an
imprecise estimate of condition but also experience or trust) rely on the ability,
perceived or actuarially observable, to repay credit extended on behalf of the device
holder. Whereas financial or credit history is transparent in many cases, private
information about an individual's history or condition are perceived to be have
20 higher implicit value to the user. Financial devices and insurance devices converge
at those points where privacy or personal information are equivalent with financial
or credit information. Both types of risk have differing requirements for updating or
adjustment over the course of use of a particular line of credit or insurance policy.

Cars may be embedded with telemetry sensors to determine the real time
condition of various components, such as the frame, engine, brakes, or any
25 combination of components mutually deemed to justify such monitoring.
Alternatively, a smart card-like device equipped with a transducer may be used to
"capture" images of items that are packed (for travel insurance purposes), insurable
items in a residence (for homeowner's insurance purposes), etc. Any image
captured may be securely watermarked by the device and then exported to an
30 insurance provider via a transmission line (an ATM, a wireless connection such as a
mobile phone, a PC modem connection, etc.). An insurance provider may offer such

services at auto service/repair facilities, airports, etc. with a mutual reduction in claims costs and adjustments costs.

Medical information may similarly be digitally stored, securely watermarked, and time-stamped (for any perceptible data stored, such as images or
5 voice) for reference to an individual's health. based on varying levels of access to stored information, which may be distributed among different physicians or handled by a central medical information infomediary. The secured image may be sent to an insurance provider as a secured image (both the device and storage facility may independently verify the security or tamperproofing of the perceptibly represented
10 information). The doctor, patient, health care provider, government agencies can all have varying degrees of access that can be made transparent to the patient. This is an inherent benefit over the prior art in that the patient can see those records that are then watermarked and securely stored.

Additionally, the present invention provides the novel feature of enabling the
15 same information, at the request or demand of the patient, to be sent to a personal or secure storage "space," so that patients may have more accessibility and control over their own medical records and medical conditions. In one embodiment, the information may be provided as digitized bits. In another embodiment, the data may be provided in a tangible form.

20 The information may be stored as tangible records or intangible, bit-represented records. Doctors may use tamperproofed signals (watermarked audio, image, video, virtual reality, any humanly-perceptible signal) and records that are perceptible to lower insurance costs and potential liability. The prior art ignores the mutual benefits afforded by bi-directional information exchange (that can be
25 tamperproofed with secure watermarking) and transparency in creating opportunities for trusted transactions.

Additional data, such as the transaction information that may be evidenced on a credit card bill or statement, may also be automatically associated with the stored image(s) for later use. In one embodiment, the user may send the same
30 secured data to a private data storage facility, or create personalized records, which may serve as a secondary set of records against which other data sent to the insurance or financial provider may be verified or validated. According to another

embodiment of the present invention, authorized mechanics, physicians, and pharmacists, may add to, but not access or manipulate, previously stored data. These individuals may also be bound by rules for establishing the history and condition of any person or physical good that is being underwritten or financed.

5 The present invention provides certification authorities the ability to determine the authenticity of data. In cases where public-key steganography or cryptosystems are preferred, the embodiments extend to those implementations as well. Moreover, they enable secure transmission capabilities over unsecured data transmission lines.

10 Referring to Fig. 11, a personal information device according to one embodiment of the present invention is provided. Personal information device (PID) 1102 may be used with financial institutions, insurance companies, etc.

 In one embodiment, PID 1102 may be smart card; that is, a device that resembles a credit card, but includes a processor, a power supply, a memory, and an
15 input and output device. In another embodiment, PID 1102 may be a card including a magnetic strip.

 PID 1102 preferably has a Unique ID. In one embodiment, the Unique ID of PID 1102 may be a policy number, a social security number, etc.

 PID 1102 may receive information from several sources. In one
20 embodiment, telemetry data 1104 may be input to PID 1102. Perceptible data 1106, such as images, photos, etc. may be input to PID 1102. In still another embodiment, associated data, such as purchase receipts, descriptions, serial numbers, registrations, etc., which may be value-adding components, may be input to PID 1102.

 PID 1102 may provide output data 1110 to a variety of entities. In one
25 embodiment, output data 1110 may be provided to company 1112 and to storage 1114. Company 1112 may include any organization the may receive output data 1110, including an insurance company, a financial institution, etc. Storage 1114 may include any personal use for output data 1110, including a private data storage such as a fixed storage media, paper records, etc. Company 1112 and storage 1114
30 may receive output data 1110 in different formats. In one embodiment, output data 1110 is provided according to predetermined parameters for the entity.

Output data 1110 may be watermarked, or it may be time stamped, or it may include both. Other types of encryption are provided.

In general, output data 1110 is preferably provided to the entity via a secure communication link. Transmission of output data 1110 may be controlled by the
5 entity (e.g., company 1112 or storage 1114) or by the user.

8. Authentication Device

According to another embodiment of the present invention, an authentication device may be provided. Referring to Fig. 12, authentication device 1202 may be a credit-card sized "smart card," including a processor, a power supply, a memory,
10 and an input and output device. In another embodiment, authentication device 1202 may be a palm sized computing device.

A variety of input devices may be provided. In one embodiment, a bar code scanner may be used. In another embodiment, a keypad may be used. Other input devices may be used as necessary.

15 In one embodiment, authentication device 1202 may include a display, such as a LCD screen. Other display technologies are within the contemplation of the present invention.

In one embodiment, authentication device 1202 may be a government-issued device.

20 Anonymous authentication 1204 may be provided. Anonymous authentication 1204 may be used to authenticate a product, a medicine, a label, etc. Anonymous authentication 1204 communicates with authentication device 1202 to authenticate the item in question. In one embodiment, authentication device 1202 may display relevant information, such as known warnings, recommended dosages,
25 etc. regarding the item in question.

In another embodiment, image capture device 1206 may be provided. Image capture device 1206 may include a digital camera, a scanner, etc. In one embodiment, image capture device 1206 may time stamp the image as it is captured.

30 Identity exchange 1208 may be provided. Identity exchange 1208 includes a Unique ID that may be authenticated or modified by the user. In one embodiment, in order to verify the identity of an individual, additional independent identify

verification may be required in addition to identity exchange 1208. This is because authentication device 1202 may be stolen, borrowed, etc.

Certification authority 1210 may be provided. Certification authority may be bound by federal, state, and local laws. In addition, private restrictions may apply to
5 certification authority 1210.

In one embodiment, certification authority may be further bound by geographical (e.g., location) or age basis (e.g., date of birth, age, etc.) to verify.

Referring to Fig. 13, a method of use for an authentication device is provided. In step 1302, a user locates information to be authenticated. This may
10 include a variety of information. The information is then entered into the authentication device.

In step 1304, perceptible data is marked with a public key secure watermark. In one embodiment, this may be done in real time.

In step 1306, the user provides a public key to initiate the authentication.

15 In step 1308, a response is sent from the certification authority, or additional prompts for higher access levels are provided.

In one embodiment, transmissions between any elements may be over a secure communication link, including SSL or similar transmission exchange.

In another embodiment of the present invention, an authentication device
20 may comprise a Internet web browser. For example, the authentication device may be a "plug in" for a web browser. Such a authentication device may be used to verify, or authenticate, items on web pages. For instance, according to one embodiment of the present invention, the authentication device may be used to
25 verify that an Internet bank that displays the FDIC logo is authorized to display this logo. In one embodiment, real time verification will allow a user to verify such, and govern transactions accordingly.

It will be evident to those of ordinary skill in the art that the above-described modes and embodiments of the present invention, while they disclose useful aspects of the present invention and its advantages, are illustrative and exemplary only, and
30 do not describe or delimit the spirit and scope of the present invention, which are limited only by the claims that follow below.

| CLAIM:

1. A method for trusted transactions, comprising:
 - establishing an agreement to exchange digitally-sampled information between a first and a second party;
 - 5 exchanging the digitally-sampled information between the first and the second party; and
 - approving the digitally-sampled information using an approval element selected from the group consisting of a predetermined key, a predetermined message, and a predetermined cipher, the step of approving the digitally-sampled
 - 10 information using an approval element consisting of a step selected from the group consisting of verifying the digitally-sampled information with the approval element, authenticating the digitally-sampled information with the approval element, and authorizing the digitally-sampled information with the approval element.
2. The method of claim 1, wherein the step of approving the digitally-
- 15 sampled information precedes the step of exchanging digitally-sampled information.
3. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:
 - transmitting a first party approval element from the first party to the
 - 20 second party; and
 - transmitting a second party approval element from the second party to the first party.
4. The method of claim 3, wherein the steps of transmitting the first party approval element and transmitting the second party approval element occur substantially simultaneously.
- 25 5. The method of claim 3, wherein the first party approval element and the second party approval element are symmetric.
6. The method of claim 3, wherein the first party approval element and the second party approval element are asymmetric.
7. The method of claim 1, wherein the approving step is accomplished
- 30 using predetermined key pairs.

8. The method of claim 7, wherein the predetermined key pairs are created by a cipher selected from the group consisting of steganographic and cryptographic ciphers.

9. The method of claim 1, wherein the predetermined cipher is selected
5 from the group consisting of a steganographic cipher and a cryptographic cipher.

10. The method of claim 1, wherein the predetermined message is selected from the group consisting of a unique identification, a unique time, data associated with a predetermined information function, and combinations thereof.

11. The method of claim 1, wherein the predetermined message has value
10 independent from at least one primary value-adding component.

12. The method of claim 1, wherein the predetermined message contains at least one value-adding component.

13. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:
15 verifying the digitally-sampled information with the approval element.

14. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:
20 authenticating the digitally-sampled information with the approval element.

15. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:
authorizing the digitally-sampled information with the approval
25 element.

16. The method of claim 1, further comprising:
entering into a security arrangement based on the exchange.

17. The method of claim 16, wherein the security arrangement is a non-cash right.

18. The method of claim 16, wherein the security arrangement is an
30 option for a non-cash right.

19. The method of claim 16, wherein the security arrangement is an equity purchase right.

20. A method for conducting a trusted transaction between two of a plurality of parties who have reached an agreement to transact, comprising:
- establishing a secure transmission channel between the two parties;
 - approving an identity of at least one of the two parties;
 - 5 determining an amount of value-added information to be exchanged between the parties, the value-added information comprising a plurality of value-adding components;
 - verifying the agreement to transact; and
 - transmitting the value-added information.
- 10 21. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:
- at least one of the parties verifying at least one value-adding component.
22. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:
- 15 at least one of the parties authorizing at least one value-adding component.
23. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:
- at least one of the parties authenticating at least one value-adding component.
- 20 24. The method of claim 20, wherein the step of establishing a secure transmission channel between two of a plurality of parties comprises:
- exchanging data between the two parties;
 - selecting a pre-determined key to exchange over the secure transmission channel; and
 - 25 securing the transmission channel by at least one of a password, a pass phrase entry, a query to a user, and real-time biometric data transfer.
25. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:
- exchanging a value-adding component for each party to the other party.
- 30 26. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

at least one of the parties independently verifying a value-adding component of the other party.

27. The method of claim 20, wherein a bandwidth of the primary value-added information comprises a description including at least one of a bandwidth
5 requirement for transmission, a bandwidth requirement for storage, and a bandwidth requirement for playback.

28. The method of claim 20, wherein at least one term for the exchange of primary value-added information is negotiated between parties, the terms selected from the group consisting of an offer, an acceptance, and consideration.

10 29. The method of claim 28, wherein the at least one term changes in real time.

30. The method of claim 28, wherein access to the at least one term is restricted by at least one of a pass phrase, a password, a correct answer to a query, a real time authentication with a biometric, a real time authentication with personal
15 entropy information, real time telemetry data, and access to additional transaction records.

31. The method of claim 28, wherein the at least one term is referenced by a subsequent transaction.

20 32. The method of claim 28, wherein the at least one term is access restricted by a provider of at least one value-adding component.

33. The method of claim 28, wherein the at least one term is traced by a provider of at least one value-adding component.

34. The method of claim 28, wherein the at least one term is authenticated by a provider of at least one value-adding component.

25 35. The method of claim 28, wherein the at least one term is accessed for at least one of verification, authentication, and authorization.

36. The method of claim 28, wherein the at least one term comprises at least one of readable text, visible color, voice command, and visual instructions.

30 37. The method of claim 28, wherein the at least one term comprises humanly perceptible information.

38. The method of claim 20, wherein the value-added information is convertible into a tangible good.

39. The method of claim 20, further comprising verifying the value-added information.

40. The method of claim 20, further comprising authenticating the value-added information.

5 41. The method of claim 20, wherein the value-adding components comprise at least one of an equity purchase right, an option, a warrant, and a security instrument.

42. The method of claim 20, wherein the value-adding components comprise a non-cash service.

10 43. A method for conducting at least one trusted transaction between at least two parties, comprising:

authenticating the at least two parties;

agreeing to a security of a transmission channel;

exchanging secondary value-added information;

15 determining at least one term for a primary value-added information exchange; and

facilitating payment for the transaction based on the terms.

44. The method of claim 43, wherein the step of facilitating payment for the transaction is accomplished in real-time.

20 45. The method of claim 44, wherein the at least one term includes micropayment systems.

46. The method of claim 43, wherein the transaction is governed by at least one of legal restrictions that apply to at least one of the parties, a timing of the transaction, a geographic location of the transaction, and value-added information.

25 47. The method of claim 43, wherein the value-added information is represented physically.

48. The method of claim 43, wherein the secondary value-added information comprises at least one of an equity option and at least one term from a previous trusted transaction.

30 49. The method of claim 43, wherein the secondary value-added information derives benefit from a previous trusted transaction.

50. The method of claim 49, wherein the at least two trusted transactions are substantially contiguous.

51. The method of claim 49, wherein the at least two trusted transactions have at least one of a time or an event limitation.

5 52. The method of claim 43, further comprising the step of:
agreeing to at least one term for a different transaction.

53. The method of claim 43, wherein the first trusted transaction enables manipulation of information in a subsequent transaction.

10 54. A method for conducting a trusted transaction between at least two parties, comprising:

establishing a steganographic cipher;

exchanging secondary value-added information between the parties;

agreeing to at least one term for the exchange of primary value-added information; and

15 facilitating payment for the transaction.

55. The method of claim 54, wherein the step of facilitating payment for the transaction is accomplished in real-time.

20 56. The method of claim 54, wherein the step of facilitating payment for the transaction is based on the at least one term for the primary value-added information exchange.

57. The method of claim 54, wherein the transaction is governed by at least an age and a geographical limitation.

25 58. The method of claim 54, wherein the transaction is governed by at least one of legal restrictions that apply to at least one of the parties, a timing of the transaction, a geographic location of the transaction, and value-added information.

59. The method of claim 54, wherein at least one of the primary and secondary value-added information is represented physically.

30 60. A method for conducting a trusted transaction between at least two parties, comprising:

identifying at least one of a unique identification for each of the at least two parties, a unique identification of the transaction, a unique identification of value-

added information to be transacted, and a unique identification of a value-adding component;

applying a steganographic cipher; and

verifying an agreement to transact between the parties.

5 61. The method of claim 60, wherein the trusted transaction is governed by at least one of a transaction age and a geographical location of the transaction.

62. The method of claim 60, wherein the trusted transaction is governed by legal restrictions that apply to at least one of the parties, a timing of the transaction, and value-added information.

10 63. The method of claim 60, wherein the value-added information is represented physically.

64. The method of claim 60, further comprising the step of:
transmitting the value-added information.

15 65. The method of claim 60, wherein the agreement causes at least one secondary term to be enabled for at least one of the parties.

66. The method of claim 60, wherein the agreement creates at least one term for a second trusted transaction.

67. The method of claim 60, further comprising the step of:
agreeing to at least one term for a second trusted transaction.

20 68. A method for bi-directionally exchanging value-added information between at least two parties, comprising:

associating a plurality of unique identifiers with the value-added information, the value-added information including at least one of a digital watermark, a file header, a file attachment, and a file wrapper;

25 associating each of the at least two parties with unique identifiers, the unique identifiers including at least one of a digital watermark, a file header, a file attachment, and a file wrapper; and

exchanging value-added information between the at least two parties.

30 69. The method of claim 68, wherein the transaction and the unique identifiers are stored for subsequent reference.

70. The method of claim 68, wherein unique identifiers are access restricted by at least one pre-determined rule.

71. The method of claim 68, wherein the unique identifiers are asymmetrically access restricted.

72. The method of claim 70, wherein the access restriction is dependent on verification of a querying party.

5 73. The method of claim 70, wherein the access restriction allows value-added information to be transmitted in an altered format.

74. The method of claim 68, further comprising the step of:
associating the bi-directional exchange of value-added information with a subsequent exchange of additional value-added information.

10 75. The method of claim 74, wherein the additional value-added information is governed by at least one separate term.

76. The method of claim 74, wherein the additional value-added information comprises a right to purchase equity in at least one of the parties to the transaction.

15 77. The method of claim 68, further comprising the step of agreeing to at least one term for a subsequent transaction.

78. A method for exchanging value-added information between at least two parties, comprising:

providing a data transmission means;

20 verifying the parties to the transaction;

negotiating at least one term selected from the group consisting of a price, a service, a selection, and combinations thereof; and

binding the at least one term to the information using at least one of a digital watermark, a file header, metadata, and a file wrapper;

25 wherein the at least one bound transaction term comprises value-added information.

79. The method of claim 78, wherein the at least one bound term cannot be removed without altering the value-added information.

30 80. The method of claim 78, wherein an authentication of the value-added information requires successful verification of the at least one bound term.

81. A method for trusted transactions, comprising the steps of:
receiving data to be processed;

determining a structure of the data;
determining if the data is authentic; and
determining an associated usage of the data based on the data structure and
the authenticity of the data.

5 82. The method of claim 81, wherein the data is comprises at least one of
aesthetic data and functional data.

83. The method of claim 81, wherein the structure of the data is
determined based on at least one of a digital signature, a digital watermark, and a
digital notary.

10 84. The method of claim 81, wherein the authenticity of the data is
determined based on at least one of a digital signature, a digital watermark and a
digital notary.

85. The method of claim 83, further comprising the step of verifying at
least one of the digital signature, the digital watermark, and the digital notary by at
15 least one of a trusted third party and a certification authority

86. The method of claim 83, wherein a bit from at least one of the digital
signature, the digital watermark and the digital notary can be verified by at least one
of a trusted third party and a certification authority.

20 87. A method for secure transaction, comprising:
receiving a request to process a transaction;
uniquely identifying a source of the request;
uniquely identifying at least one term of the request; and
storing identification information for transaction negotiation.

88. The method of claim 87, wherein the at least one term of the request
25 includes at least one of a condition and a timing of the request.

89. The method of claim 87, wherein the request may be received over at
least one of a secure and an unsecure transmission line.

90. The method of claim 87, wherein the source of the request is
identified by at least one of a determinable origin of the source and a predetermined
30 routing of the request by the seller.

91. The method of claim 87, wherein the at least one term of the request
comprises a value-adding component.

92. The method of claim 87, wherein the transaction is noncontiguous with the request.

93. The method of claim 87, wherein the transaction and the request are processed in real time.

5 94. A method for the facilitation of the exchange of information data between at least a first party and a second party, comprising:

receiving a rule governing information data from a first party;

receiving a request for the information data from a second party;

matching the rule with the request; and

10 uniquely identifying the information data and the first and second parties;

wherein the information data is selected from the group consisting of unstructured data and structured data.

95. The method of claim 94, wherein the rule governs a use of the information data.

15 96. The method of claim 95, wherein the use comprises manipulating the information data.

97. The method of claim 95, wherein the use comprises transferring the information data.

20 98. The method of claim 95, wherein the use comprises subsequently changing to the information data.

99. The method of claim 95, wherein the use comprises playing the information data.

100. The method of claim 95, wherein the use comprises recording the information data.

25 101. The method of claim 95, wherein the use comprises converting the information data from at least one of analog to digital format and digital to analog format.

102. The method of claim 94, wherein the structured data comprises at least one of source code and executable code.

30 103. The method of claim 94, wherein the request may be filtered according to at least one of a characteristic, a function, an aesthetic, a condition, a history, a context, a consideration, a cost, a time, a bandwidth requirement, a storage

requirement, an available format, an owner identification, a creator identification, a seller identification, an infomediary identification, a distributor identification, a distribution parameter, an age in unit of time, and a upcoming information data.

104. The method of claim 94, wherein the unique identification is
5 cryptographically secure.

105. The method of claim 104, wherein the unique identification may be cryptographically secured by using at least one of a cryptographic cipher, a steganographic cipher for digital signatures, a special one-way hash, a digital watermark, and a time stamp, and combinations thereof.

106. The method of claim 94, further comprising the step of verifying the
10 unique identification by an independent third party

107. The method of claim 106, wherein the independent third party comprises at least one of a certification authority, a creator of the information, an owner of the information, and a mutually agreed to third party.

108. The method of claim 94, wherein the exchange is in real time.

100. The method of claim 94, wherein the exchange is substantially
15 noncontiguous.

110. A method for rights management, comprising:

receiving information;

20 determining whether the information is structured information or unstructured information;

identifying the information with a steganographic cipher;

25 authenticating the information with at least one of a digital signature and digital watermark check; and

associating the identification and authentication results with at least one of a predetermined record, a predetermined rule, and a predetermined function.

111. The method of claim 110, further comprising the step of:

30 limiting an access to the information based on a predetermined exposure of a decision maker.

112. The method of claim 110, further comprising the step of:

limiting a financial exposure based on a predetermined exposure of a decision maker.

113. A method for rights management, comprising:
exchanging information between at least two parties;
verifying the information, the verification performed by at least one of the
parties; and

5 activating at least one of a predetermined act and a rule based on the result of
the verification of information.

114. The method of claim 113, wherein information is exchanged in a
format selected from the group consisting of an analog waveform and binary data.

10 115. The method of claim 113, further comprising the step of
authenticating the verification by a trusted third party.

116. The method of claim 113, wherein an anonymity of each party is
maintained during the step of verifying the information.

117. The method of claim 113, further comprising the step of making the
verification publicly available for additional verification.

15 118. The method of claim 113, wherein the predetermined rule is activated
noncontiguously with verification.

119. The method of claim 113, further comprising the step of making the
accessible for further authentication and identification.

20 120. A method for risk management, comprising:
receiving information;
determining whether the information is structured or unstructured;
identifying information with a predetermined ciphered key;
authenticating information with at least one of a digital signature, a digital
watermark check, and a predetermined ciphered key;
25 associating identification and authentication results with a predetermined
rule; and
limiting access based on a predetermined exposure of a decision maker.

30 121. A method for securely exchanging information data between at least
two parties, comprising:
creating a private key;
deriving a corresponding public key corresponding to the information data
sought and at least one of (a) verifiable data associated with different versions of the

information data, (b) verifiable data associated with a transmitting device, and (c) verifiable data associated with an identity of the party seeking the information data;
establishing a set of one time signatures relating to the information data;
establishing a hierarchy of access to the set of one time signatures;
5 creating a public key signature that is verifiable with the public key,
including the hierarchy of access to the set of one time signatures;
providing the information to a certification authority for verification; and
verifying the one time signature and the hierarchy of access to enable
transfer of predetermined data.

- 10 122. A method for authenticating an exchange of a plurality of sets of information data between at least two parties, comprising:
creating a plurality of hierarchical classes based on a perceptual quality of the information data;
assigning each set of information data to a corresponding hierarchical class;
15 defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged;
predetermining access to the sets of information data by perceptually-based quality determinations;
20 establishing at least one connection between the exchanging parties;
perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; and
enabling a trusted transaction based on verification, and associated access, governing at least one of a set of information data sets.

- 25 123. The method of claim 122, further comprising the step of grouping each hierarchical class by at least one of a quality, a price, and a service.

124. The method of claim 123, wherein the grouping is determined by at least one of a buyer and a seller.

- 30 125. The method of claim 123, wherein the grouping enables greater exchange of information.

126. A method for authenticating the exchange of perceptual information data between at least two parties over a networked system, comprising:

creating a plurality of hierarchical classes based on a perceptual quality of the information data;

assigning each set of information data to a corresponding hierarchical class;

5 defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged;

perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data;

10 enabling a trusted transaction of the information data based on verification of means of payment, and associated access, governing at least one copy of the information data sought;

associating the transaction event with the information data prior to transmission of the information data; and

transmitting and confirming delivery of the information data

15 127. The method of claim 126, further comprising the step of grouping the class of data by at least one of quality, price, and service.

128. The method of claim 127, wherein the grouping is determined by at least one of a buyer and a seller.

20 129. The method of claim 127, wherein the grouping enables greater exchange of information.

130. The method of claim 126, further comprising the step of: confirming both a digital and an analog copy of the transmission.

25 131. The method of claim 127, further comprising the step of: associating the transaction event with the buyer or seller to develop trust with other party

132. The method of claim 126, further comprising the step of: charging at least one party based on a transaction bandwidth requirement.

133. A device for conducting a trusted transaction between at least two parties who have agreed to transact, comprising:

30 means for uniquely identifying unique identification information selected from the group consisting of a unique identification of one of the parties, a unique

identification of the transaction, a unique identification of value-added information to be transacted, and a unique identification of a value-adding component;

a steganographic cipher; and

means for verifying an agreement to transact between the parties.

5 134. The device of claim 133, wherein the unique identification information seeds the steganographic cipher.

135. The device of claim 133, wherein the unique identification information is verifiable.

136. The device of claim 133, further comprising:

10 means for transmitting value-added information.

137. The device of claim 136, wherein the means for transmitting value-added information transmits the value-added information by a method selected from the group consisting of electrical and physical.

138. The device of claim 136, wherein the wherein the means for
15 transmitting value-added information transmits the value-added information in a medium selected from the group consisting of a pre-determined file format and a predetermined carrier medium.

139. A device for conducting a trusted transaction between at least two parties who have agreed to transact, comprising:

20 means for uniquely identifying unique identification information selected from the group consisting of a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value-added information to be transacted, and a unique identification of a value-adding component; and

means for enabling a subsequent mutually agreed to at least one term.

25 140. The method of claim 139, wherein the at least one subsequent term concerns at least one of equity, service, and recognition.

141. A device for conducting trusted transactions between at least two parties, comprising:

a steganographic cipher;

30 a controller for receiving input data or outputting output data; and

at least one input/output connection,

wherein the device has a unique identification code.

142. The device of claim 141, wherein the unique identification code is predetermined.

143. The device of claim 141, wherein the unique identification code is upgradeable.

5 144. The device of claim 141, wherein the steganographic cipher comprises:

a number generator selected from the group consisting of a pseudo-random number generator and a random number generator;

10 a predetermined key generation algorithm selected from the group consisting of a hash function and a special one-way function;

a predetermined message information selected from the group consisting of a digital signature, a time stamp, a digital watermark, and function-dependent data;

a predetermination of the information carrier signals characteristics selected from the group consisting of a perceptual characteristic and a signal feature.

15 145. The device of claim 141, wherein the steganographic cipher manipulates the input data.

146. The device of claim 141, wherein the steganographic cipher manipulates the output data.

20 147. The device of claim 141, wherein the input of input data is controlled by predetermined information selected from the group consisting of a pass phrase, a password, biometric data, and a personal entropy query.

148. The device of claim 144, wherein an identification of a device holder requires at least one additional iteration of verification by at least one of a pass phrase, a password, biometric data, and a personal entropy query.

25 149. The device of claim 141, wherein the device converts at least one value-added information metrics selected from the group consisting of a price, a selection, and a service into humanly perceptible information.

30 150. The device of claim 149, wherein the humanly perceptible information relates to at least one of a present value cost to the party, at least one term for use, a level of confidence over the transaction, a level of confidence over transmission security, and a data integrity metric of the value-added information.

151. The device of claim 141, wherein the device is manufactured as a device selected from the group consisting of a smart card, a microchip, and a software application.

5 152. The device of claim 151, wherein the manufactured device is tamper-resistant.

153. The device of claim 151, wherein the manufactured device ceases to function if at least one function of the manufactured device is altered by an unauthorized party.

10 154. The device of claim 151, wherein the software application is subject to a steganographic cipher for serialization or creating unique instances of individual copies of the application.

155. The device of claim 141, further comprising an analog to digital converter.

15 156. The device of claim 141, wherein the device is securely linked to at least one of a means for payment and a transmission channel for private key exchange and approval.

157. The device of claim 156, wherein the key approval is selected from the group consisting of identification, authentication, and authorization.

20 158. The device of claim 141, wherein the device transacts according to at least one predetermination of at least an identity of the vendor, a plurality of conditions of the information transfer, a payment, and an identity of a separate but similar device.

159. The device of claim 141, wherein the device further comprises:
an internal memory.

25 160. A trusted transaction device for transmitting authentic value-added information data between at least two parties, comprising:

a display;

a unique identifier;

means for ciphering information input and output;

30 means for interacting with other similarly functional devices; and

means for storing or retrieving value-added information and a value-adding component.

161. The device of claim 160, wherein the display transceives cryptographically verifiable information.

162. The device of claim 161, wherein the cryptographically verifiable information is observed by a user.

5 163. The device of claim 160, wherein the unique identifier is upgradeable.

164. The device of claim 160, wherein the unique identifier is serialized.

165. The device of claim 160, wherein the unique identifier comprises at least one of a means for facilitating transaction authorization, a means for facilitating
10 bandwidth requirements, and a means for associating the unique identifier with information.

166. The device of claim 160, wherein the means for ciphering information comprises at least one of a means for facilitating transaction authorization, a means for facilitating bandwidth requirements, and a means for
15 associating the unique identifier with information.

167. The device of claim 160, further comprising:

a means for establishing communications/connecting with other similarly outfitted devices;

a means for storing or retrieving trusted transaction value-adding component
20 data; and

a means for attaching storage or transducers to the device.

168. The device of claim 167, further comprising:

means for anonymous tracing of the transaction.

169. The device of claim 167, wherein information is processed in real
25 time.

170. A device for securely exchanging information data, comprising:

means for creating a private key by the party seeking predetermined data;

means for deriving a corresponding public key based on the predetermined data and at least one of verifiable data associated with different versions of the
30 information, verifiable data associated with a transmitting device, and verifiable data associated with the identity of the party seeking information;

means for creating a set of one-time signatures relating to the predetermined data;

means for validating a predetermined hierarchy of access of the set of one-time signatures;

5 means for creating a public key signature, verifiable with the public key, including the access hierarchy of one time signatures;

means for securely transacting predetermined data by providing information relating to a proposed transaction; and

10 means for verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

171. The device of claim 170, further comprising a means for interacting with other equipped devices.

172. The device of claim 171, further comprising: means for establishing a secure transmission.

15 173. A system for the secure exchange of predetermined, verifiable information data between at least two parties, comprising:

at least one condition for the use of the information;

means for differentiating between predetermined information and other seemingly identical information based on an authentication protocol;

20 means for associating authenticity of verifiable information data with at least one condition for use;

a storage unit for storing the predetermined, verifiable information; and

means for communicating with the predetermined, verifiable information storage.

25 174. The system of claim 173, wherein the means for differentiating between predetermined information and the seemingly identical information based on an authentication protocol comprises at least one of a hash, a signature, and a secure watermark.

175. The system of claim 173, further comprising:

30 means for authenticating verifiable information flow between transacting parties.

176. The system of claim 173, wherein the system securely exchanges predetermined, verifiable information data prior to consummating verifiable financial transaction between the parties.

5 177. A system for the exchange of information, comprising:
at least one sender;
at least a receiver;
a verifiable message; and
a verification of the message by at least one of the senders and the receivers;
10 wherein a verification of the message enables a decision over receiving additional related information.

178. A system for computer based decision protocol comprising:
a means for identifying between structured and unstructured information;
a means for authenticating structured information; and
15 a means for enabling a decision rule based on the identity and authenticity of the information.

179. The system of claim 178, further comprising:
a means for comparing decision results with at least one predetermined rule.

180. A system for computer-based decision protocol, comprising:
20 means for identifying between structured and unstructured information;
means for identifying structured information; and
means for enabling a predetermined decision rule based on the identity of the information.

181. The system of claim 180, wherein the structured information is defined by at least one of a digital signal processor and a general purpose computing
25 device.

182. The system of claim 180, wherein the structured information comprises binary data.

183. The system of claim 180, wherein the structured information is humanly perceptible.

30 184. The system of claim 180, wherein the structured information is defined in a bit addressable manner.

185. The system of claim 180, wherein the structured information has at least one mathematically definable characteristic.

186. The system of claim 180, wherein the structured information is selected from the group consisting of pseudo-random and random.

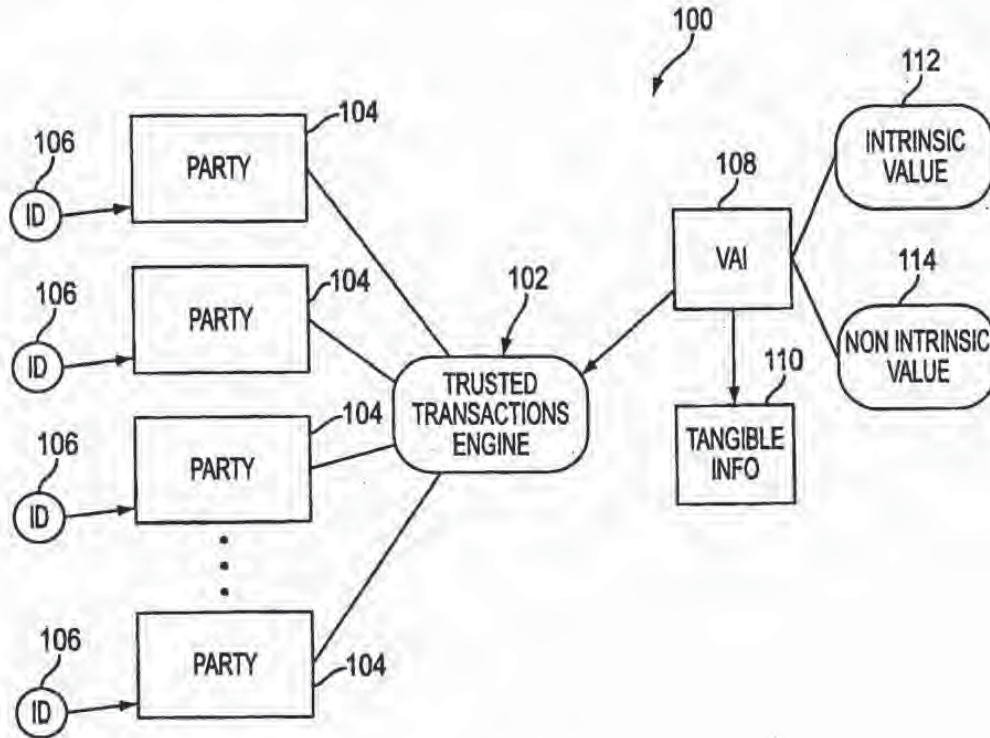


FIG. 1

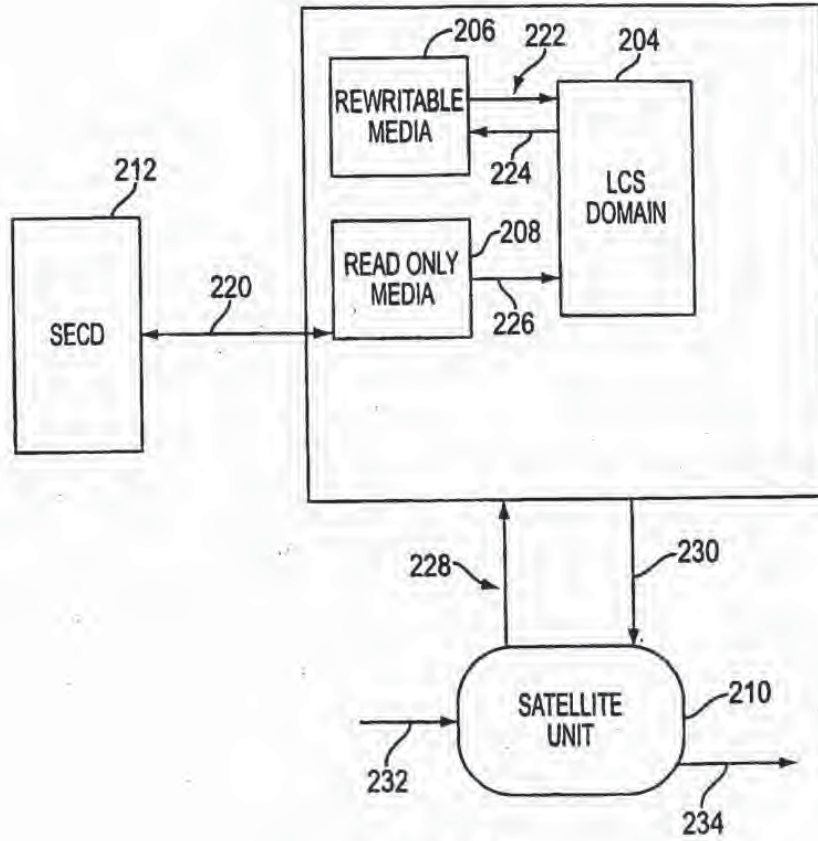


FIG. 2

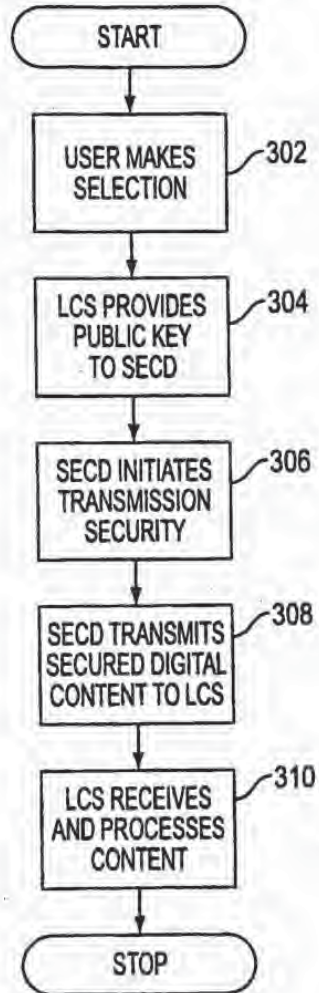


FIG. 3

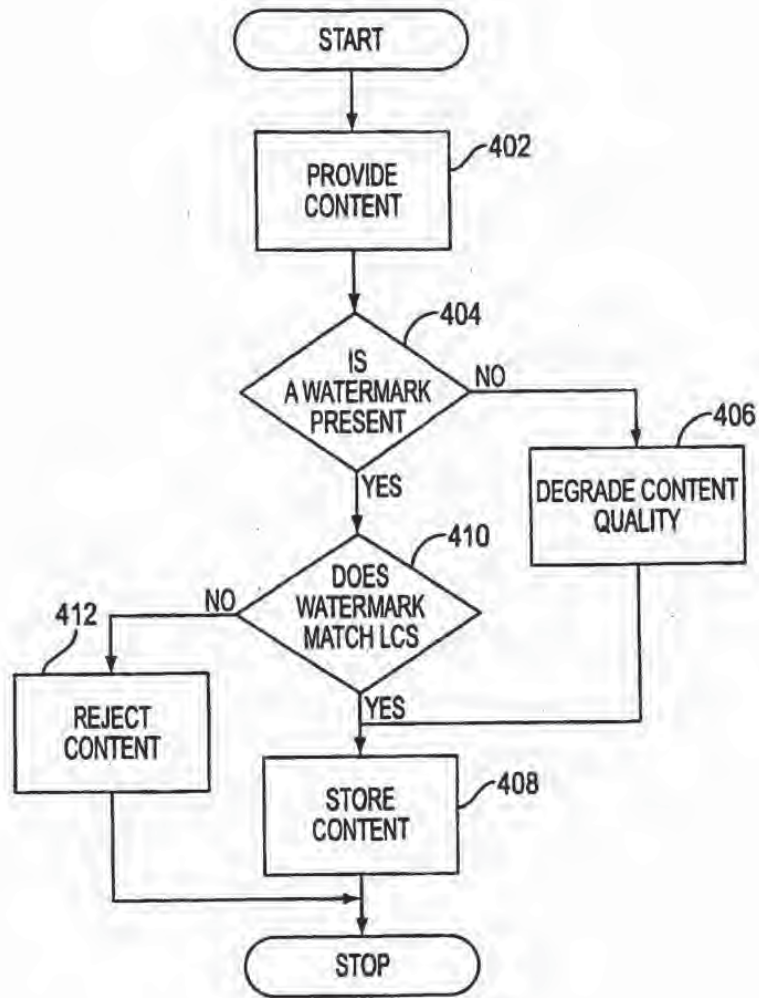


FIG. 4

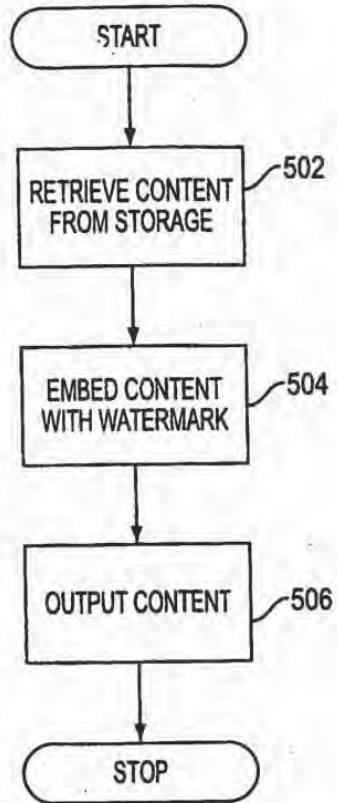


FIG. 5

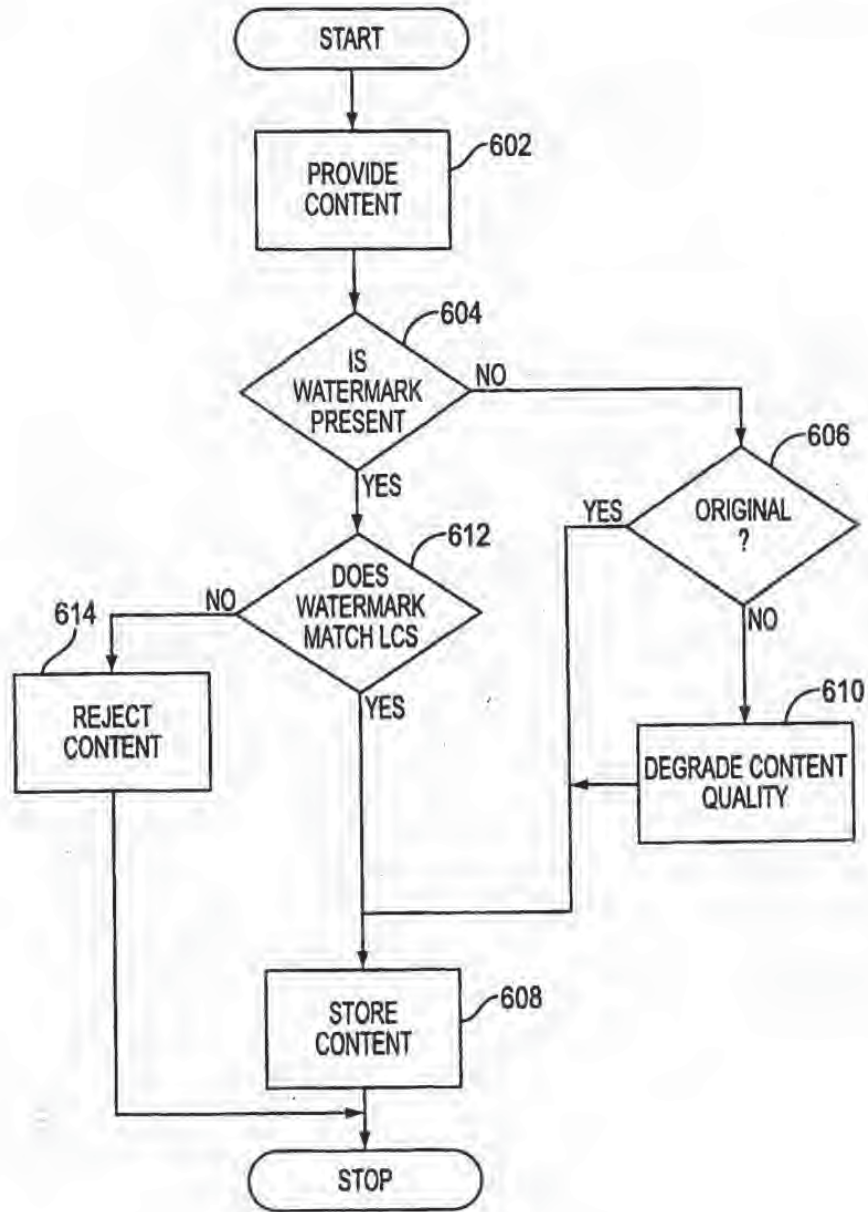


FIG. 6

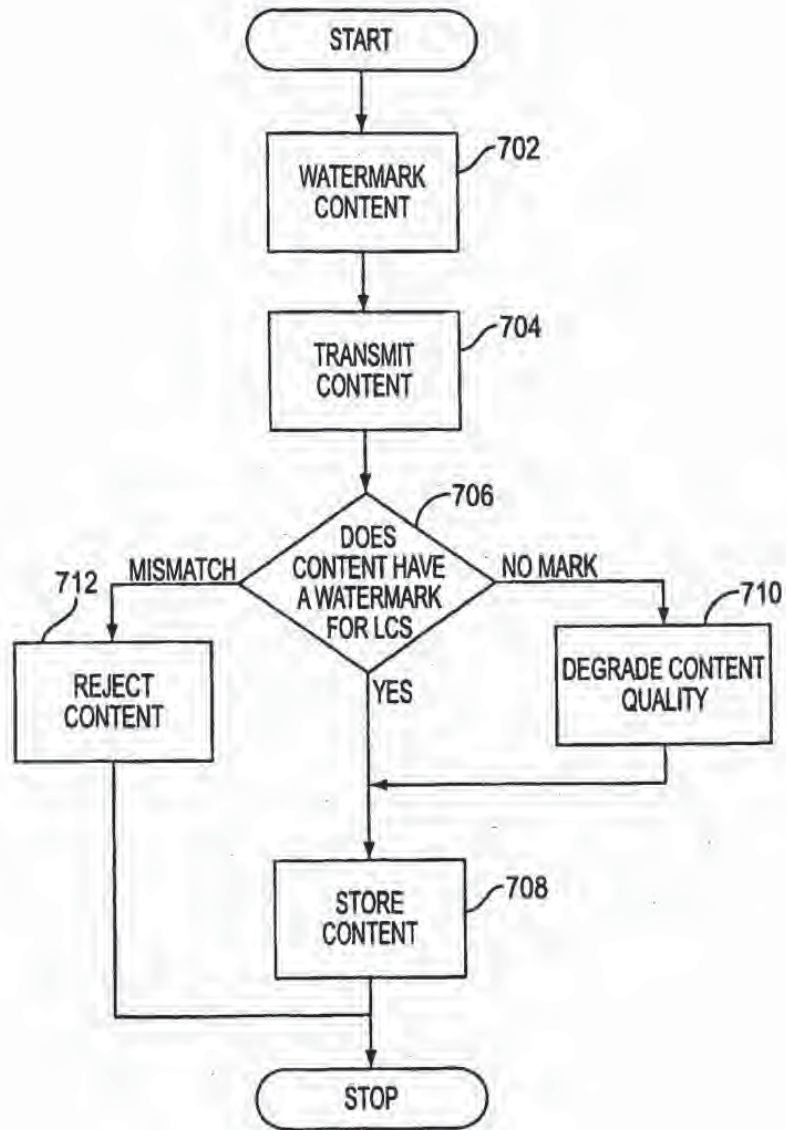


FIG. 7

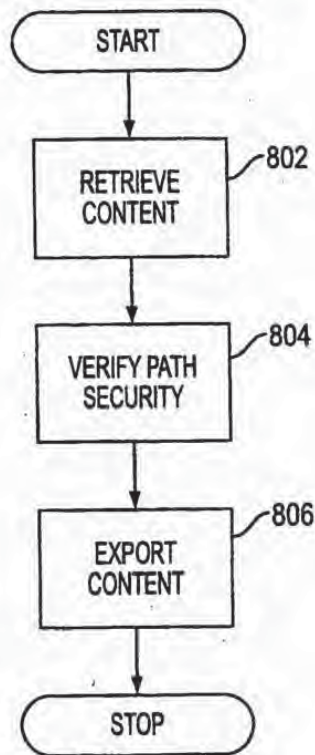


FIG. 8

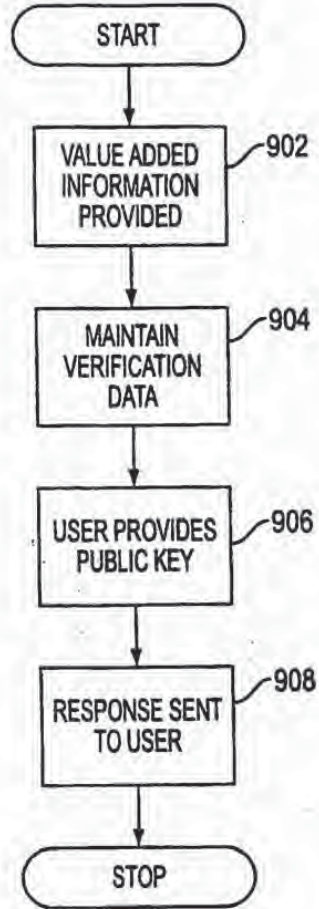


FIG. 9

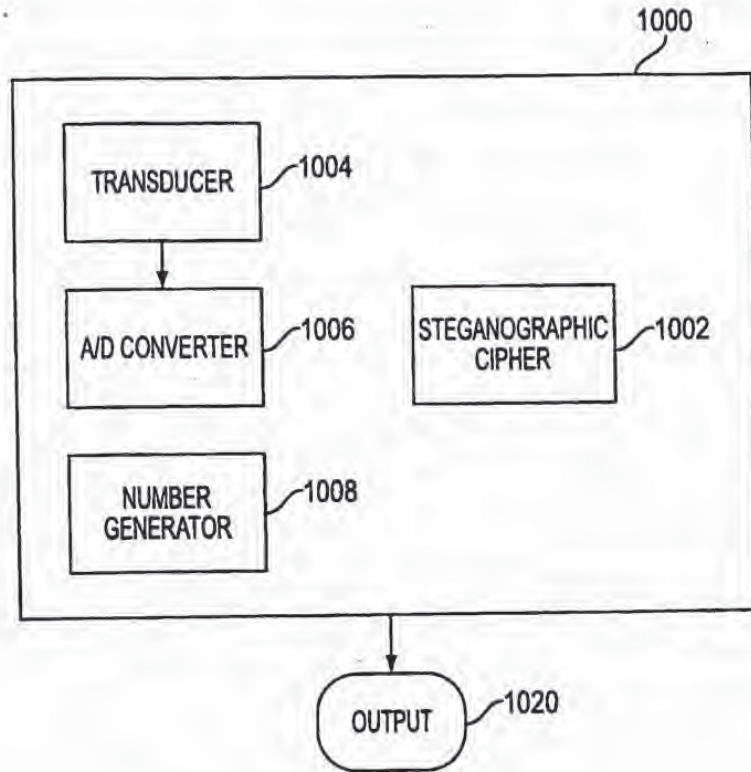


FIG. 10

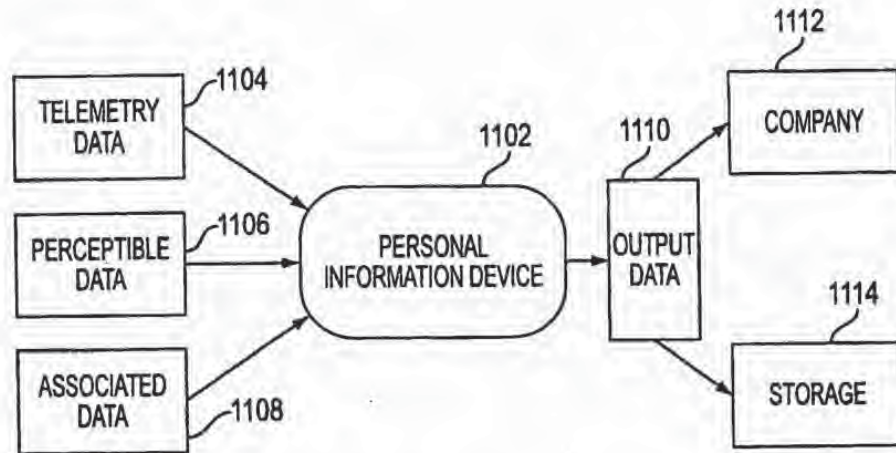


FIG. 11

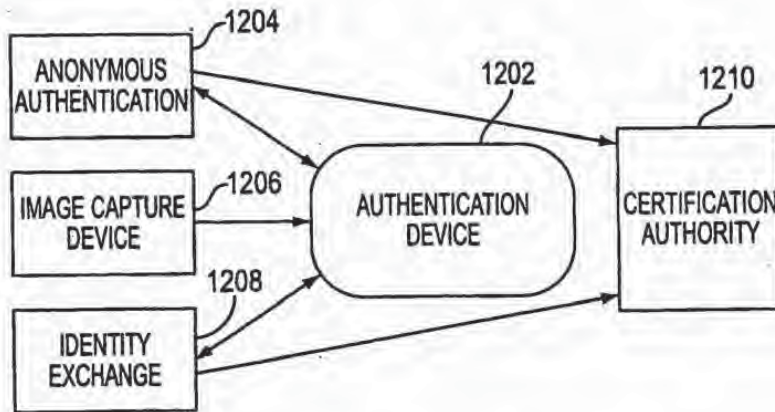


FIG. 12

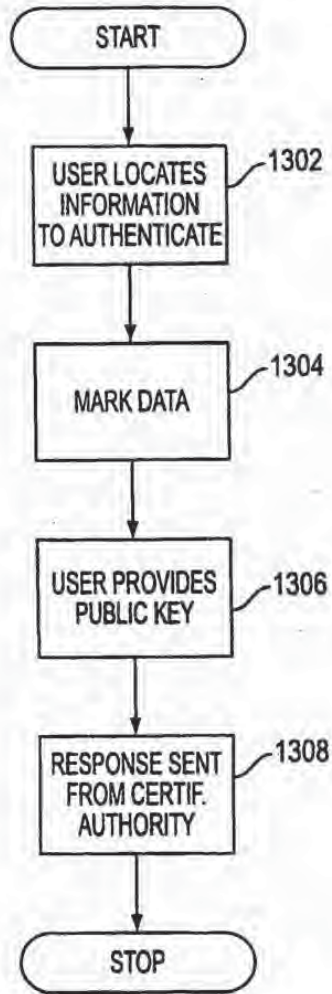


FIG. 13

INTERNATIONAL SEARCH REPORT

Int. Patent Application No
PCT/US 00/33126

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F17/60		
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) IPC 7 G06F		
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 practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) abstract column 3, line 26 -column 5, line 31	1-19
X	US 5 790 677 A (SPELMAN JEFFREY F ET AL) 4 August 1998 (1998-08-04) abstract column 2, line 6 -column 4, line 39	1-19
X	WO 96 29795 A (MICALI SILVIO) 26 September 1996 (1996-09-26) abstract page 5, line 27 -page 8, line 6	1-19
	-/-	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C		
<input checked="" type="checkbox"/> Patent family members are listed in 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 but published on or after the international filing date *L* document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document relating 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. *S* document member of the same patent family
Date of the actual completion of the international search 20 March 2001		Date of mailing of the international search report 04.04.01
Name and mailing address of the ISA European Patent Office, P.O. 5016 Patentkanal NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 851 edo nl, Fax (+31-70) 340-3016		Authorized officer Corcoran, P

Form PCT/ISA/210 (second sheet) (July 2002)

INTERNATIONAL SEARCH REPORT

 In and Application No
 PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 24833 A (NICALI SILVIO) 10 July 1997 (1997-07-10) abstract page 2, line 12 -page 5, line 8	1-19
A	US 5 539 735 A (MOSKOWITZ SCOTT A) 23 July 1996 (1996-07-23) abstract column 1, line 60 -column 4, line 29	1-19
A	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK DELIVERED SERVICES" DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE (SPRING) COMPCON,US,LOS ALAMITOS, IEEE COMP. SOC. PRESS, vol. CONF. 40, 5 March 1995 (1995-03-05), pages 20-25, XP000577034 ISBN: 0-7803-2657-1 The whole document	1-19
A	SCHUNTER M ET AL: "A status report on the SEMPER framework for secure electronic commerce" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING, AMSTERDAM, vol. 30, no. 16-18, 30 September 1998 (1998-09-30), pages 1501-1510, XP004138681 ISSN: 0169-7552 2. Model for electronic commerce 3. The SEMPER framework	1-19
A	KONRAD K ET AL: "Trust and electronic commerce-more than a technical problem" PROCEEDINGS OF THE 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, PROCEEDINGS 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, LAUSANNE, SWITZERLAND, 19-22 OCT. 1999, pages 360-365, XP002162270 1999, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-0290-3 3. Trust, Security and Electronic Commerce 4. Technology and Institutions	1-19

-/-

INTERNATIONAL SEARCH REPORT

Int: Oral Application No.

PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KINI A ET AL: "Trust in electronic commerce: definition and theoretical considerations" PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (CAT. NO.98TB100216), PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, KOHALA COAST, HI, USA, 6-9 JAN. 1998, pages 51-61, XP002162271 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8255-8 1.3 The Significance of Trust in Electronic Commerce,	1-19
A	STEINAUER D D ET AL: "Trust and traceability in electronic commerce" STANDARD VIEW, SEPT. 1997, ACM, USA, vol. 5, no. 3, pages 118-124, XP002162272 ISSN: 1067-9936 The whole document	1-19
A	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) abstract	8,9
A	US 5 745 569 A (MOSKOWITZ SCOTT A ET AL) 28 April 1998 (1998-04-28) abstract	8,9

Form PCT/AS/10 (continuation of previous sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/US 00/33126

Patent document cited in search report	Publication date	Patent family number(s)	Publication date
US 5903721 A	11-05-1999	AU 6549498 A	29-09-1998
		DE 1008022 T	25-01-2001
		EP 1008022 A	14-06-2000
		ES 2150892 T	16-12-2000
		NO 994428 A	09-11-1999
		NO 9840809 A	17-09-1998
		NONE	
US 5790677 A	04-08-1998	NONE	
WO 9629795 A	26-09-1996	NO 9806198 A	12-02-1998
		CA 2215908 A	26-09-1996
		EP 0815671 A	07-01-1998
		US 5553145 A	03-09-1996
		US 5629982 A	13-05-1997
		US 5666420 A	09-09-1997
		US 6137884 A	24-10-2000
		US 6141750 A	31-10-2000
		EP 0917781 A	26-05-1999
		JP 2000515649 T	21-11-2000
WO 9724833 A	10-07-1997	US 5615269 A	25-03-1997
		AU 1951497 A	28-07-1997
US 5539735 A	23-07-1996	US 5428606 A	27-06-1995
		WO 9701892 A	16-01-1997
US 5687236 A	11-11-1997	US 5613004 A	18-03-1997
		EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
US 5745569 A	28-04-1998	AU 1829497 A	11-08-1997
		WO 9726732 A	24-07-1997

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/33126

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.: 20-185
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
 No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 20-186

In view of the large number and also the wording of the claims presently on file, which render it difficult, if not impossible, to determine the matter for which protection is sought, the present application fails to comply with the clarity and conciseness requirements of Article 6 PCT (see also Rule 6.1(a) PCT) to such an extent that a meaningful search is impossible.

Moreover, the proliferation of independent claims and the broad manner in which these have been worded make it impossible to determine which parts of the claims may be said to define subject-matter for which protection might legitimately be sought (Article 6 PCT). For these reasons, a meaningful search over the whole breadth of the claim(s) is impossible.

Consequently, the search has been restricted to the subject matter recited in claims 1-19.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

Best Available Copy



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 9016

Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Moskowitz, Scott A.

Townhouse 4, 20191 East Country Club Drive
North Miami Beach, FL 33180
ETATS-UNIS D'AMERIQUE



EPO Customer Services
Tel: +31 (0)70 340 45 00

Date
01.10.07

Reference	Application No./Patent No. 07112420.0-1228
Applicant/Proprietor Wistaria Trading, Inc.	

Designation as inventor - communication under Rule 17(3) EPC

You have been designated as inventor in the above-mentioned European patent application. Below you will find the data contained in the Designation of Inventor and further data mentioned in Art. 128(5) EPC:

DATE OF FILING . 07.06.96

PRIORITY US/07.06.95/ USA 489172

TITLE Steganographic method and device

DESIGNATED STATES AT BE CH DE DK ES FI FR GB GR IE IT LI LU MO NL PT SE

INVENTOR (PUBLISHED = 1, NOT PUBLISHED = 2):
 1/Cooperman, Marc S./ 20 Wildwood/Short Hills, NJ 07078/US
 1/Moskowitz, Scott A./ Townhouse 4, 20191 East Country Club Drive/North Miami Beach, FL 33180/US

DECLARATION UNDER ARTICLE 81 EPC:
The applicant(s) has (have) acquired the right to the European patent as employer(s).

RECEIVING SECTION



Best Available Copy

PayWord and MicroMint:
Two simple micropayment schemes

Ronald L. Rivest* and Adi Shamir**

April 27, 2001

*MIT Laboratory for Computer Science
545 Technology Square, Cambridge, Mass. 02139

**Weizmann Institute of Science
Applied Mathematics Department
Rehovot, Israel

{rivest,shamir}@theory.lcs.mit.edu

1 Introduction

We present two simple micropayment schemes, "PayWord" and "MicroMint," for making small purchases over the Internet. We were inspired to work on this problem by DEC's "Millicent" scheme [10]. Surveys of some electronic payment schemes can be found in Hallam-Baker [6], Schneier [16], and Wayne [18].

Our main goal is to minimize the number of public-key operations required per payment, using hash operations instead whenever possible. As a rough guide, hash functions are about 100 times faster than RSA signature verification, and about 10,000 times faster than RSA signature generation: on a typical workstation, one can sign two messages per second, verify 200 signatures per second, and compute 20,000 hash function values per second.

To support micropayments, exceptional efficiency is required; otherwise the cost of the mechanism will exceed the value of the payments. As a consequence, our micropayment schemes are light-weight compared to full macropayment schemes. We "don't sweat the small stuff": a user who loses a micropayment is similar to someone who loses a nickel in a candy machine. Similarly, candy machines aren't built with expensive mechanisms for detecting forged coins, and yet they work well in practice, and the overall level of abuse is low. Large-scale and/or persistent fraud must be detected and eliminated, but if the scheme delivers a volume of payments to the right parties that is roughly correct, we're happy.

In our schemes the players are brokers, users, and vendors. Brokers authorize users to make micropayments to vendors, and redeem the payments collected by the vendors. While user-vendor relationships are transient, broker-user and broker-vendor relationships are long-term. In a typical transaction a vendor sells access to a World-Wide Web page for one cent. Since a user may access only a few pages before moving on, standard credit-card arrangements incur unacceptably high overheads.

The first scheme, "PayWord," is a credit-based scheme, based on chains of "passwords" (hash values). Similar chains have been previously proposed for different purposes: by Lamport [9] and Haller (in S/Key) for access control [7], and by Winternitz [11] as a one-time signature scheme. The application of this idea for micropayments has also been independently discovered by Anderson et al. [2] and by Pederson [14], as we learned after distributing the initial draft of this paper. We discuss these related proposals further in Section 5. The user authenticates a complete chain to the vendor with a single public-key signature, and then successively reveals each password in the chain to the vendor to make micropayments. The incremental cost of a payment is thus one hash function computation per party. PayWord is optimized for sequences of micropayments, but is secure and flexible enough to support larger variable-value payments as well.

The second scheme, "MicroMint," was designed to eliminate public-key operations altogether. It has lower security but higher speed. It introduces a new paradigm of representing coins by k -way hash-function collisions. Just as for a real mint, a broker's "economy of scale" allows him to produce large quantities of such coins at very low cost per coin, while small-scale forgery attempts can only produce coins at a cost exceeding their value.

2 Generalities and Notation

We use public-key cryptography (e.g. RSA with a short public exponent). The public keys of the broker B , user U , and vendor V are denoted PK_B , PK_U , and PK_V , respectively, their secret keys are denoted SK_B , SK_U , and SK_V . A message M with its digital signature produced by secret key SK is denoted $\{M\}_{SK}$. This signature can be verified using the corresponding public key PK .

We let h denote a cryptographically strong hash function, such as MD5[15] or SHA[13]. The output (nominally 128 or 160 bits) may be truncated to shorter lengths as described later. The important property of h is its one-wayness and collision-resistance; a very large search should be required to find a single input producing a given output, or to find two inputs producing the same output. The input length may, in some cases, be equal to the output length.

3 PayWord

PayWord is credit-based. The user establishes an account with a broker, who issues her a digitally-signed PayWord Certificate containing the broker's name, the user's name and IP-address, the user's public key, the expiration date, and other information. The certificate has to be renewed by the broker (e.g. monthly), who will do so if the user's account is in good standing. This certificate authorizes the user to make Payword chains, and assures vendors that the user's paywords are redeemable by the broker. We assume in this paper that each payword is worth exactly one cent (this could be varied).

In our typical application, when U clicks on a link to a vendor V 's non-free web page, his browser determines whether this is the first request to V that day. For a first request, U computes and signs a "commitment" to a new user-specific and vendor-specific chain of paywords w_1, w_2, \dots, w_n . The user creates the payword chain in reverse order by picking the last payword w_n at random, and then computing

$$w_i = h(w_{i+1})$$

for $i = n-1, n-2, \dots, 0$. Here w_0 is the root of the payword chain, and is not a payword itself. The commitment contains the root w_0 , but not any payword w_i for $i > 0$. Then U provides this commitment and her certificate to V , who verifies their signatures.

The i -th payment (for $i = 1, 2, \dots$) from U to V consists of the pair (w_i, i) , which the vendor can verify using w_{i-1} . Each such payment requires no calculations by U , and only a single hash operation by V .

At the end of each day, V reports to B the last (highest-indexed) payment (w_l, l) received from each user that day, together with each corresponding commitment. B charges U 's account l cents and pays l cents into V 's account. (The broker might also charge subscription and/or transaction fees, which we ignore here.)

A fundamental design goal of PayWord is to minimize communication (particularly on-line communication) with the broker. We imagine that there will be only a few nationwide

brokers; to prevent them from becoming a bottleneck, it is important that their computational burden be both reasonable and "off-line." PayWord is an "off-line" scheme: V does not need to interact with B when U first contacts V , nor does V need to interact with B as each payment is made. Note that B does not even receive every payword spent, but only the *last* payword spent by each user each day at each vendor.

PayWord is thus extremely efficient when a user makes repeated requests from the same vendor, but is quite effective in any case. The public-key operations required by V are only signature verifications, which are relatively efficient. We note that Shamir's probabilistic signature screening techniques[17] can be used here to reduce the computational load on the vendor even further. Another application where PayWord is well-suited is the purchase of pay-per-view movies; the user can pay a few cents for each minute of viewing time.

This completes our overview; we now give some technical details.

3.1 User-Broker relationship and certificates

User U begins a relationship with broker B by requesting an account and a PayWord Certificate. She gives B over a secure authenticated channel: her credit-card number, her public key PK_U , and her "delivery address" A_U . Her aggregated PayWord charges will be charged to her credit-card account. Her delivery address is her Internet/email or her U.S. mail address; her certificate will only authorize payments by U for purchases to be delivered to A_U .

The user's certificate has an expiration date E . Certificates might expire monthly, for example. Users who don't pay their bills won't be issued new certificates.

The broker may also give other (possibly user-specific) information I_U in the certificate, such as: a certificate serial number, credit limits to be applied per vendor, information on how to contact the broker, broker/vendor terms and conditions, etc.

The user's certificate C_U thus has the form:

$$C_U = \{B, U, A_U, PK_U, E, I_U\}_{SK_B}$$

The PayWord certificate is a statement by B to any vendor that B will redeem authentic paywords produced by U turned in before the given expiration date (plus a day's grace).

PayWord is not intended to provide user anonymity. Although certificates could contain user account numbers instead of user names, the inclusion of A_U effectively destroys U 's anonymity. However, some privacy is provided, since there is no record kept as to which documents were purchased.

If U loses her secret key she should report it at once to B . Her liability should be limited in such cases, as it is for credit-card loss. However, if she does so repeatedly the broker may refuse her further service. The broker may also keep a "hot list" of certificates whose users have reported lost keys, or which are otherwise problematic.

As an alternative to hot-lists, one can use hash-chains in a different manner as proposed by Micali [12] to provide daily authentication of the user's certificate. The user's certificate would additionally contain the root w_0 of a hash chain of length 31. On day $j - 1$ of the month, the broker will send the user (o.g. via email) the value w_j^i if and only if the user's

account is still in good standing. Vendors will then demand of each user the appropriate w^i value before accepting payment.

3.2 User-Vendor relationships and payments

User-vendor relationships are transient. A user may visit a web site, purchase ten pages, and then move on elsewhere.

Commitments

When U is about to contact a new vendor V , she computes a fresh payword chain w_1, \dots, w_n with root w_0 . Here n is chosen at the user's convenience; it could be ten or ten thousand. She then computes her commitment for that chain:

$$M = \{V, C_U, w_0, D, I_M\}_{SK_U}$$

Here V identifies the vendor, C_U is U 's certificate, w_0 is the root of the payword chain, D is the current date, and I_M is any additional information that may be desired (such as the length n of the payword chain). M is signed by U and given to V . (Since this signature is necessarily "on-line," as it contains the vendor's name, the user might consider using an "on-line/off-line" signature scheme[5].)

This commitment authorizes B to pay V for any of the paywords w_1, \dots, w_n that V redeems with B before date D (plus a day's grace). Note that paywords are *vendor-specific* and *user-specific*; they are of no value to another vendor.

Note that U must sign a commitment for each vendor she pays. If she rapidly switches between vendors, the cost of doing so may become noticeable. However, this is PayWord's only significant computational requirement, and the security it provides makes PayWord usable even for larger "macropayments" (e.g. software selling at \$19.99).

The vendor verifies U 's signature on M and the broker's signature on C_U (contained within M), and checks expiration dates.

The vendor V should cache verified commitments until they expire at the end of the day. Otherwise, if he redeemed (and forgot) paywords received before the expiration date of the commitment, U could cheat V by replaying earlier commitments and paywords. (Actually, to defeat this attack, V need store only a short hash of each commitment he has reported to B already today.)

The user should preferably also cache her commitment until she believes that she is finished ordering information from V , or until the commitment expires. She can always generate a fresh commitment if she re-visits a vendor whose commitment she has deleted.

Payments

The user and vendor need to agree on the amount to be paid. In our exemplary application, the price of a web page is typically one cent, but could be some other amount. A web page should presumably be free if the user has already purchased it that day, and is just requesting it again because it was flushed from his cache of pages.

A payment P from U to V consists of a payword and its index:

$$P = (w_i, i)$$

The payment is short: only twenty or thirty bytes long. (The first payment to V that day would normally accompany U 's corresponding commitment; later payments are just the payword and its index, unless the previous chain is exhausted and a new chain must be committed to.) The payment is not signed by U , since it is self-authenticating (using the commitment).

The user spends her paywords in order: w_1 first, then w_2 , and so on. If each payword is worth one cent, and each web page costs one cent, then she discloses w_i to V when she orders her i -th web page from V that day.

This leads to the PayWord payment policy: *for each commitment a vendor V is paid l cents, where (w_i, l) is the corresponding payment received with the largest index.* This means that V needs to store only one payment from each user: the one with the highest index. Once a user spends w_i , she can not spend w_j for $j < i$. The broker can confirm the value to be paid for w_i by determining how many applications of h are required to map w_i into w_0 .

PayWord supports variable-size payments in a simple and natural manner. If U skips paywords, and gives w_7 after giving w_2 , she is giving V a nickel instead of a penny. When U skips paywords, during verification V need only apply h a number of times proportional to the value of the payment made.

A payment does not specify what item it is payment for. The vendor may cheat U by sending him nothing, or the wrong item, in return. The user bears the risk of losing the payment, just as if he had put a penny in the mail. Vendors who so cheat their customers will be shunned. This risk can be moved to V , if V specifies payment *after* the document has been delivered. If U doesn't pay, V can notify B and/or refuse U further service. For micropayments, users and vendors might find either approach workable.

3.3 Vendor-Broker relationships and redemption

A vendor V needn't have a prior relationship with B , but does need to obtain PK_B in an authenticated manner, so he can authenticate certificates signed by B . He also needs to establish a way for B to pay V for paywords redeemed. (Brokers pay vendors by means outside the PayWord system.)

At the end of each day (or other suitable period), V sends B a redemption message giving, for each of B 's users who have paid V that day (1) the commitment C_U received from U , (2) the last payment $P = (w_i, l)$ received from U .

The broker then needs to (1) verify each commitment received (he only needs to verify user signatures, since he can recognize his own certificates), including checking of dates, etc., and (2) verify each payment (w_i, l) (this requires l hash function applications). We assume that B normally honors all valid redemption requests.

Since hash function computations are cheap, and signature verifications are only moderately expensive, B 's computational burden should be reasonable, particularly since it is more-or-less proportional to the payment volume he is supporting; B can charge transaction or subscription fees adequate to cover his computation costs. We also note that B never needs to respond in real-time; he can batch up his computations and perform them off-line overnight.

3.4 Efficiency

We summarize PayWord's computational and storage requirements:

- The broker needs to sign each user certificate, verify each user commitment, and perform one hash function application per payment. (All these computations are off-line.) The broker stores copies of user certificates and maintains accounts for users and vendors.
- The user needs to verify his certificates, sign each of his commitments, and perform one hash function application per payword committed to. (Only signing commitments is an on-line computation.) He needs to store his secret key SK_U , his active commitments, the corresponding payword chains, and his current position in each chain.
- The vendor verifies all certificates and commitments received, and performs one hash function application per payword received or skipped over. (All his computations are on-line.) The vendor needs to store all commitments and the last payment received per commitment each day.

3.5 Variations and Extensions

In one variation, $h(\cdot)$ is replaced by $h_s(\cdot) = h(s, \cdot)$, where s is a "salt" (random value) specified in the commitment. Salting may enable the use of faster hash functions or hash functions with a shorter output length (perhaps as short as 64–80 bits).

The value of each payword might be fixed at one cent, or might be specified in C_U or M . In a variation, M might authenticate several chains, whose paywords have different values (for penny paywords, nickel paywords, etc.).

The user name may also need to be specified in a payment if it is not clear from context. If U has more than one payword chain authorized for V , then the payment should specify which is relevant.

Paywords could be sold on a debit basis, rather than a credit basis, but only if the user interacts with the broker to produce each commitment: the certificate could require that the broker, rather than the user, sign each commitment. The broker can automatically refund the user for unused paywords, once the vendor has redeemed the paywords given to him.

In some cases, for macropayments, it might be useful to have the "commitment" act like an electronic credit card order or check without paywords being used at all. The commitment would specify the vendor and the amount to be paid.

The broker may specify in user certificates other terms and conditions to limit his risk. For example, B may limit the amount that U can spend per day at any vendor. Or, B may refuse payment if U 's name is on B 's "hot list" at the beginning of the day. (Vendors can download B 's hot-list each morning.) Or, B may refuse to pay if U 's total expenditures over all vendors exceeds a specified limit per day. This protects B from extensive liability if SK_U is stolen and abused. (Although again, since C_U only authorizes delivery to A_U , risk is reduced.) In these cases vendors share the risk with B .

Instead of using *payword chains*, another method we considered for improving efficiency was to have V *probabilistically select* payments for redemption. We couldn't make this idea work out, and leave this approach as an open problem.

4 MicroMint

MicroMint is designed to provide reasonable security at very low cost, and is optimized for unrelated low-value payments. MicroMint uses *no* public-key operations at all.

MicroMint "coins" are produced by a broker, who sells them to users. Users give these coins to vendors as payments. Vendors return coins to the broker in return for payment by other means.

A coin is a bit-string whose validity can be easily checked by anyone, but which is hard to produce. This is similar to the requirements for a public-key signature, whose complexity makes it an overkill for a transaction whose value is one cent. (PayWord uses signatures, but not on every transaction.)

MicroMint has the property that generating many coins is very much cheaper, per coin generated, than generating few coins. A large initial investment is required to generate the first coin, but then generating additional coins can be made progressively cheaper. This is similar to the economics for a regular mint, which invests in a lot of expensive machinery to make coins economically. (It makes no sense for a forger to produce coins in a way that costs more per coin produced than its value.)

The broker will typically issue new coins at the beginning of each month; the validity of these coins will expire at the end of the month. Unused coins are returned to the broker at the end of each month, and new coins can be purchased at the beginning of each month. Vendors can return the coins they collect to the broker at their convenience (e.g. at the end of each day).

We now describe the "basic" variant of MicroMint. Many extensions and variations are possible on this theme; we describe some of them in section 4.2.

Hash Function Collisions

MicroMint coins are represented by *hash function collisions*, for some specified one-way hash function h mapping m -bit strings x to n -bit strings y . We say that x is a pre-image of y if $h(x) = y$. A pair of distinct m -bit strings (x_1, x_2) is called a (*2-way*) *collision* if $h(x_1) = h(x_2) = y$, for some n -bit string y .

If h acts "randomly," the only way to produce even one acceptable 2-way collision is to hash about $\sqrt{2^n} = 2^{n/2}$ x -values and search for repeated outputs. This is essentially the "birthday paradox." (We ignore small constants in our analyses.)

Hashing c times as many x -values as are needed to produce the first collision results in approximately c^2 as many collisions, for $1 \leq c \leq 2^{n/2}$, so producing collisions can be done increasingly efficiently, per coin generated, once the threshold for finding collisions has been passed.

Coins as k -way collisions

A problem with 2-way collisions is that choosing a value of n small enough to make the

broker's work feasible results in a situation where coins can be forged a bit too easily by an adversary. To raise the threshold further against would-be forgers, we propose using k -way collisions instead of 2-way collisions.

A k -way collision is a set of k distinct x -values x_1, x_2, \dots, x_k that have the same hash value y . The number of x -values that must be examined before one expects to see the first k -way collision is then approximately $2^{n(k-1)/k}$. If one examines c times this many x -values, for $1 \leq c \leq 2^{n/k}$, one expects to see about c^k k -way collisions. Choosing $k > 2$ has the dual effect of delaying the threshold where the first collision is seen, and also accelerating the rate of collision generation, once the threshold is passed.

We thus let a k -way collision (x_1, \dots, x_k) represent a coin. The validity of this coin can be easily verified by anyone by checking that the x_i 's are distinct and that

$$h(x_1) = h(x_2) = \dots = h(x_k) = y$$

for some n -string y .

Minting coins

The process of computing $h(x) = y$ is analogous to tossing a ball (x) at random into one of 2^n bins; the bin that ball x ends up in is the one with index y . A coin is thus a set of k balls that have been tossed into the same bin. Getting k balls into the same bin requires tossing a substantial number of balls altogether, since balls can not be "aimed" at a particular bin. To mint coins, the broker will create 2^n bins, toss approximately $k2^n$ balls, and create one coin from each bin that now contains at least k balls. With this choice of parameters each ball has a chance of roughly $1/2$ of being part of a coin.

Whenever one of the 2^n bins has k or more balls in it, k of those balls can be extracted to form a coin. Note that if a bin has more than k balls in it, the broker can in principle extract k -subsets in multiple ways to produce several coins. However, an adversary who obtains two different coins from the same bin could combine them to produce multiple new coins. Therefore, we recommend that a *MicroMint broker should produce at most one coin from each bin*. Following this rule also simplifies the Broker's task of detecting multiply-spent coins, since he needs to allocate a table of only 2^n bits to indicate whether a coin with a particular n -bit hash value has already been redeemed.

A small problem in this basic picture, however, is that computation is much cheaper than storage. The number of balls that can be tossed into bins in a month-long computation far exceeds both the number of balls that can be memorized on a reasonable number of hard disks and the number of coins that the broker might realistically need to mint. One could attempt to balance the computation and memory requirements by utilizing a very slow hash algorithm, such as DES iterated many times. Unfortunately, this approach also slows down the verification process.

A better approach, which we adopt, is to make most balls unusable for the purpose of minting coins. To do so, we say that a ball is "good" if the high-order bits of the hash value y have a value z specified by the broker. More precisely, let $n = t + u$ for some specified nonnegative integers t and u . If the high-order t bits of y are equal to the specified value z then the value y is called "good," and the low-order u bits of y determine the index of the bin into which the (good) ball x is tossed. (General z values are referred to merely as

"balls," and those that are not good can be thought of as having been conceptually tossed into nonexistent virtual bins that are "out of range.")

A proper choice of t enables us to balance the computational and storage requirements of the broker, without slowing down the verification process. It slows down the generation process by a factor of 2^t , while limiting the storage requirements of the broker to a small multiple of the number of coins to be generated. The broker thus tosses approximately $k2^n$ balls, memorizes about $k2^n$ good balls that he tosses into the 2^n bins, and generates from them approximately $(1/2) \cdot 2^n$ valid coins.

Remark: We note that with standard hash functions, such as MD5 and DES, the number of output bits produced may exceed the number n of bits specified in the broker's parameters. A suitable hash function for the broker can be obtained by discarding all but the low-order n bits of the standard hash function output. This discarding of bits other than the low-order n bits is a different process than that of specifying a particular value for the high-order t bits out of the n that was described above.

A detailed scenario

Here is a detailed sketch of how a typical broker might proceed to choose parameters for his minting operation for a given month. The calculations are approximate (values are typically rounded to the nearest power of two), but instructive; they can be easily modified for other assumptions.

The broker will invest in substantial hardware that gives him a computational advantage over would-be forgers, and run this hardware continuously for a month to compute coins valid for the next month. This hardware is likely to include many special-purpose chips for computing h efficiently.

We suppose that the broker wishes to have a net profit of \$1 million per month (approximately 2^{27} cents/month). He charges a brokerage fee of 10%. That is, for every coin worth one cent that he sells, he only gives the vendor 0.9 cents when it is redeemed. Thus, the broker needs to sell one billion coins per month (approximately 2^{30} coins/month) to collect his \$1M fee. If an average user buys 2500 (\$25.00) coins per month, he will need to have a customer base of 500,000 customers.

The broker chooses $k = 4$; a coin will be a good 4-way collision.

To create 2^{30} coins, the broker chooses $n = 31$, so that he creates an array of 2^{31} (approximately two billion) bins, each of which can hold up to 4 x -values that hash to an n -bit value that is the concatenation of a fixed t -bit pattern z and the n -bit index of the bin.

The broker will toss an average of 4 balls into each bin. That is, the broker will generate $4 \cdot 2^{31} = 2^{32}$ (approximately eight billion) x -values that produce good y -values. When he does so, the probability that a bin then contains 4 or more x -values (and thus can yield a coin) is about 1/2. (Using a Poisson approximation, it can be calculated that the correct value is approximately 0.56.) Since each of the 2^{31} bins produces a coin with probability 1/2, the number of coins produced is 2^{30} , as desired.

In order to maximize his advantage over an adversary who wishes to forge coins, the broker invests in special-purpose hardware that allows him to compute hash values very quickly. This will allow him to choose a relatively large value of t , so that good hash values are relatively rare. This increases the work factor for an adversary (and for the broker) by a

factor of 2^t . The broker chooses his hash function h as the low-order n bits of the encryption of some fixed value v_0 with key x under the Data Encryption Standard (DES):

$$h(x) = \{DES_x(v_0)\}_{t..n}.$$

The broker purchases a number of field-programmable gate array (FPGA) chips, each of which is capable of hashing approximately 2^{25} (approximately 30 million) x -values per second. (See [3].) Each such chip costs about \$200; we estimate that the broker's actual cost per chip might be closer to \$400 per chip when engineering, support, and associated hardware are also considered. The broker purchases 2^8 (= 256) of these chips, which costs him about \$100,000. These chips can collectively hash 2^{33} (approximately 8.6 billion) values per second. Since there are roughly 2^{21} (two million) seconds in a month, they can hash about 2^{54} (approximately 18 million billion) values per month.

Based on these estimates the broker chooses $n = 52$ and $t = 21$ and runs his minting operation for one month. Of the $k2^n = 2^{54}$ hash values computed, only one in 2^{21} will be good, so that approximately 2^{33} good x -values are found, as necessary to produce 2^{30} coins.

Storing a good $(x, h(x))$ pair takes less than 16 bytes. The total storage required for all good pairs is less than 2^{37} bytes (128 Gigabytes). Using standard magnetic hard disk technology costing approximately \$300 per Gigabyte, the total cost for storage is less than \$40,000. The total cost for the broker's hardware is thus less than \$150,000, which is less than 15% of the first month's profit.

Rather than actually writing each pair into a randomly-accessible bin, the broker can write the 2^{33} good pairs sequentially to the disk array, and then sort them into increasing order by y value, to determine which are in the same bin. With a reasonable sorting algorithm, the sorting time should be under one day.

Selling coins

Towards the end of each month, the broker begins selling coins to users for the next month. At the beginning of each month, B reveals the new validity criterion for coins to be used that month. Such sales can either be on a debit basis or a credit basis, since B will be able to recognize coins when they are returned to him for redemption. In a typical purchase, a user might buy \$25.00 worth of coins (2500 coins), and charge the purchase to his credit card. The broker keeps a record of which coins each user bought. Unused coins are returned to the broker at the end of each month.

Making payments

Each time a user purchases a web page, he gives the vendor a previously unspent coin (x_1, x_2, \dots, x_k) . (This might be handled automatically by the user's web browser when the user clicks on a link that has a declared fee.) The vendor verifies that it is indeed a good k -way collision by computing $h(x_i)$ for $1 \leq i \leq k$, and checking that the values are equal and good. Note that while the broker's minting process was intentionally slowed down by a factor of 2^t , the vendor's task of verifying a coin remains extremely efficient, requiring only k hash computations and a few comparisons (in our proposed scenario, $k = 4$).

Redemptions

The vendor returns the coins he has collected to the broker at the end of each day. The broker checks each coin to see if it has been previously returned, and if not, pays the vendor

one cent (minus his brokerage fee) for each coin. We propose that if the broker receives a specific coin more than once, he does not pay more than once. Which vendor gets paid can be decided arbitrarily or randomly by the broker. This may penalize vendors, but eliminates any financial motivation a vendor might have had to cheat by redistributing coins he has collected to other vendors.

4.1 Security Properties

We distinguish between small-scale attacks and large-scale attacks. We believe that users and vendors will have little motivation to cheat in order to gain only a few cents; even if they do, the consequences are of no great concern. This is similar to the way ordinary change is handled: many people don't even bother to count their change following a purchase. Our security mechanisms are thus primarily designed to discourage large-scale attacks, such as massive forgery or persistent double-spending.

Forgery

Small-scale forgery is too expensive to be of interest to an adversary: with the recommended choice of $k = 4$, $n = 54$, and $r = 31$, the generation of the first forged coin requires about 2^{46} hash operations. Since a standard work-station can perform only 2^{14} hash operations per second, a typical user will need 2^{31} seconds (about 80 years) to generate just one forged coin on his workstation.

Large-scale forgery can be detected and countered as follows:

- All forged coins automatically become invalid at the end of the month.
- Forged coins can not be generated until after the broker announces the new monthly coin validity criterion at the beginning of the month.
- The use of hidden predicates (described below) gives a finer time resolution for rejecting forged coins without affecting the validity of legal coins already in circulation.
- The broker can detect the presence of a forger by noting when he receives coins correspondings to bins that he did not produce coins from. This works well in our scenario since only about half of the bins produce coins. To implement this the broker need only work with a bit-array having one bit per bin.
- The broker can at any time declare the current period to be over, recall all coins for the current period, and issue new coins using a new validation procedure.
- The broker can simultaneously generate coins for several future months in a longer computation, as described below; this makes it harder for a forger to catch up with the broker.

Theft of coins

If theft of coins is judged to be a problem during initial distribution to users or during redemption by vendors, it is easy to transmit coins in encrypted form during these operations.

User/broker and vendor/broker relationships are relatively stable, and long-term encryption keys can be arranged between them.

To protect coins as they are being transferred over the Internet from user to vendor, one can of course use public-key techniques to provide secure communication. However, in keeping with our desire to minimize or eliminate public-key operations, we propose below another mechanism, which makes coins user-specific. This does not require public-key cryptography, and makes it harder to re-use stolen coins.

Another concern is that two vendors may collude so that both attempt to redeem the same coins. The recommended solution is that a broker redeem a coin at most once, as discussed earlier. Since this may penalize honest vendors who receive stolen coins, we can make coins vendor-specific as well as user-specific, as described below.

Double-spending

Since the MicroMint scheme is not anonymous, the broker can detect a doubly-spent coin, and can identify which vendors he received the two instances from. He also knows which user the coin was issued to. With the vendors' honest cooperation, he can also identify which users spent each instance of that coin. Based on all this information, the broker can keep track of how many doubly-spent coins are associated with each user and vendor. A large-scale cheater (either user or vendor) can be identified by the large number of duplicate coins associated with his purchases or redemptions; the broker can then drop a large-scale cheater from the system. A small-scale cheater may be hard to identify, but, due to the low value of individual coins, it is not so important if he escapes identification.

MicroMint does not provide any mechanism for preventing purely malicious framing (with no financial benefit to the framer). We believe that the known mechanisms for protecting against such behavior are too cumbersome for a light-weight micropayment scheme. Since MicroMint does not use real digital signatures, it may be hard to legally prove who is guilty of duplicating coins. Thus, a broker will not be able to pursue a cheater in court, but can always drop a suspected cheater from the system.

4.2 Variations

User-specific coins

We describe two proposals for making coins that are user-specific in a way that can be easily checked by vendors. Such coins, if stolen, are of no value to most other users. This greatly reduces the motivation for theft of coins.

In the first proposal, the broker splits the users into "groups," and gives each user coins whose validity depends on the identity of the group. For example, the broker can give user U coins that satisfy the additional condition $h'(x_1, x_2, \dots, x_k) = h'(U)$, where hash function h' produces short (e.g. 16-bit) output values that indicate U 's group. A vendor can easily check this condition, and reject a coin that is not tendered by a member of the correct group.

The problem with this approach is that if the groups are too large, then a thief can easily find users of the appropriate group who might be willing to buy stolen coins. On the other hand, if the groups are too small (e.g. by placing each user in his own group), the broker may be forced to precompute a large excess of coins, just to ensure that he has a large enough

supply to satisfy each user's unpredictable needs.

In the second proposal, we generalize the notion of a "collision" to more complicated combinatorial structures. Formally, a coin (x_1, \dots, x_k) will be valid for a user U if the images $y_1 = h(x_1), y_2 = h(x_2), \dots, y_k = h(x_k)$ satisfy the condition

$$y_{i+1} - y_i = d_i \pmod{2^n}$$

for $i = 1, 2, \dots, k-1$, where

$$(d_1, d_2, \dots, d_{k-1}) = h'(U)$$

for a suitable auxiliary hash function h' . (The original proposal for representing coins as collisions can be viewed as the special case where all the distances d_i 's between the k bins are zero.)

To mint coins of this form, the broker fills up most of his bins by randomly tossing balls into them, except that now it is not necessary to have more than one ball per bin. We emphasize that this pre-computation is not user-specific, and the broker does not need to have any prior knowledge of the number of coins that will be requested by each user, since each good ball can be used in a coin for *any* user. After this lengthy pre-computation, the broker can quickly create a coin for any user U by

- Computing $(d_1, \dots, d_{k-1}) = h'(U)$.
- Picking a random bin index y_1 . (This bin should have been previously unused as a y_1 for another coin, so that y_1 can be used as the "identity" of the coin when the broker uses a bit-array to determine which coins have already been redeemed.)
- Computing $y_{i+1} = y_i + d_i \pmod{2^n}$ for $i = 1, 2, \dots, k-1$.
- Taking a ball x_1 out of bin y_1 , and taking a copy of one ball out of each bin y_2, \dots, y_k . (If any bin y_i is empty, start over with a new y_1 .) Note that balls may be re-used in this scheme.
- Producing the ordered k -tuple (x_1, \dots, x_k) as the output coin.

A convenient feature of this scheme is that it is easy to produce a large number of coins for a given user even when the broker's storage device is a magnetic disk with a relatively slow seek time. The idea is based on the observation that if the y_i values for successive coins are consecutive, then so also will be the y_i values for each i , $1 < i \leq k$. Therefore, a request for 2500 new coins with $k = 4$ requires only four disk seeks, rather than 10,000 seeks: at 10 milliseconds per seek, this reduces the total seek time from 100 seconds to only 40 milliseconds.

Note that in principle coins produced for different users could re-use the same ball x_1 . Conceivably, someone could forge a new coin by combining pieces of other coins he has seen. However, he is unlikely to achieve much success by this route unless he sees balls from a significant fraction of all the bins. For example, suppose that there are 2^{31} bins, of which the forger has seen a fraction 2^{-10} (i.e., he has collected 2^{21} balls from coins spent by other users). Then the expected number of coins he can piece together from these balls that satisfy

the condition of being a good coin for himself is only $2^{21}(2^{-10})^3 = 2$. (Even if he had 1000 customers for these coins, he would expect to make only 2000 coins total, or two coins per customer on the average.) Thus, we are not too concerned about this sort of "cut-and-paste" forgery.

Vendor-specific coins

To further reduce the likelihood that coins will be stolen, the user can give coins to vendors in such a way that each coin can be redeemed only by a small fraction of the vendors. This technique makes a stolen coin less desirable, since it is unlikely to be accepted by a vendor other than the one where it was originally spent. The additional check of validity can be carried out both by the vendor and by the broker. (Having vendor-specific coins is also a major feature of the Millicent [10] scheme.)

The obvious difficulty is that neither the broker nor the user can predict ahead of time which vendors the user will patronize, and it is unreasonable to force the user to purchase in advance coins specific for each possible vendor. Millicent adopts the alternative strategy whereby the user must contact the broker in real-time whenever the user needs coins for a new vendor. (He also needs to contact the broker to return excess unused coins that are specific to that vendor.) We can overcome these problems with an extension of the user-specific scheme described above, in which the user purchases a block of "successive" MicroMint coins.

Intuitively, the idea is the following. Choose a value v (e.g. 1024) less than u . Let a u -bit bin-index y be divided into a $u-v$ -bit upper part y' and a v -bit lower part y'' . We consider that y' specifies a "superbin" index and that y'' specifies a bin within that superbin. A user now purchases balls in bulk and makes his own coins. He purchases balls by the superbin, obtaining 2^v balls per superbin with one ball in each bin of the superbin. He buys k superbins of balls for 2^u cents. A coin from user U is valid for redemption by vendor V if:

$$y'_{i+1} = y'_i + d'_i \pmod{2^{u-v}} \text{ for } i = 1, \dots, k-1,$$

and

$$y''_{i+1} = y''_i + d''_i \pmod{2^v} \text{ for } i = 1, \dots, k-1,$$

where

$$h'(U) = (d'_1, \dots, d'_{k-1})$$

and

$$h''(V) = (d''_1, \dots, d''_{k-1}).$$

The broker chooses the next available superbin as the first superbin to give the user; the other superbins are then uniquely determined by the differences $\{d'_i\}$ defined by the user's identity and the choice of the first superbin. Analogously, to make a coin for a particular vendor the user chooses a ball from the next bin from his first superbin, and must use balls from bins in the other superbins that are then uniquely determined by the differences $\{d''_i\}$ defined by the vendor's identity and the choice of the first bin. Note that balls from the first superbin are used only once, to permit detection of double-spending, whereas balls from the other superbins may appear more than once (in coins paid to different vendors), or not at all. It may be difficult for a broker to create superbins that are perfectly full even if he

throws more balls. He might sell superbins that are almost full, but then a user may have difficulty producing some coins for some vendors. To compensate, the broker can reduce the price by one cent for each empty bin sold.

Simultaneously generating balls for multiple months

Our major line of defense against large-scale forgery is the fact that the broker can compute coins in advance, whereas a forgery attempt can only be started once the new validity condition for the current month is announced. We now describe a technique whereby computing the balls for a single month's coins takes eight months, but the broker doesn't fall behind because he can generate balls for eight future months concurrently. The forger will thus have the dual problems of starting late and being too slow, even if he uses the same computational resources as the real broker.

In this method, the broker changes the monthly validity criterion, not by changing the hash function h , but by announcing each month a new value z such that ball x is good when the high-order t bits of $h(x)$ are equal to z . The broker randomly and secretly chooses in advance the values z that will be used for each of the next eight months. Tossing a ball still means performing one hash function computation, but the tossed ball is potentially "good" for any of the next eight months, and it is trivial for the broker to determine if this is the case. In contrast, the forger only knows the current value of z , and can not afford to memorize all the balls he tosses, since memory is relatively expensive and only a tiny fraction (e.g., 2^{-24} in our running example) of the balls are considered "good" at any given month.

We now describe a convenient way of carrying out this calculation. Assume that at the beginning of the month j , the broker has all of the balls needed for month j , $7/8$ of the balls needed for month $j+1$, $6/8$ of the balls needed for month $j+2$, ..., and $1/8$ of the balls needed in for month $j+7$. During month j , the broker tosses balls by randomly picking x values, calculating $y = h(x)$, and checking whether the top-most t bits of y are equal to any of the z values to be used in months $j+1, \dots, j+8$. To slow the rate at which he generates good balls for each upcoming month, he increases n and t each by three. After the month-long computation, we expect him to have all the coins he needs for month $j+1$, $7/8$ of the coins he needs for month $j+2$, and so on; this is the desired "steady-state" situation. The broker needs four times as much storage to hold the balls generated for future months, but balls for future months can be temporarily stored on inexpensive magnetic tapes because he doesn't need to respond quickly to user requests for those coins yet.

Hidden Predicates

The "hidden predicate" technique for defeating forgers works as follows. We choose $m > n$, and require each m -bit pre-image to satisfy a number of hidden predicates. The hidden predicates should be such that generating pre-images satisfying the predicates is easy (if you know the predicate). To generate an x_i , one can pick its last n bits randomly, and define the j -th bit of x_i , for $j = m-n, \dots, 1$, to be the j -th hidden predicate applied to bits $j+1, \dots, m$ of x_i . The hidden predicates must be balanced and difficult to learn from random examples. Suggestions of hard-to-learn predicates exist in the learning-theory literature. For example the parity/majority functions of Blum et al. [4] (which are the exclusive-or of some of the input bits together with the majority function on a disjoint set of input bits) are interesting, although slightly more complicated functions may be appropriate in this application when word lengths are short. With $m-n = 32$, the broker can have one hidden

predicate for each day of the month. He could reveal a new predicate each day, and ask vendors to check that the coins they receive satisfy these predicates (otherwise the coins will not be accepted by the broker). This would not affect the validity of legitimate coins already in circulation, but makes forgery extremely difficult, since the would-be forger would have to discard much of his precomputation work as each new predicate is revealed. We feel that such techniques are strongly advisable in MicroMint.

Other Extensions

Peter Wayner (private communication) has suggested a variation on MicroMint in which coins of different values are distinguished by publicly-known predicates on the x -values.

5 Relationship to Other Micropayment Schemes

In this section we compare our proposals to the Millicent[10], NetBill [1], NetCard [2], and Pedersen [14] micropayment schemes.

NetBill offers a number of advanced features (such as electronic purchase orders and encryption of purchased information), but it is relative expensive: digital signatures are heavily used and the NetBill server is involved in each payment.

Millicent uses hash functions extensively, but the broker must be on-line whenever the user wishes to interact with a new vendor. The user buys vendor-specific scrip from the broker. For applications such as web browsing, where new user-vendor relationships are continually being created, Millicent can place a heavy real-time burden on the broker. Compared to Millicent, both PayWord and MicroMint enable the user to generate vendor-specific "scrip" without any interaction with the broker, and without the overhead required in returning unused vendor-specific scrip. Also, PayWord is a credit rather than debit scheme.

Anderson, Maniavas, and Sutherland [2] have developed a micropayment system, "NetCard," which is very similar to PayWord in that it uses chains of hash values with a digitally signed root. (The way hash chains are created differs in a minor way.) However, in their proposal, it is the bank rather than the user who prepares the chain and signs the root, which adds to the overall burden of the bank. This approach prevents the user from creating new chains, although a NetCard user could spend a single chain many times. Compared to PayWord, NetCard is debit-based, rather than credit-based. We have heard that a patent has been applied for on the NetCard system.

Torben Pedersen outlines a micropayment proposal[14] that is also based on hash chains. His motivating application was for incremental payment of telephone charges. His paper does not provide much detail on many points (e.g. whether the system is credit or debit-based, how to handle exceptions, whether chains are vendor-specific, and other auxiliary security-related matters). The CAFE project has filed for a patent on what we believe is an elaboration of Pedersen's idea. (The details of the CAFE scheme are not available to us.)

Similarly following Pedersen's exposition, the iKP developers Hausser, Steiner, and Waidner have independently adopted a similar approach [8].

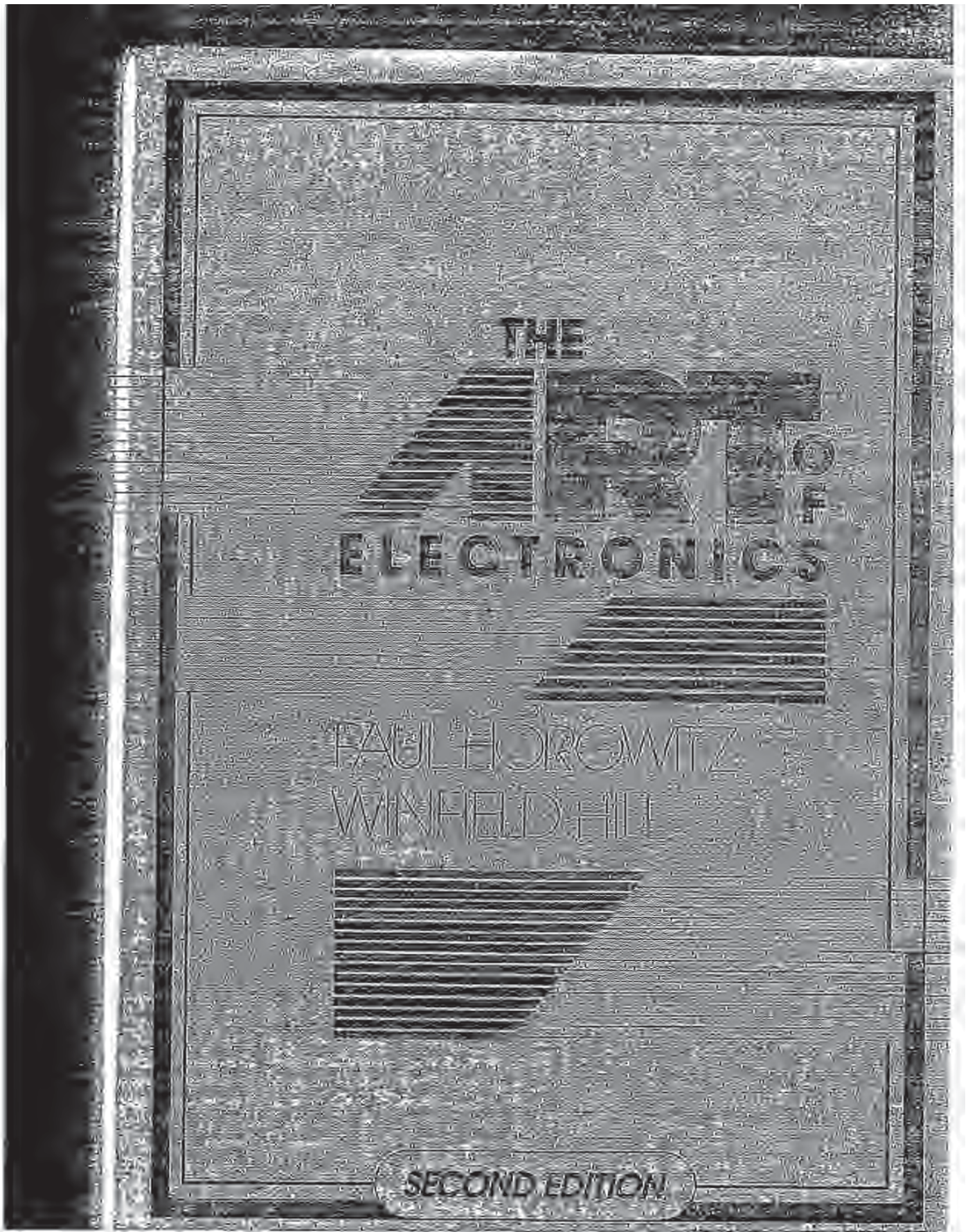
6 Conclusions and Discussion

We have presented two new micropayment schemes which are exceptionally economical in terms of the number of public-key operations employed. Furthermore, both schemes are *off-line* from the broker's point of view.

References

- [1] The NetBill Electronic Commerce Project, 1995. <http://www.inl.cmu/NETBILL/home.html>.
- [2] Ross Anderson, Harry Maniavas, and Chris Sutherland. A practical electronic cash system, 1995. Available from author: Ross.Anderson@cl.cam.ac.uk.
- [3] Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener. Minimal key lengths for symmetric ciphers to provide adequate commercial security: A report by an ad hoc group of cryptographers and computer scientists, January 1996. Available at <http://www.bsa.org>.
- [4] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *Proc. CRYPTO 99*, pages 278–291. Springer, 1994. Lecture Notes in Computer Science No. 773.
- [5] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. In G. Brassard, editor, *Proc. CRYPTO 89*, pages 263–277. Springer-Verlag, 1990. Lecture Notes in Computer Science No. 435.
- [6] Philip Hallam-Baker. W3C payments resources, 1995. <http://www.w3.org/hypertext/WWW/Payments/overview.html>.
- [7] Neil M. Haller. The S/KEY one-time password system. In *ISOC*, 1994.
- [8] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-Payments based on IKP, December 17, 1995. Available from authors: sti@zurich.ibm.com.
- [9] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–771, November 1981.
- [10] Mark S. Manasse. Millicent (electronic microcommerce), 1995. http://www.research.digital.com/SRC/personal/Mark_Manasse/uncommon/ucom.html.
- [11] Ralph C. Merkle. A certified digital signature. In G. Brassard, editor, *Proc. CRYPTO 89*, pages 218–238. Springer-Verlag, 1990. Lecture Notes in Computer Science No. 435.
- [12] Silvio Micali. Efficient certificate revocation. Technical Report TM-542b, MIT Laboratory for Computer Science, March 22, 1996.

- [13] National Institute of Standards and Technology (NIST). *FIPS Publication 180: Secure Hash Standard (SHS)*, May 11, 1993.
- [14] Torben P. Pedersen. Electronic payments of small amounts. Technical Report DAIMI PB-495, Aarhus University, Computer Science Department, Århus, Denmark, August 1995.
- [15] Ronald L. Rivest. The MD5 message-digest algorithm. Internet Request for Comments, April 1992. RFC 1321.
- [16] Bruce Schneier. *Applied Cryptography (Second Edition)*. John Wiley & Sons, 1996.
- [17] Adi Shamir. Fast signature screening. CRYPTO '95 rump session talk; to appear in RSA Laboratories' *CryptoBytes*.
- [18] Peter Wayner. *Digital Cash: Commerce on the Net*. Academic Press, 1996.



Some more home-grown philology: There is a tendency among beginners to want to compute resistor values and other circuit component values to many significant places, and the availability of inexpensive calculators has only made matters worse. There are two reasons you should try to avoid falling into this habit: (a) the components themselves are of finite precision (typical resistors are $\pm 5\%$; the parameters that characterize transistors, say, frequently are known only to a factor of two); (b) one mark of a good recent design is insensitivity of the finished circuit to precise values of the components (there are exceptions, of course). You'll also learn circuit intuition more easily if you get into the habit of doing approximate calculations in your head, rather than watching meaningless numbers pop up on a calculator display.

In trying to develop intuition about resistance, some people find it helpful to think about *conductance*, $G = 1/R$. The current through a device of conductance G bridging a voltage V is then given by $I = GV$ (Ohm's law). A small resistance is large conductance, with correspondingly large current under the influence of an applied voltage.

Viewed in this light, the formula for parallel resistors is obvious: When several resistors or conducting paths are connected across the same voltage, the total current is the sum of the individual currents. Therefore the net conductance is simply the sum of the individual conductances, $G = G_1 + G_2 + G_3 + \dots$, which is the same as the formula for parallel resistors derived earlier.

Engineers are fond of defining reciprocal units, and they have designated the unit of conductance the siemens ($S = 1/\Omega$), so known as the mho (that's ohm spelled backward, given the symbol Ω). Although the concept of conductance is helpful in developing intuition, it is not used widely; most people prefer to talk about resistance instead.

Power in resistors

The power dissipated by a resistor (or any other device) is $P = IV$. Using Ohm's law, you can get the equivalent forms $P = I^2R$ and $P = V^2/R$.

EXERCISE 15

Show that it is not possible to exceed the power rating of a 1/4 watt resistor of resistance greater than 1k, no matter how you connect it, in a circuit operating from a 15 volt battery.

EXERCISE 16

Optional exercise: New York City requires about 10^{10} watts of electrical power, at 110 volts (this is plausible: 10 million people averaging 1 kilowatt each). A heavy power cable might be an inch in diameter. Let's calculate what will happen if we try to supply the power through a cable 1 foot in diameter made of pure copper. Its resistance is $0.05\mu\Omega$ (5×10^{-8} ohms) per foot. Calculate (a) the power lost per foot from " I^2R losses," (b) the length of cable over which you will lose all 10^{10} watts, and (c) how hot the cable will get. If you know the physics involved ($\sigma = 6 \times 10^{-12} \text{ W/}^\circ\text{K}^4\text{cm}^2$).

If you have done your computations correctly, the result should seem proposterous. What is the solution to this puzzle?

Input and output

Nearly all electronic circuits accept some sort of applied *input* (usually a voltage) and produce some sort of corresponding *output* (which again is often a voltage). For example, an audio amplifier might produce a (varying) output voltage that is 100 times as large as a (similarly varying) input voltage. When describing such an amplifier, we imagine measuring the output voltage for a given applied input voltage. Engineers speak of the *transfer function* H , the ratio of (measured) output divided by (applied) input; for the audio amplifier above, H is simply a constant ($H = 100$). We'll get to amplifiers soon enough, in the next chapter. However, with just resistors we can already look at a very important circuit fragment, the *voltage divider* (which you might call a "de-amplifier").

Digital watermarking

J.-F. Delaigle, C. De Vleeschouwer, B. Macq

Laboratoire de Télécommunications et Télédétection
Université catholique de Louvain
Bâtiment Stévin - 2, place du Levant
B-1348 Louvain-la-Neuve
Tel.: +32 10 47.80.72 - Fax: +32 10 47.20.89
E-mail: delaigle@tele.ucl.ac.be

ABSTRACT

This paper presents a process able to mark digital pictures with an invisible and undetectable *secrete* information, called the watermark. This process can be the basis of a complete copyright protection system. The process first step consists in producing a *secrete* image. The first part of the secret resides in a basic information that forms a binary image. That picture is then frequency modulated. The second part of the secret is precisely the frequencies of the carriers. Both secrets depends on the identity of the copyright owner and on the original picture contents. The obtained picture is called the stamp. The second step consists in modulating the amplitude of the stamp according to a masking criterion stemming from a model of human perception. That too theoretical criterion is corrected by means of morphological tools helping to locate in the picture the places where the criterion is supposed not to match. This is followed by the adaptation of the level of the stamp at that places. The so formed watermark is then added to the original to ensure its protection. That watermarking method allows the detection of watermarked pictures in a stream of digital images, only with the knowledge of the picture owner's secrets.

Keywords: copyright protection, watermark, *secrete* key, masking, human vision model, perceptive components, morphology, robustness, detection, correlation.

1 GENERAL INTRODUCTION

With the increasing availability of digitally stored information and the development of new multimedia services, security questions are becoming even more urgent. The acceptance of new services depends on whether suitable techniques for the protection of the work providers' interests are available.¹

Moreover the nature of digital media threatens its own viability:

- * First the replication of digital works is very easy and, what is more dangerous, really perfect: The copy is identical to the original.

- The ease of transmission and multiple uses is very worrying, too. Once a single pirate copy has been made, it is instantaneously accessible to anyone who wants it, without any control of the original picture owner.
- Eventually the plasticity of digital media is a great menace. Any malevolent user (*a pirate*) can modify an image at will. Such manipulations are really easy for a pirate and put many copyright protection methods at risk.

According to these considerations the conception of a copyright protection system is really vital and it constitutes a great challenge, because it should cope with all these threats. Without watermarking, most authors will not dare to broadcast their work.

This paper presents an additive watermarking technique. It consists in producing a synthetic picture (also called the stamp) which holds informations about the ownership of the original image and depends on the picture contents. That stamp is added to the original in a way that resulting picture is perceptually identical to the original one and so that the stamp is undetectable by a pirate computer. The aim of that technique is not the authentication of the picture content nor the identification of the owner. It is to allow a controller (i.e. the owner's computer or a Trusted Third Part) to find out watermarked pictures in a stream of images with the knowledge of the owner's secret key in order to detect broadcast of illegal copies.

The most interesting part of that method is the embedding process i.e. the weighting of each pixels of the stamp before adding it to the original. This is based on the masking concept coming from a model of human vision (the perceptive model). From this concept was deduced a method which reveals itself actually efficient. Another interesting part is the presentation of two methods used for the detection of watermarked pictures without the original. This last point is fundamental for the management of the copyright protection. Eventually this paper ends with the analyse of the results and the system robustness.

2 THE MASKING

2.1 Introduction

The aim of a watermarking technique is to provide an invisible embedding of a secret information, the watermark. This watermark must be masked (hidden) by the picture it is inlayed in. Precisely a master thesis has lead to a masking criterion deduced from physiological and psychophysic studies.² Nevertheless, this theoretical criterion having been formulated for monochromatic signals, it had to be adapted to suit real images.

2.2 The perceptive model: approximation of the eye functioning

It is now admitted that the retina of the eye splits an image in several components. These components circulate from the eye to the cortex by different tuned channels, one channel being tuned to one component.

The characteristics of one component are:

- the location in the visual field (in the image).
- the spatial frequency (in the Fourier domain: the amplitude in polar coordinates)
- the orientation (in the Fourier domain: the phase in polar coordinates)

So, one perceptive channel can only be excited by one component of a signal whose characteristics are tuned to its. Components that have different characteristics are independent.

2.3 The masking concept

According to perceptive model of human vision,³ signals that have same (near) components take the same channels from the eye to the cortex. It appears that such signals interact and are submitted to non-linear effects. The masking is one of those effects.

Definition: *the detection threshold* is the minimum level below which a signal can not be seen.

Definition: *the masking* occurs when the detection threshold is increased because of the presence of another signal.

In other words, there is masking when a signal can not be seen because of another with near characteristics and at a higher level.

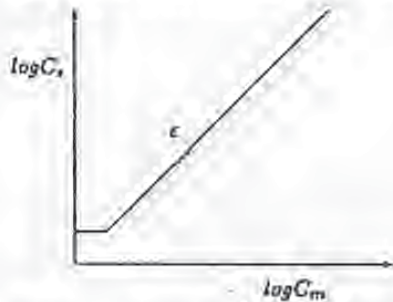
2.4 The masking model

With the object of modalizing the masking phenomenon, tests have been made on monochromatic signals, also called *gratings*. It appears that the eye is sensitive to the contrast of those gratings. This contrast is defined by:

$$C = \frac{2(L_{max} - L_{min})}{L_{max} + L_{min}} \quad (1)$$

where L is the luminance.

It is possible to determine experimentally the detection threshold of one signal of contrast C_s with respect to the contrast C_m of the masking signal. That threshold can be modalized as follows:



Such bilogarithmic curves are traced for signals of one single frequency and one orientation (f_0, θ_0). The expression of the detection threshold is thus:

$$C_s = \max[C_0, C_0 \left(\frac{C_m}{C_0}\right)^\epsilon] \quad (2)$$

where ϵ (the slope) depends on $[f_0, \theta_0]$, typically, $0.6 \leq \epsilon \leq 1.1$.

It is possible to extend that expression to introduce frequency dependence. The general expression of the detection threshold is becomes:

$$C_s(C_m, f, \theta) = C_0 + k_{(f_0, \theta_0)}(f, \theta)[C_{s(f_0, \theta_0)}(C_m) - C_0] \quad (3)$$

where:

$$k_{(f_0, \theta_0)}(f, \theta) = \exp\left[-\left(\frac{\log^2\left(\frac{f}{f_0}\right)}{F^2(f_0)} + \frac{(\theta - \theta_0)^2}{\Theta^2(f_0)}\right)\right] \quad (4)$$

In that expression, f_0 and θ_0 are relevant to the masking signal, f and θ are relevant to the masked signal, $F(f_0)$ and $\Theta(f_0)$ are parameters that represent the spreading of the Gaussian function, C_0 is often negligible. The spread of the gaussian function depends upon the frequency f_0 : For frequency, typical bandwidth at half response are 2,5 octaves at 1 c/d and 1,5 octaves at 16 c/d with a linear decrease between both frequencies.⁴ For orientation, half bandwidth at half response depends on f_0 and it takes typical values like 30 degrees at 1 c/d and 15 degrees at 16 c/d.⁵

After this expression, the frequency dependence of the detection threshold has a Gaussian form. Only near frequency signals can interact. When the frequency of the masking signal (the mask) is far from this of the signal to mask, the detection threshold is almost equal to C_0 .

2.5 The masking criterion

It is important to notice that those results concern only gratings signals. To deduce a masking criterion that will apply to signals like real images, the preceding masking condition has to be adapted. So, it is necessary to define a new concept able to take the place of the contrast, because the contrast is not define for real images. That new concept,² is the *local energy*.

The local energy is defined on narrowband signals centered around one frequency and one orientation. A picture which is a broadband signal is first filtered by Gabor narrowband filters, whose characteristics are near to human perception. The local energy around one frequency and one orientation is calculated following the scheme presented in this figure:



The masking criterion: If the local energy of one picture is less than the local energy of the mask, around all the frequencies (f_0, θ_0) and for each pixel (x, y) , then one can say that the picture is masked by the mask. Strictly, a picture is masked by a mask if $\forall(x, y)$ and $\forall(f_0, \theta_0)$, $E_{mask}(f_0, \theta_0)(x, y) \geq E_{picture}(f_0, \theta_0)(x, y)$. For real images, a good approximation of this criterion can be obtained by using a bank of filters whose central frequencies correspond to independent components and which are spread on all the Fourier space. It is admitted that 4 or 5 frequencies and 4 to 9 orientations are sufficient. The standard choice is twenty filters (5 frequencies and 4 orientations).



Figure 1: Example of basic information used

2.6 Conclusion

This section has led to the expression of an easily implementable masking criterion applicable to any image. But this criterion is only an extension of a theoretic criterion applicable to monochromatic signals. Thus cases where that criterion does not match are possible.

3 PRINCIPLE OF THE SYSTEM

3.1 Basic information of the watermark

This information is a binary picture looking like a modified checkerboard (figure 1). As explained later, the pixels value of the square forming that picture can correspond to a binary sequence deduced from the copyright owner's (CO) *secrete key*.

3.2 The stamp

In order to take advantage of the eye behaviour, the basic information is modulated at different frequencies and orientations corresponding to rather independent components. Moreover, we take care to filter the initial checkerboard with a low pass filter (LPF) (i.e. a Butterworth LPF) so that the resulting signal is bandlimited. This point is very important because it permits to limit the verification of the masking criterion in the corresponding channel.

The position of the modulating carriers is *secrete*. It can be deduced from CO's *secrete key*. In practice, the frequency plan is divided into sectors. Each sector is relevant to one perceptive component and defined a group of couples (f, θ) where basic information can be modulated. Only one couple is chosen for each sector (because couples of a same sector don't stimulate independent components). The picture obtained from the sum of each modulated grid is called *the stamp* $S(x, y)$.

$$S(x, y) = \sum_{j \in K} G(x, y) \cdot \cos(f_{x_j} \cdot x + f_{y_j} \cdot y) \quad (5)$$

K represents the set of sectors and (f_{x_j}, f_{y_j}) correspond to the couple chosen in sector j (this couple is designed by the CO's *secrete key*).

3.3 The position of the process in a global copyright scheme

The process should be placed in a copyright protection scheme like drawn at figure 2. The skeletization function consists in an image processing program extracting essential characteristics from an image. The result is a bitstream. This must be followed by a *hash-function*⁵ whose result is a succession of blocks of bits. Every block has the same length. The skeletization function gives the same result for two near images (i.e. original image and watermarked image). But the H-function always gives different results from different bitstreams as inputs. So, the inscription keys will be different for perceptually distinct pictures. After the H-function, the ciphering function is a trapdoor function.⁶ Thanks to this function the inscription keys used to deduce the basic grid and the position of the carriers depends on the CO's secret key. The aim of the use of a trapdoor function is to prevent someone from reproducing the same inscription keys with the knowledge of the H-function result. But it is possible for anyone to inverse that trapdoor function and to find the H-function result from the inscription keys. It can be interesting in a proof procedure.

4 IMPLEMENTATION

4.1 Inscription

The purpose of the inscription is to adapt the level of each part of the stamp (for all frequencies) to make it invisible once added to the picture. As mentioned above, each part of the stamp is narrow band. Inscriptions at different frequencies are thus independent and one can treat the different components of the stamp one at a time. For each frequency designed by the inscription keys, the procedure is divided in three steps : the modulation, the regulation of the level and the correction.

- Modulation

The first step consists in the modulation of the particular carrier by the lowpass grid $G(x, y)$. The result is $G(x, y) \cdot \cos(f_{x_j} x + f_{y_j} y)$, where f_{x_j} and f_{y_j} are the carrier position.

- Regulation of the level

According to the perceptual model, in order to guarantee the invisibility of the watermark its local energy has to be inferior to the picture local energy for each pixel around the inscription frequency. A way to reach this objective is to multiply the modulated grid by a weighting mask $Weight_j(x, y)$ reducing the amplitude of the stamp where energy in the corresponding component of the original picture is weak. Nevertheless, one must take care to keep the narrow band characteristic of the resulting signal $S_j(x, y)$ ($= Weight_j(x, y) \cdot G(x, y) \cdot \cos(f_{x_j} x + f_{y_j} y)$) in order to avoid non linear interactions between different parts of the stamp. In conclusion, $\forall j$, we have to find a signal $Weight_j(x, y)$ so that:

- $\forall(x, y) E_{S_j}(x, y) < E_{I,(f_{x_j}, f_{y_j})}(x, y)$
- S_j is narrow band

For simplification, lets consider $Weight_j(x, y)$ be composed of two factors:

- α_j , a constant factor (fixing the global level of the stamp).
- $M_j(x, y)$, a mask whose values $\in [0, 1]$.

When α_j is chosen, the way to find $M_j(x, y)$ so that $Weight_j(x, y)$ satisfy the conditions defined above is the following:

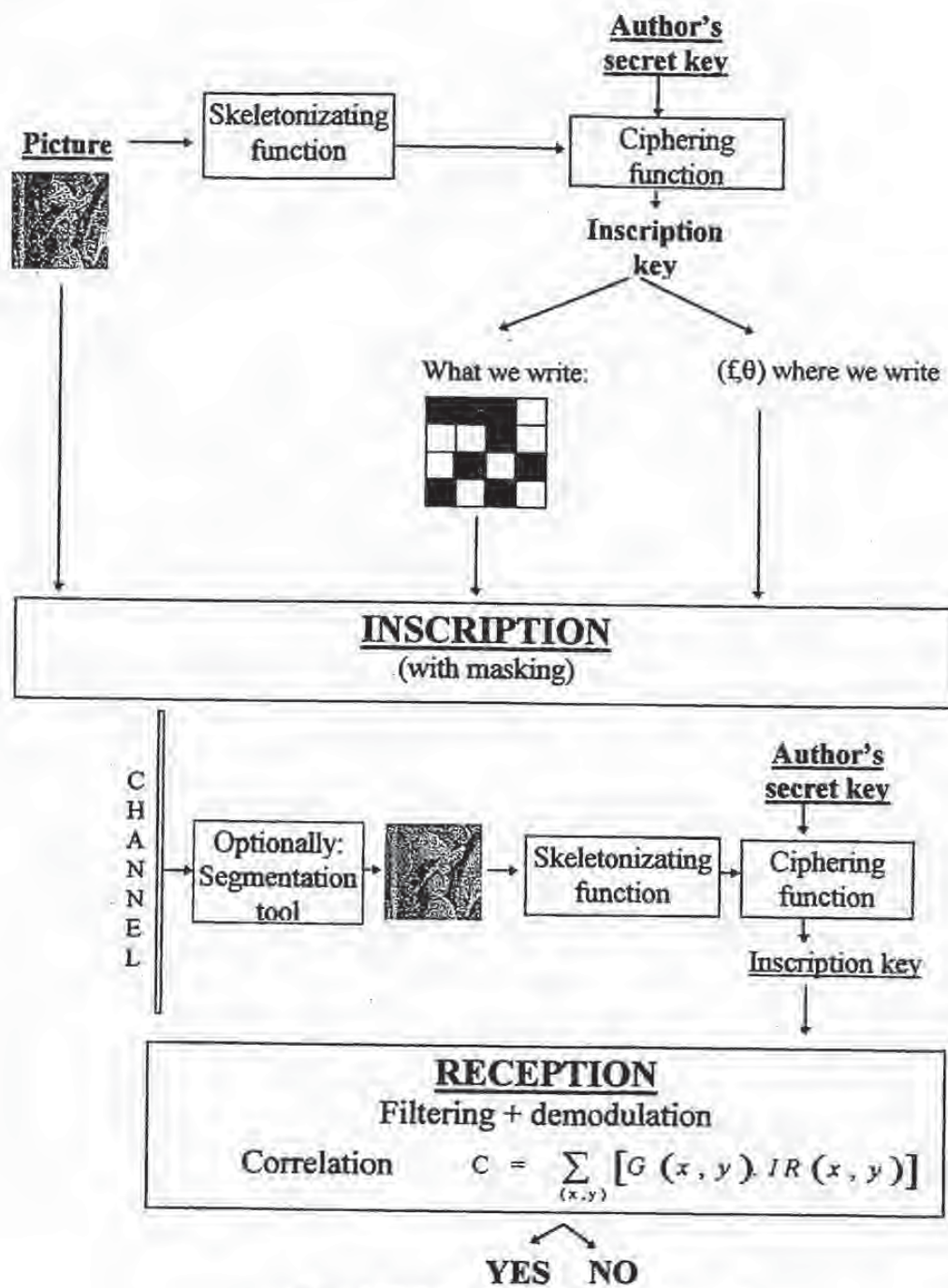


Figure 2: Global scheme for copyright protection

- Firstly, $M_j(x, y)$ is a binary mask. $M_j(x, y) = 1$ when the local energy of the stamp permits the masking and $M_j(x, y) = 0$ when the local energy of the stamp is too important. It is obvious that the initial choice of α_j has a direct influence on $M_j(x, y)$. Indeed, a great α_j value will lead to put most of the $M_j(x, y)$ values to zero, while a small α_j value will lead to keep most of $M_j(x, y)$ values at one.
- Secondly, $Weight_j(x, y)$ is filtered so that the stamp remains narrow band.
- After this second step, one has found a signal $\alpha_j M_j(x, y) G(x, y)$ which is better masked than $\alpha_j G(x, y)$. In order to really satisfy the masking criterion $V(x, y)$, this procedure must be repeated iteratively, taking $M_j(x, y) G(x, y)$ as new $G(x, y)$. Experiments have shown that only two iterations are sufficient to have a result satisfying the masking criterion everywhere.

One important question remains: how to choose α_j ?

It has already been said that the more α_j increases, the more $M_j(x, y)$ has points equal to zero. A trade off has to be found by means of a defined criterion. Maximizing the correlation at the detection (by maximizing $\sum \alpha_j M_j(x, y) G(x, y)$) could have been a good criterion, but such a criterion often tends to impose an optimum with a lot of points equal to zero and a small number of points with a great value. The addition of the so obtained watermark generally entails a degradation of the picture quality. This emphasizes the lack of the masking criterion used.

As mentioned in section 2.6, the invisibility criterion used here is an extension for real images. It appears that this extension entails some imperfections. This criterion being insufficient, some improvements have been brought thanks to experimental results.

The conclusion of these observations is that the invisibility is only strictly observed in high activity regions, where the local energy of high frequencies is important. These regions have to be favoured during the inscription in the sense that the level of the watermark will be increased in those regions while it has to be decreased in other regions.

The correction process first isolates the high activity regions (figure 3.a). Then, an homogenization of this picture is performed by use of morphological tools, e.g. one opening and one closing (figure 3.b). After a leveling (in fact, a division by the mean or mean square value of the homogenized mask), we obtain a new mask used to multiply the picture local energy and so, giving an advantage to regions of high frequency energy in comparison with other areas. After that correction, the process is identical to the one described previously. Moreover, the complexity is not increased. Indeed, we first work on the inscription at high frequencies (where there is no quality problems). The value of high frequency local energy is then used for the calculation of the correcting mask used for inscription at lower frequencies. The correction scheme is drawn in the following schema.



4.2 Detection

The aim is to detect if a watermark has been embedded. This can be done with the use of a correlation, but first it is necessary to isolate the watermark and then to demodulate it in order to reconstruct something that is highly correlated with the basic information (the grid).

The formulation of the watermark is:

$$W(x, y) = \sum_{j \in K} A_j \cos(f_{x_j} x + f_{y_j} y) \quad (1)$$

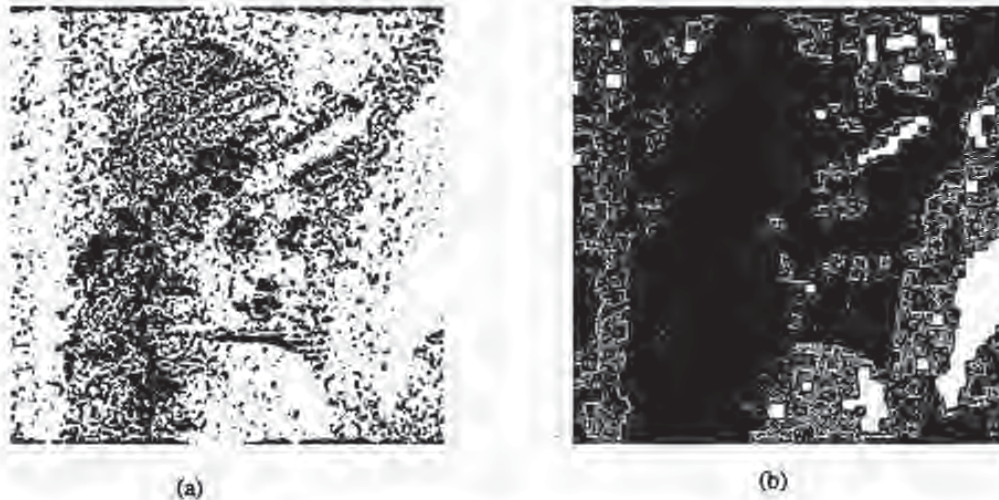


Figure 3: Correcting mask for Lena: (a) Areas of high frequencies, (b) Morphological homogeneity of the mask.

$$\text{where } A_j = \alpha_j \cdot G(x, y) \cdot M(x, y) \quad (7)$$

In this expression, $M(x, y)$ adjusts the level of the grid in order it becomes invisible, it is called a mask, and its maximal value is one.

α_j is a constant that used to normalize the mask, it must be as high as possible.

The detection is divided in three steps : teh demodulation, the correlation and the decision.

- Demodulation

$$I_W(x, y) = \sum_{j \in K} A_j \cdot \cos(f_{x_j} \cdot x + f_{y_j} \cdot y) + I_O + N(x, y) \quad (8)$$

where $I_W(x, y)$ is the watermarked picture, $I_O(x, y)$ is the original picture and $N(x, y)$ is an additive noise from the channel.

The demodulation consists in multiplying I_W by $\cos(f_{x_j} \cdot x + f_{y_j} \cdot y), \forall j \in K$ and then to filter with a LP filter.

The result will be :

$$D_j(x, y) = \frac{1}{2} \cdot A_j(x, y) + N^*(x, y) \quad (9)$$

$N^*(x, y)$ depends on the image and on the additive noise. The other parts of the stamp will be eliminated by the LP filter.

- Correlation It consists in multiplying the demodulated information $D(x, y) = \sum_{j \in K} D_j(x, y)$ with the basic grid $G(x, y)$. If the picture has not been too deteriorated, $D(x, y)$ and $G(x, y)$ should be similar.

$$C = \sum_{j \in K} \sum_{x, y} D_j(x, y) \cdot G(x, y) \quad (10)$$

$$= \sum_{j \in K} \alpha_j \sum_{x,y} [G^2(x,y) \cdot M_j(x,y) + G(x,y) \cdot N^*(x,y)] \quad (11)$$

In 11, the first term is even greater than the second, because G and N^* have null average values. So C exclusively depends on the watermark value. In the case the grid is not the good one, the correlation gives:

$$C^* = \sum_{j \in K} \alpha_j \sum_{x,y} G(x,y) \cdot G^*(x,y) \cdot M_j(x,y) \quad (12)$$

$C^* \ll C$ if the choice of the basic information has been appropriate.

- decision

The detection algorithm performs demodulations and correlations at diverse frequencies and with diverse grids. The decision is made after the comparison of these correlations.

5 RESULTS

The first and probably mostly important result is the invisibility of the stamp in all images that were tested. Figure 4.a and b compares the original and stamped picture for Lena. In figure 4.e, one observes the watermark that was added to the original picture.

Two methods were used to determine whether an image is watermarked or not. The first one consists in comparing the result of C the correlation made with the right grid $G(x,y)$ from the right key with C^* the correlation made with $G^*(x,y)$, the grid obtained by random keys see 12. If the picture is watermarked, the correlation with the right key is even greater than the random correlations. The results below (Figure 5) show the pertinence of this method.

The second method uses a grid $G(x,y)$ formed from a MLS sequence, having good correlation properties. Correlations are made with shifted versions of the basic grid. Due to these good correlation properties, the correlation with the the right grid gives a result even greater than the correlations with shifted grids. Results are presented below (figure 4.c and d), if a picture is watermarked, a pick appears in the center.

6 SYSTEM ROBUSTNESS

Many tests have been performed concerning usual pictures deteriorations in image processing like blurring and compression. The inspection of these results are quite satisfying, but expected due to the frequency approach. For all classical pirate attacks like zoom, cropping, overwatermarking it is not as simple. The overwatermarking makes no problem, the presence of the watermark is still detected. But for zoom and cropping, the remaining point is to find a few tools permitting to complete the process. The concept of these tools is already defined but yet no implementation has been achieved.⁷

7 CONCLUSION

The process developed here allows the watermarking of the ownership of any picture. The perceptual approach used here is probably the best one, that is why the results obtained are so satisfying compared with other methods and this method is so performant. Nevertheless studies are still running to achieve a new goal, consisting in

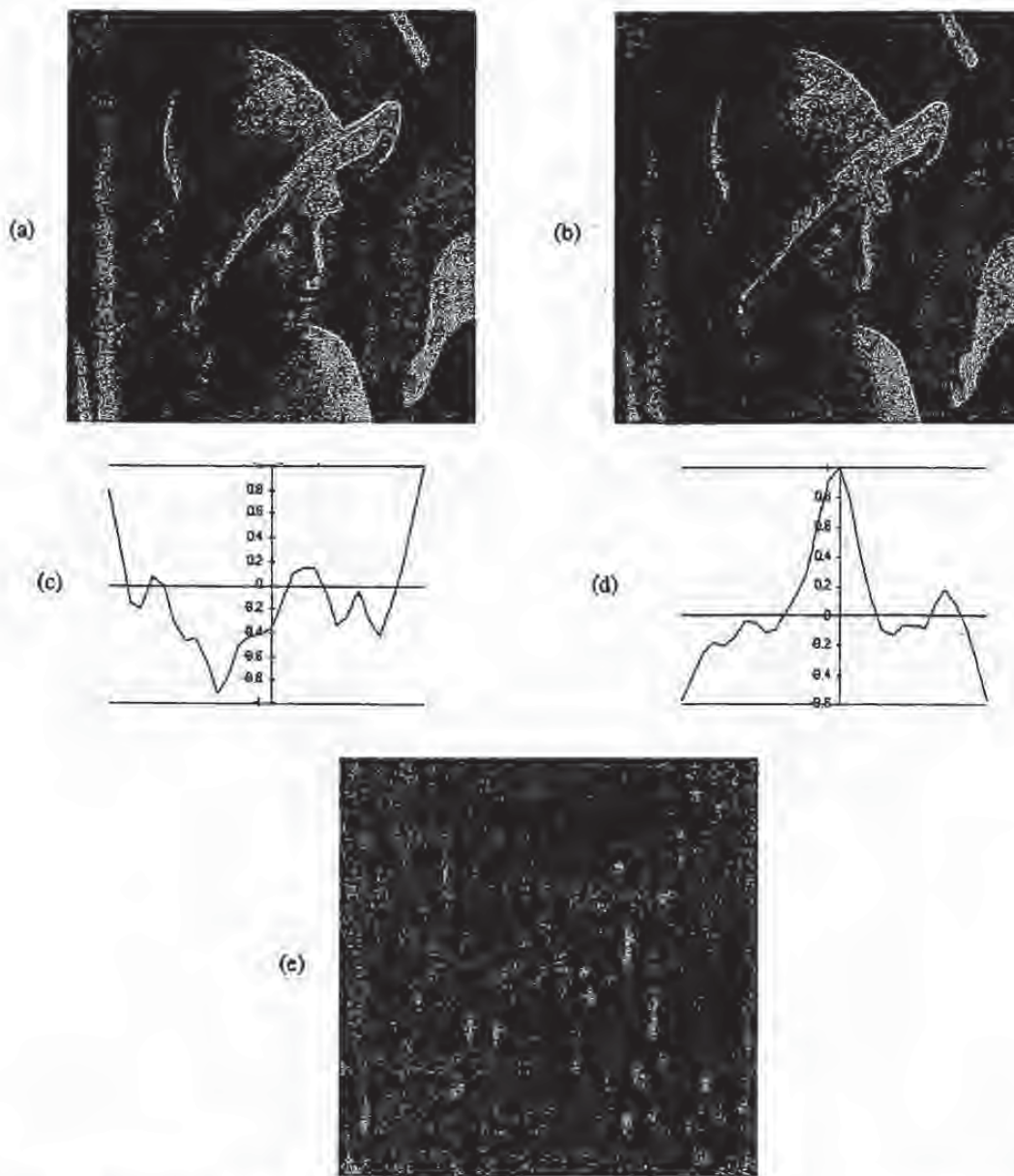


Figure 4: Results for Lena: (a) Original, (b) Watermarked one, (c) Correlation graphic for original, (d) Correlation graphic for watermarked, (e) Watermark.

Image Name	Optimal correlation	Random correlation 1	Random correlation 2	Random correlation3	Random correlation 4	Conclusion
Lena watermarked	584609	92605	133920	80534	143633	<i>watermarked</i>
Lena original	94538	98099	135492	76739	137120	<i>Non watermarked</i>

Figure 5: Results of correlation for Lena and decision.

making more information (e.g. ownership, date of marking) readable by the key owner from the watermark. This could be useful for real copyright protection protocols^{9, 8}.

8 REFERENCES

- [1] Kahin B. The strategic environment for protecting multimedia. volume 1, pages 1-8. IMA Intellectual Property Project Proceedings, January 1994.
- [2] Comes S. *Les traitements perceptifs d'images numérisées*. PhD thesis, Université Catholique de Louvain, June 1995.
- [3] Ohsak L.A. and Thomas J.P. Handbook of perception and human performance vol.1: Seeing spatial patterns. chapter 7.
- [4] G.C. Phillips H.R. Wilson, D.K. McFarlane. Spatial frequency tuning of orientation selective units estimated by oblique masking. *Vision Research*, 23(9):873-847, 1983.
- [5] G.C. Phillips H.R. Wilson. Orientation bandwidths of spatial mechanisms measured by masking. *J. Opt. Soc. Am. A*, 1(2):226-232, February 1984.
- [6] Edited by Gustavus J. Simmons. Section 1: Chapter 4: 'public key cryptography' and section 2: Chapter 6: 'authentication: Digital signature' from 'contemporary cryptology: the science of information integrity' IEEE press. 1992.
- [7] J.F. Delaigle and C. De Vleeschouwer. Etiquetage d'images numériques en vue de la protection des droits d'auteur, Juin 1995.
- [8] J.F. Delaigle C. Simon and B. Macq. Talisman (ac019): Technical state of the art. January 1996.
- [9] O. Bruyndonckx J.M. Boucqueau and B. Macq. Watermarking: workpackage 5 of accopi. June 1995.

A ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION

Marc Schneider and Shih-Fu Chang

Columbia University
Image and Advanced Television Laboratory
Room 801 Schapiro Research Building
530 West 120th Street
New York, NY 10027-6699
USA
E-mail: {mars, sfchang}@ctr.columbia.edu

Abstract

A methodology for designing content based digital signatures which can be used to authenticate images is presented. A continuous measure of authenticity is presented which forms the basis of this methodology. Using this methodology signature systems can be designed which allow certain types of image modification (e.g. lossy compression) but which prevent other types of manipulation. Some experience with content based signatures is also presented.

The idea of signature based authentication is extended to video, and a system to generate signatures for video sequences is presented. This signature also allows smaller segments of the secured video to be verified as unmanipulated.

1.0 Motivation

Powerful, and easy to use image manipulation software has made it possible to alter digital images. It has been suggested that the authenticity of digital images can be preserved by having a camera "sign" the image using a digital signature. [1] However, applying a signature scheme directly to the image has some drawbacks. For many applications, image compression is desired to reduce transmission bandwidth, storage space, etc. Authenticity, the ability to detect image manipulation, is also desired. These two functions are at odds with each other since lossy compression is a form of manipulation. Our goal is to develop a way to be able to prove some form of authenticity, while still allowing desired forms of manipulation, such as lossy compression. Ideally, a robust signature scheme should not declare an image modified under these circumstances.

2.0 Previous Work

Previous work on image authentication falls into two groups, digital signatures [1] and digital watermarks [3]. A digital signature is based upon the idea of public key encryption. A private key is used to encrypt a hashed version of the image. This encrypted file then forms a unique "signature" for the image since only the entity signing the image has knowledge of the private key used. An associated public key can be used to decrypt the signature. The image under question can be hashed using the same hashing function as used originally. If these hashes match then the image is authenticated.

Digital signatures can be used for more than just image authentication. In particular when combined with secure timestamp, a digital signature can be used as a proof of first authorship.

A watermark, on the other hand, is a code secretly embedded into the image. The watermark allows for verification of the origin of an image. However, a watermark alone is not enough to prove first authorship, since an image could be marked with multiple watermarks. It has also been pointed out [6] that digital watermarks are not well suited to protecting the authenticity of an image.

3.0 Content Based Signatures

The key to developing a robust digital signature for images is to examine what the digital signature should protect. Ideally the signature should protect the message conveyed by the content of the image, and not the particular representation of that content. Thus the robust signature can be used to verify the authenticity of an image which has been modified by processing that does not affect the content of the image. Examples of this type of processing are removal of noise or lossy compression. However, manipulation of the image which changes the content, such as removal of a portion from a scene, can still be detected by the use of this signature.

Additionally, the use of a content based signature fits well with other content based image processing, such as content based coding and queries. By using the same content for both the signature and the compression algorithm, the signature will be able to authenticate images highly compressed using content based coding. With content based queries a signature can be the basis of a query.

4.0 Authenticity and Feature Selection

Often people think of authenticity as a binary quantity, either an image is authentic or it is not authentic. However, this is not always what people want when they are concerned with detecting image manipulation. We propose a continuous interpretation of authentic. An image which is bit by bit identical to the original image is considered completely authentic (authenticity measure of 1.0). An image which has nothing in common with the original image would be considered unauthentic (authenticity measure of 0.0). All other images would be partially authentic. Partially authentic is a loosely defined concept and measurement of the authenticity is subjective, and changes from application domain to application domain. One

way of thinking of this authenticity measure is as an authenticity vs. modification curve (see Figure 1). For example a curve could be drawn relating authenticity to the bit rate of a compressed image. Thus for each different type of modification there would be a corresponding curve. The old concept of authenticity would be represent as a Dirac delta function or a unit step function for all of the possible types of modification.

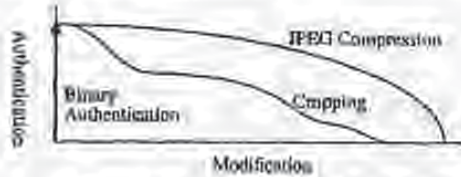


Figure 1. Authenticity vs. Modification Curve

Since authenticity is a subjective quantity, it is difficult to use directly as the basis of an authenticity verification system. We therefore need an approximation to authenticity which is analytical and can be computed from an image. The approach we are taking is to define a concept call feature authenticity A_f which is one minus the normalized distance between a feature vector computed for the original image, I_o , and the same feature vector computed from the image whose authenticity is to be measured, I_m . The key

$$A_f = 1 - \frac{\|feature(I_o) - feature(I_m)\|_{normalized}}{\|feature(I_o)\|_{normalized}}$$

is to find a set of features such that the feature authenticity closely approximates the image authenticity curves for the allowable forms of modification (e.g. lossy compression). Additionally, the feature authenticity curves for undesired forms of modification should be significantly below the curves for allowable forms of manipulation. Using the continuous measure of feature authenticity, a minimum acceptable authenticity can be defined. This can be defined directly, or defined in terms of some acceptable amount of manipulation. For example, the minimum acceptable authenticity can be defined in terms of maximum compression ratio. This minimum authenticity becomes a constraint on the optimization of the feature set. Once acceptable forms of manipulation are specified (e.g. compression, noise reduction, etc.) and the unacceptable forms are specified (e.g. cropping, cut and paste, etc.) the optimal set of features can be found. The goal is to have the authenticity vs. modification curve have a gentle slope for desired type of manipulation, and to have a very steep slope for the undesired forms of manipulation.

5.0 Generating and Verifying a Content Based Signature

The general procedure for generating a content based signature is diagrammed in figure 2. First, the content of interested, C_o is extracted from the image I_o to be signed, using an extraction function f_c . The content is then possibly hashed, using a hash function f_h to reduce the amount of data. This may be necessary since the size of the signature is dependent upon the amount of data

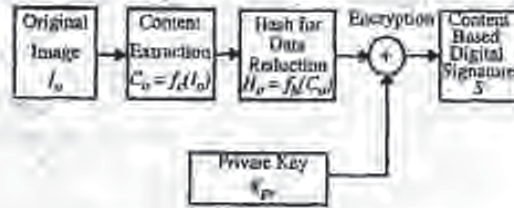


Figure 2. Generating a Content Based Signature

encrypted. The hash H_o is then encrypted using the private key K_{pr} of the signing entity to produce the final signature S . To verify

$$C_o = f_c(I_o)$$

$$H_o = f_h(C_o)$$

$$S = H_o \oplus K_{pr}$$

the authenticity of an questionable image I_q , the signator is decrypted using the public key K_{pu} and is compared to the hashed content extracted from the questionable image. If the distance between the feature vectors is less than a threshold value τ , then the questionable image is declared unmanipulated. This procedure is shown in figure 3.

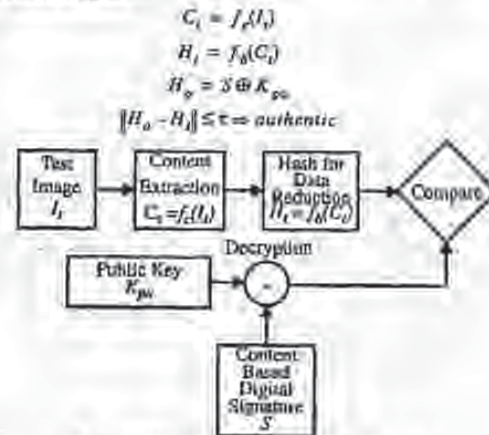


Figure 3. Verifying a Content Based Signature

The threshold value can be set by examining the amount of error introduced into an image by lossy compression. The difference between the image content hash at a target compression rate and the original image content hash can be used to set the threshold value. Note: If the threshold value is non zero, a cryptographically based hashing function can not be used, since there is no significance in closeness once a cryptographic hash has been applied to the content. A non cryptographic hashing function can be used to reduce the size of the signature, however this will typically weaken the signature.

It should be noted that a cryptographic hash can be used as the content extraction function. This content is of course not related to the way visual information is processed. Thus operations such as lossy compression as well as most other forms of image modification will have very steep authentication vs. modification curves. This is of course the signature scheme proposed in [1].

The problem is now one of finding a set of features which adequately describe the content of an image. Several different features can be used such as edge information, DCT coefficients, and color or intensity histograms.

We examined using the intensity histogram to sign the image. However, the histogram of the entire image itself is not very useful, since it contains no spatial information about the image intensities. Thus the images were divided into blocks and the intensity histogram for each block was computed separately. This allows some spatial information to be incorporated into the signature since the location of these blocks are fixed. Further spatial information can be incorporated by using a variable size block. Starting with small blocks, the histograms can be combined to form the histogram of a larger block. This can be used to produce blocks of different sizes for different parts of the image, allowing fine details to be protected by a small block size, and larger regions to be protected by a larger block size.

The distance function for detecting content changes is a subtle and challenging issue. The euclidean distance between intensity histograms was used as a measure of the content of the image. This performed well in detecting modification of the image. The amount of lossy compression which could be applied to the image and not pro-

duce a false positive was limited to at most 4:1. If we used a reduced distance function, then the maximum permissible compression ratio is increased. However, this increased robustness is achieved at the cost of sensitivity to subtle image manipulation. For example, it was found that the mean of the intensity histograms was a useful measure for detecting image content manipulation. Several different images were signed using the block average intensity technique. These images were then altered, typical altered test images are shown in figures 5 and 6, and the signatures were used to successfully detect the image manipulation. Note that the white boxes were added to highlight the modified regions and did not appear in the original test images. The original image was also compressed using JPEG compression. The signature system was not triggered even at high compression ratios of 14:1. As opposed to the euclidean distance using the full histogram, the maximum compression ratio is increased, but we can clearly see the trade-off.

Content based signatures for images can also be used to have an author sign an image. A typical use of this would be proof of first authorship. For this application the signature would have to be processed by a secure timestamp server. Additionally, it would be desirable to have the signature embedded into the image for this application. The signature should travel with the image so that authorship can readily be confirmed. It should be embedded so that even if the image is converted from one format to another the signature will remain with the image.

Embedding the signature into the image brings forth an additional issue, development of an embedding process which does not effect the signature verification process, since the embedding processes manipulates the image data. Information embedding in images is a



Figure 4. Original Image



Figure 5. JPEG Compressed 14:1



Figure 6. Manipulated Image Strip on Fireman's Jacket Removed



Figure 7. Manipulated Image Fire Hose Removed

generalization of the image watermark problem. One possible approach to embed a watermark into an image is to code the signature such that it resembles quantization noise and embed this in the image.[7] Another technique embeds a message into an image in the frequency domain. The image is broken into 8x8 blocks and a Discrete Cosine Transform is performed on each of the blocks. The signature is embedded by modifying the middle frequency coefficients and transforming the block back to the spatial domain.[8] This technique could easily be used with a signature based on the DC component, since this is unaffected by the embedding process. A third method also embeds a message in the frequency domain, however, here the image is treated as a noisy communication channel. The watermark is transmitted in this channel using a spread spectrum technique. [9]

6.0 Authentication of Video

It is also possible to extend authentication systems to video. There are two additional problems that need to be addressed when dealing with video sequences. The first is that of maintaining frame order integrity. The still image authentication techniques can be applied to each frame of the video sequence, but an additional signature must be provided to insure that the frames aren't reordered. The second problem is that we would like an unmodified clip from the larger sequence to be detected as unmodified. Here we present an extension to the original trustworthy camera [1]. A cryptographic hash is applied to each frame of the video. The hashes are ordered according to the corresponding frame order. This ordered sequence of hashes is then itself hashed (See Figure 8). All of these hashes are then encrypted using a public key cryptographic system to prevent forging of the hashes. To verify the authenticity of the entire video sequence only the second level hash is needed. The first level hashes are generated from the video sequence to be checked. These are then used to compute the second level hash. This second level hash is then compared to the original second level hash. To verify a subsection of the video sequence, first level hashes are generated from the subsection. Missing hashes are supplied from the signature. The second level hash can then be generated and checked. This system can be used to protect any group of pictures, not just video. For example, it could be used to protect the authenticity and order of multiple slices of MRI data.



Figure 8. Two Level Video Hashing

This idea can be extended to provide a more flexible method of verifying the authenticity of still pictures. In order to do this we can break the still picture into blocks. A hash is generated for each of the blocks. The blocks are then ordered, for instance by scanning across the rows. The sequence of hashes is then hashed to generate a signature which can protect the order. This image signature can be used to verify the authenticity of sections of cropped images. The blocks not effected by the cropping can be verified using the hashes for those blocks.

7.0 Contribution and Conclusion

The contributions of this work are the idea of using the image content to form a signature which can be used to protect the authenticity of images and survive acceptable compression. We also proposed a method for the extension of the authentication system to video. We have also presented a methodology for determining the set of features which can be used to approximate the image authenticity. We have also presented a method to extend digital signatures to video sequences, which can also be used to enhance the robustness of signatures for still images.

8.0 References

- [1] Friedman, Gary L., "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", *IEEE Transactions on Consumer Electronics*, vol. 39 no. 4, November 1993, pp. 905-910.
- [2] Netravali, Arun N. and Haskell, Barry G. "Digital Pictures: Representation and Compression", New York, NY, Plenum Press, 1988.
- [3] Walton, Steve, "Image Authentication for a Slippery New Age", *Dr. Dobbs' Journal*, April 1995, pp. 18-26.
- [4] Stinson, Douglas R., "Cryptography: Theory and Practice" Boca Raton, FL, CRC Press, 1995.
- [5] Wallace, G.K., "The JPEG still picture compression standard.", *Communications of the ACM*, vol. 34, no. 4, April 1991, pp. 30-40.
- [6] Macq, B.M. and Quisquater, J.J., "Cryptography for Digital TV Broadcasting", *Proceedings of the IEEE*, vol. 83, no. 6, June 1995.
- [7] Matsui, Kinoo and Tanaka, Kiyoshi, "Video-Steganography: How to Secretly Embed a Signature in a Picture", *IMA Intellectual Property Project Proceedings*, vol. 1, pp. 187-206, 1994.
- [8] Zhao, Jim and Koch, Eckhard, "Embedding Robust Labels into Images for Copyright Protection", *Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Vienna, Austria, August 21-25, 1995.
- [9] Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", *NEC Research Institute Technical Report 95-10*, 1995.

Secure Spread Spectrum Watermarking for Multimedia

Ingemar J. Cox, Senior Member, IEEE, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, Member, IEEE

Abstract—This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. We advocate that a watermark should be constructed as an independent and identically distributed (I.I.D.) Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. We argue that insertion of a watermark under this regime makes the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, requantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available and that it can be successfully registered against the transformed watermarked image. In these cases, the watermark detector unambiguously identifies the owner. Further, the use of Gaussian noise, ensures strong resilience to multiple-document, or collusional, attacks. Experimental results are provided to support these claims, along with an exposition of pending open problems.

Index Terms—Intellectual property, fingerprinting, multimedia, security, steganography, watermarking.

I. INTRODUCTION

THE PROLIFERATION of digitized media (audio, image, and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Therefore, conventional cryptography provides little protection against data piracy, in which a publisher is confronted with unauthorized reproduction of information. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within

the data after any decryption process. In the context of this work, data refers to audio (speech and music), images (photographs and graphics), and video (movies). It does not include ASCII representations of text, but does include text represented as an image. Many of the properties of the scheme presented in this work may be adapted to accommodate audio and video implementations, but the algorithms here specifically apply to images.

A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright owner (e.g., [2]). A visible watermark is limited in many ways. It mars the image fidelity and is susceptible to attack through direct image processing. A watermark may contain additional information, including the identity of the purchaser of a particular copy of the material. In order to be effective, a watermark should have the characteristics outlined below.

Unobtrusiveness: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Robustness: The watermark must be difficult (hopefully impossible) to remove. If only partial knowledge is available (for example, the exact location of the watermark in an image is unknown), then attempts to remove or destroy a watermark should result in severe degradation in fidelity before the watermark is lost. In particular, the watermark should be robust in the following areas:

- * **Common signal processing:** The watermark should still be retrievable even if common signal processing operations are applied to the data. These include, digital-to-analog and analog-to-digital conversion, resampling, quantization (including dithering and recompression), and common signal enhancements to image contrast and color, or audio bass and treble, for example.
- * **Common geometric distortions (image and video data):** Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling.
- * **Subterfuge attacks (collusion and forgery):** In addition, the watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data. That is, the watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.

Manuscript received January 14, 1996; revised January 24, 1997. Portions of this work were reprinted, with permission, from the Proceedings of the IEEE Conference on Image Processing, 1996, and from the Proceedings of the First International Conference on Data Hiding (Springer-Verlag, 1996). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Seshu Rajala.

I. J. Cox and J. Kilian are with NEC Research Institute, Princeton, NJ 08540 USA (e-mail: ingemar@research.nj.nec.com; joe@research.nj.nec.com).

F. T. Leighton is with the Mathematics Department and Laboratory for Computer Science, The Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: ftl@math.mit.edu).

T. Shamoon is with InterTrust STAR Laboratory, Sunnyvale, CA 94086 USA (e-mail: talal@intertrust.com).

Publisher Item Identifier S 1057-7149(97)04460-1

Universality: The same digital watermarking algorithm should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conducive to implementation of audio and image/video watermarking algorithms on common hardware.

Unambiguity: Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

There are two parts to holding a strong watermark: the watermark structure and the insertion strategy. In order for a watermark to be robust and secure, these two components must be designed correctly. We provide two key insights that make our watermark both robust and secure. We argue that the watermark be placed explicitly in the perceptually most significant components of the data, and that the watermark be composed of random numbers drawn from a Gaussian ($N(0, 1)$) distribution.

The stipulation that the watermark be placed in the perceptually significant components means that an attacker must target the fundamental structural components of the data, thereby heightening the chances of fidelity degradation. While this strategy may seem counterintuitive from the point of view of steganography (how can these components hide any signal?), we discovered that the significant components have a perceptual capacity that allows watermark insertion without perceptual degradation. Further, most processing techniques applied to media data tend to leave the perceptually significant components intact. While one may choose from a variety of such components, in this paper, we focus on the perceptually significant spectral components of the data. This simultaneously yields high perceptual capacity and achieves a uniform spread of watermark energy in the pixel domain.

The principle underlying our watermark structuring strategy is that the mark be constructed from independent, identically distributed (i.i.d.) samples drawn from a Gaussian distribution. Once the significant components are located, Gaussian noise is injected therein. The choice of this distribution gives excellent performance against collusion attacks. The Gaussian watermark also gives our scheme strong performance in the face of quantization, and may be structured to provide low false positive and false negative detection. This is discussed below, and elaborated on in [13].

Finally, note that the techniques presented herein do not provide proof of content ownership on their own. The focus of this paper are algorithms that insert messages into content in an extremely secure and robust fashion. Nothing prevents someone from inserting another message and claiming ownership. However, it is possible to couple our methods with strong authentication and other cryptographic techniques in order to provide complete, secure and robust owner identification and authentication.

Section III begins with a discussion of how common signal transformations, such as compression, quantization, and manipulation, affect the frequency spectrum of a signal. This discussion motivates our belief that a watermark should be embedded in the data's perceptually significant frequency

components. Of course, the major problem then becomes how to imperceptibly insert a watermark into perceptually significant components of the frequency spectrum. Section III-A proposes a solution based on ideas from spread spectrum communications. In particular, we present a watermarking algorithm that relies on the use of the original image to extract the watermark. Section IV provides an analysis based on possible collusion attacks that indicates that a binary watermark is not as robust as a continuous one. Furthermore, we show that a watermark structure based on sampling drawn from multiple i.i.d. Gaussian random variables offers good protection against collusion. Ultimately, no watermarking system can be made perfect. For example, a watermark placed in a textual image may be eliminated by using optical character recognition technology. However, for common signal and geometric distortions, the experimental results of Section V suggest that our system satisfies most of the properties discussed in the introduction, and displays strong immunity to a variety of attacks in a collusion resistant manner. Finally, Section VI discusses possible weaknesses and potential enhancements to the system and describes open problems and subsequent work.

II. PREVIOUS WORK

Several previous digital watermarking methods have been proposed. Turner [25] proposed a method for inserting an identification string into a digital audio signal by substituting the "insignificant" bits of randomly selected audio samples with the bits of an identification code. Bits are deemed "insignificant" if their alteration is inaudible. Such a system is also appropriate for two-dimensional (2-D) data such as images, as discussed in [26]. Unfortunately, Turner's method may easily be circumvented. For example, if it is known that the algorithm only affects the least significant two bits of a word, then it is possible to randomly flip *all* such bits, thereby destroying any existing identification code.

Chen et al. [6] suggests adding tags—small geometric patterns—in digitized images at brightness levels that are imperceptible. While the idea of hiding a spatial watermark in an image is fundamentally sound, this scheme may be susceptible to attack by filtering and resampling. The fainter such watermarks are, the more susceptible they are such attacks and geometric shapes provide only a limited alphabet with which to encode information. Moreover, the scheme is not applicable to audio data and may not be robust to common geometric distortions, especially cropping.

Bruce et al. [4] propose three methods appropriate for document images in which text is common. Digital watermarks are coded by 1) vertically shifting text lines, 2) horizontally shifting words, or 3) altering text features such as the vertical outlines of individual characters. Unfortunately, all three proposals are easily defeated, as discussed by the author. Moreover, these techniques are restricted exclusively to images containing text.

Timko et al. [19], [24] describe several watermarking schemes that rely on embedding watermarks that resemble quantization noise. Their ideas hinge on the notion that quantization noise is typically imperceptible to viewers. Their

first scheme injects a watermark into an image by using a predetermined data stream to guide level selection in a predictive quantizer. The data stream is chosen so that the resulting image looks like quantization noise. A variation on this scheme is also presented, where a watermark in the form of a dithering matrix is used to dither an image in a certain way. There are several drawbacks to these schemes. The most important is that they are susceptible to signal processing, especially requantization, and geometric attacks such as cropping. Furthermore, they degrade an image in the same way that predictive coding and dithering can.

In [24], the authors also propose a scheme for watermarking discrete data. This scheme exploits run lengths (or run) of data in the run length code used to generate the coded fax image. This proposal is susceptible to digital-to-analog and analog-to-digital attacks. In particular, randomizing the least significant bit (LSB) of each pixel's intensity will completely alter the resulting run length encoding. Tanaka *et al.* also propose a watermarking method for "inter-coded picture and video sequences". This method applies the same signal transform as the Joint Photographers Expert Group (JPEG) (discrete cosine transform of 8×8 subblocks of an image) and embeds a watermark in the coefficient quantization module. While being compatible with existing transform coders, this scheme may be susceptible to requantization and filtering and is equivalent to coding the watermark in the LSB's of the transform coefficients.

In a recent paper, Macq and Quispelater [18] briefly discuss the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provide a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours. Bender *et al.* [3] describe two watermarking schemes. The first is a statistical method called *patchwork*. Patchwork randomly chooses a pair of image points, (a, b) , and increases the brightness at a , by one unit while correspondingly decreasing the brightness of b . The expected value of the sum of the differences of the n pairs of points is then $2n$, provided certain statistical properties of the image are true.

The second method is called "texture block coding," wherein a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this technique is that it is only appropriate for images that possess large areas of random texture. The technique could not be used on images of text, for example, nor is there a direct analog for audio.

Rhoads [21] describes a method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by comparing a binary mask of L bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images

and then by examining the sign of the difference (pixel by pixel), to determine if it corresponds to the original sequence of additions and subtractions. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be prefiltered to provide some robustness to lowpass filtering. This scheme does not consider the problem of collusion attacks.

Koch, Rodriguez, and Zhao [14] propose two general methods for watermarking images. The first method, attributed to Scott Burgess, breaks up an image into 8×8 blocks and computes the discrete cosine transform (DCT) of each of these blocks. A pseudorandom subset of the blocks is chosen, then, in each such block, a triple of frequencies is selected from one of 18 predetermined triples and modified so that their relative strengths encode a one or zero value. The 18 possible triples are composed by selection of three out of eight predetermined frequencies within the 8×8 DCT block. The choice of the eight frequencies to be altered within the DCT block is based on a belief that the "middle frequencies" have moderate variance, i.e. they have similar magnitude. This property is needed in order to allow the relative strength of the frequency triples to be altered without requiring a modification that would be perceptually noticeable. Superficially, this scheme is similar to our own proposal, also drawing an analogy to spread spectrum communications. However, the structure of their watermark is different from ours, and the set of frequencies is not chosen based on any direct perceptual significance, or relative energy considerations. Further, because the variance between the eight frequency coefficients is small, one would expect that their technique may be sensitive to noise or distortion. This is supported by the experimental results that report that the "embedded labels are robust against JPEG compression for a quality factor as low as about 50%." By comparison, we demonstrate that our method performs well with compression quality factors as low as 5%. An earlier proposal by Koch and Zhao [15] used one triple of frequencies (or pairs of frequencies), and was again designed specifically for robustness to JPEG compression. Nevertheless, they state that "a lower quality factor will increase the likelihood that the changes necessary to superimpose the embedded code on the signal will be noticeably visible." In a second method, designed for black and white images, no frequency transform is employed. Instead, the selected blocks are modified so that the relative frequency of white and black pixels encodes the final value. Both watermarking methods are particularly vulnerable to multiple document attacks. To protect against this, Zhao and Koch propose a *distributed* 8×8 block created by randomly sampling 64 pixels from the image. However, the resulting DCT has no relationship to that of the raw image and consequently may be likely to cause noticeable artifacts in the image and be sensitive to noise.

In addition to direct work on watermarking images, there are several works of interest in related areas. Adelson [1] describes a technique for embedding digital information in an analog TV signal. The analog signal is quantized into one of two disjoint ranges $\{0, 2, 4, \dots\}$, $\{1, 3, 5, \dots\}$, for example, that are selected based on the binary digit to be transmitted. Thus,

Adelson's method is equivalent to watermark schemes that encode information into the LSB's of the data or its transform coefficients. Adelson recognizes that the method is susceptible to noise and therefore proposes an alternative scheme wherein a 2×1 Hadamard transform of the digitized analog signal is taken. The differential coefficient of the Hadamard transform is offset by zero or one unit prior to computing the inverse transform. This corresponds to encoding the watermark into the least significant bit of the differential coefficient of the Hadamard transform. It is not clear that this approach would demonstrate enhanced resilience to noise. Furthermore, like all such LSB schemes, an attacker can eliminate the watermark by randomization.

Schreiber *et al.* [22] describe a method to interleave a standard NTSC signal within an enhanced definition television (EDTV) signal. This is accomplished by analyzing the frequency spectrum of the EDTV signal (larger than that of the NTSC signal) and decomposing it into three subbands (L, M, H for low-, medium- and high-frequency, respectively). In contrast, the NTSC signal is decomposed into two subbands, L and M. The coefficients, M_h , within the M band are quantized into m levels and the high frequency coefficients, H_h , of the EDTV signal are scaled such that the addition of the H_h signal plus any noise present in the system is less than the minimum separation between quantization levels. Once more, the method relies on modifying least significant bits. Presumably, the midrange rather than low frequencies were chosen because these are less perceptually significant. In contrast, the method proposed here modifies the *most* perceptually significant components of the signal.

Finally, it should be noted that existing techniques are generally not resistant to collusion attacks by multiple documents.

III. WATERMARKING IN THE FREQUENCY DOMAIN

In order to understand the advantages of a frequency-based method, it is instructive to examine the processing stages that an image (or sound) may undergo in the process of copying, and to study the effect that these stages could have on the data, as illustrated in Fig. 1. In the figure, "transmission" refers to the application of any source or channel code, and/or standard encryption technique to the data. While most of these steps are information lossless, many compression schemes (JPEG, MPEG, etc.) are lossy, and can potentially degrade the data's quality, through *irretrievable* loss of information. In general, a watermarking scheme should be resilient to the distortions introduced by such algorithms.

Lossy compression is an operation that usually eliminates perceptually nonsalient components of an image or sound. Most processing of this sort takes place in the frequency domain. In fact, data loss usually occurs among the high-frequency components.

After receipt, an image may endure many common transformations that are broadly categorized as geometric distortions or signal distortions. Geometric distortions are specific to images and video, and include such operations as rotation, translation, scaling and cropping. By manually determining a minimum of four or nine corresponding points between the

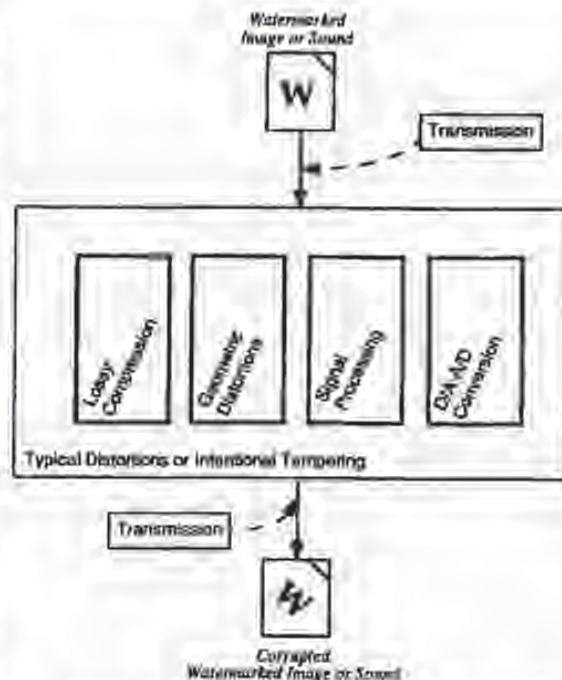


Fig. 1. Common processing operations that a media document could undergo.

original and the distorted watermark, it is possible to remove any two or three-dimensional (3-D) affine transformation [8]. However, an affine scaling (shrinking) of the image leads to a loss of data in the high-frequency spectral regions of the image. Cropping, or the cutting out and removal of portions of an image, leads to irretrievable loss of image data, which may seriously degrade any spatially based watermark such as [6]. However, a frequency-based scheme spreads the watermark over the whole spatial extent of the image, and is therefore less likely to be affected by cropping, as demonstrated in Section V-E.

Common signal distortions include digital-to-analog and analog-to-digital conversion, resampling, requantization, including dithering and recompression, and common signal enhancements to image contrast and/or color, and audio frequency equalization. Many of these distortions are nonlinear, and it is difficult to analyze their effect in either a spatial- or frequency-based method. However, the fact that the original image is known allows many signal transformations to be undone, at least approximately. For example, histogram equalization, a common nonlinear contrast enhancement method, may be removed substantially by histogram specification [10] or dynamic histogram warping [7] techniques.

Finally, the copied image may not remain in digital form. Instead, it is likely to be printed, or an analog recording made (onto analog audio or video tape). These reproductions introduce additional degradation into the image that a watermarking scheme must be robust to.

The watermark must not only be resistant to the inadvertent application of the aforementioned distortions; it must also

be immune to intentional manipulation by malicious parties. These manipulations can include combinations of the above distortions, and can also include collusion and forgery attacks, which are discussed in Section IV-E.

A. Spread Spectrum Coding of a Watermark

The above discussion illustrates that the watermark should *not* be placed in perceptually insignificant regions of the image (or its spectrum), since many common signal and geometric processes affect these components. For example, a watermark placed in the high-frequency spectrum of an image can be easily eliminated with little degradation to the image by any process that directly or indirectly performs lowpass filtering. The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum in a fidelity preserving fashion. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise.

To solve this problem, the frequency domain of the image or sound at hand is viewed as a *communication channel*, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the immersed signal must be immune to. While we use this methodology to hide watermarks in data, the same rationale can be applied to sending any type of message through media data.

We originally conceived our approach by analogy to spread spectrum communications [20]. In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into a single output with high signal-to-noise ratio (SNR). However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins.

Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures severe degradation of the original data following any attack on the watermark.

A watermark that is well placed in the frequency domain of an image or a sound track will be practically impossible to see or hear. This will always be the case if the energy in the watermark is sufficiently small in any single frequency coefficient. Moreover, it is possible to increase the energy present in particular frequencies by exploiting knowledge of masking phenomena in the human auditory and visual systems. Perceptual masking refers to any situation where information in certain regions of an image or a sound is occluded by perceptually more prominent information in another part of the scene. In digital waveform coding, this frequency domain (and, in some cases, time/pixel domain) masking is exploited

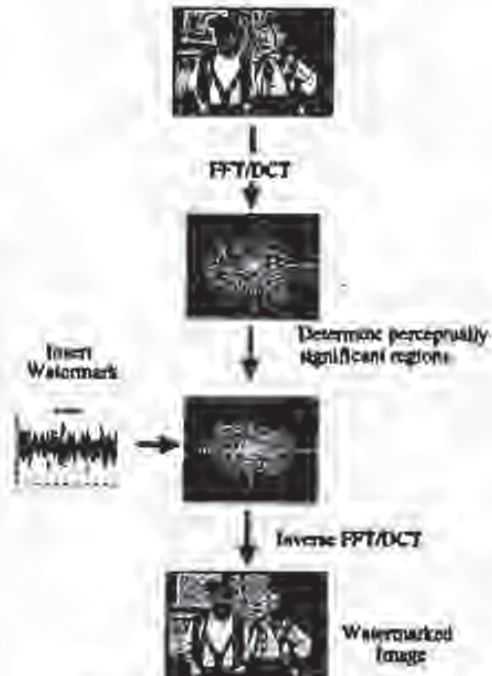


Fig. 2. Stages of watermark insertion process.

extensively to achieve low bit rate encoding of data [9], [12]. It is known that both the auditory and visual systems attach more resolution to the high-energy, low-frequency, spectral regions of an auditory or visual scene [12]. Further, spectrum analysis of images and sounds reveals that most of the information in such data is located in the low-frequency regions.

Fig. 2 illustrates the general procedure for frequency domain watermarking. Upon applying a frequency transformation to the data, a *perceptual mask* is computed that highlights perceptually significant regions in the spectrum that can support the watermark without affecting perceptual fidelity. The watermark signal is then inserted into these regions in a manner described in Section IV-B. The precise magnitude of each modification is only known to the owner. By contrast, an attacker may only have knowledge of the possible range of modification. To be confident of eliminating a watermark, an attacker must assume that each modification was at the limit of this range, despite the fact that few such modifications are typically this large. As a result, an attack creates visible (or audible) defects in the data. Similarly, unintentional signal distortions due to compression or image manipulation, must leave the perceptually significant spectral components intact, otherwise the resulting image will be severely degraded. This is why the watermark is robust.

In principle, any frequency domain transform can be used. However, in the experimental results of Section VI we use a Fourier domain method based on the DCT [16], although we are currently exploring the use of wavelet-based schemes as a variation. In our view, each coefficient in the frequency domain has a *perceptual capacity*, that is, a quantity of additional

information can be added without any (or with minimal) impact to the perceptual fidelity of the data. To determine the perceptual capacity of each frequency, one can use models for the appropriate perceptual system or simple experimentation.

In practice, in order to place a length n watermark into an $N \times N$ image, we computed the $N \times N$ DCT of the image and placed the watermark into the n highest magnitude coefficients of the transform matrix, excluding the DC component.¹ For most images, these coefficients will be the ones corresponding to the low frequencies.

In the next section, we provide a high level discussion of the watermarking procedure, describing the structure of the watermark and its characteristics.

IV. STRUCTURE OF THE WATERMARK

We now give a high-level overview of our basic watermarking scheme; many variations are possible. In its most basic implementation, a watermark consists of a sequence of real numbers $X = x_1, \dots, x_n$. In practice, we create a watermark where each value x_i is chosen independently according to $N(0,1)$ (where $N(\mu, \sigma^2)$ denotes a normal distribution with mean μ and variance σ^2). We assume that numbers are represented by a reasonable but finite precision and ignore these insignificant roundoff errors. Section IV-A introduces notation to describe the insertion and extraction of a watermark and Section IV-D describes how two watermarks (the original one and the recovered, possibly corrupted one) can be compared. This procedure exploits the fact that each component of the watermark is chosen from a normal distribution. Alternative distributions are possible, including choosing x_i uniformly from $\{-1, 1\}$, $[0, 1]$ or $[0, 1]$. However, as we discuss in IV-D, using such distributions leaves one particularly vulnerable to attacks using multiple watermarked documents.

A. Description of the Watermarking Procedure

We extract from each document D a sequence of values $V = v_1, \dots, v_n$, into which we insert a watermark $X = x_1, \dots, x_n$ to obtain an adjusted sequence of values $V' = v'_1, \dots, v'_n$. V' is then inserted back into the document in place of V to obtain a watermarked document D' . One or more attackers may then alter D' , producing a new document D^* . Given D and D^* , a possibly corrupted watermark X^* is extracted and is compared to X for statistical significance. We extract X^* by first extracting a set of values $V^* = v^*_1, \dots, v^*_n$ from D^* (using information about D) and then generating X^* from V^* and V .

Frequency-domain based methods for extracting V and V^* and inserting V' are given in Section III. For the rest of this section, we ignore the manipulations of the underlying documents.

¹More generally, n randomly chosen coefficients could be chosen from the M , $M \geq n$ most perceptually significant coefficients of the transform. The choice of appropriate components remains a subject of research.

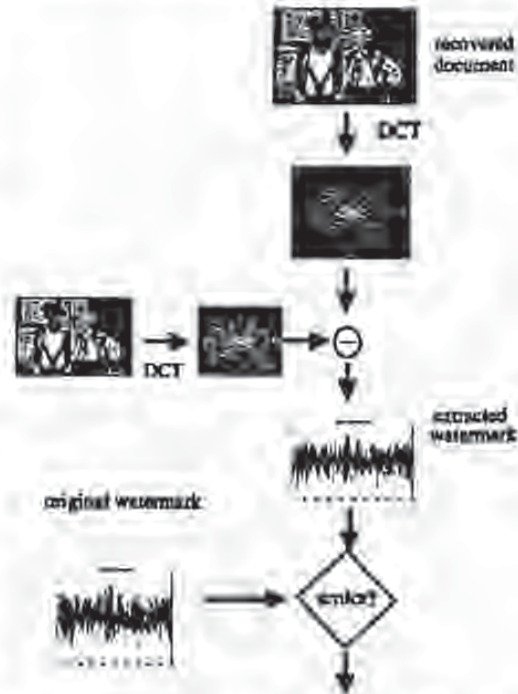


Fig. 3. Finalizing and decoding of the watermark string.

B. Inserting and Extracting the Watermark

When we insert X into V to obtain V' we specify a scaling parameter α , which determines the extent to which X alters V . Three natural formulae for computing V' are

$$v'_i = v_i + \alpha x_i \quad (1)$$

$$v'_i = v_i(1 + \alpha x_i) \quad (2)$$

$$v'_i = v_i(e^{\alpha x_i}) \quad (3)$$

Equation (1) is always invertible, and (2) and (3) are invertible if $v_i \neq 0$, which holds in all of our experiments. Given V^* , we can therefore compute the inverse function to derive X^* from V^* and V .

Equation (1) may not be appropriate when the v_i values vary widely. If $v_i = 10^6$ then adding 100 may be insufficient for establishing a mark, but if $v_i = 10$ adding 100 will distort this value unacceptably. Insertion based on (2) or (3) are more robust against such differences in scale. We note that (2) and (3) give similar results when αx_i is small. Also, when v_i is positive, then (3) is equivalent to $\lg(v'_i) = \lg(v_i) + \alpha x_i$, and may be viewed as an application of (1) to the case where the logarithms of the original values are used.

1) *Determining Multiple Scaling Parameters:* A single scaling parameter α may not be applicable for perturbing all of the values v_i , since different spectral components may exhibit more or less tolerance to modification. More generally one can have multiple scaling parameters $\alpha_1, \dots, \alpha_n$ and use update rules such as $v'_i = v_i(1 + \alpha_i x_i)$. We can view α_i as a relative measure of how much one must alter v_i to alter the perceptual quality of the document. A large α_i means that one

can perceptually "get away" with altering v_i by a large factor without degrading the document.

There remains the problem of selecting the multiple scaling values. In some cases, the choice of α_i may be based on some general assumption. For example, (2) is a special case of the generalized (1) ($v_i' = v_i + \alpha_i x_i$), for $\alpha_i = \alpha v_i$. Essentially, (2) makes the reasonable assumption that a large value is less sensitive to additive alterations than a small value.

In general, one may have little idea of how sensitive the image is to various values. One way of empirically estimating these sensitivities is to determine the distortion caused by a number of attacks on the original image. For example, one might compute a degraded image D^* from D , extract the corresponding values v_1', \dots, v_n' and choose α_i to be proportional to the deviation $|v_i' - v_i|$. For greater robustness, one should try many forms of distortion and make α_i proportional to the average value of $|v_i' - v_i|$. As alternatives to taking the average deviation one might also take the median or maximum deviation.

One may combine this empirical approach with general global assumptions about the sensitivity of the values. For example, one might require that $\alpha_i \geq \alpha_j$ whenever $v_i \geq v_j$. One way to combine this constraint with the empirical approach would be to set α_i according to

$$\alpha_i \sim \max_{|v_j| \leq v_i} |v_j' - v_j|$$

A still more sophisticated approach would be to weaken the monotonicity constraint to be robust against occasional outliers.

In all our experiments we simply use (2) with a single parameter $\alpha = 0.1$. When we computed JPEG-based distortions of the original image, we observed that the higher energy frequency components were not altered proportional to their magnitude (the implicit assumption of (2)). We suspect that we could make a less obtrusive mark of equal strength by attenuating our alterations of the high-energy components and amplifying our alterations of the lower energy components. However, we have not yet performed this experiment.

C. Choosing the Length, n , of the Watermark

The choice of n dictates the degree to which the watermark is spread out among the relevant components of the image. In general, as the number of altered components are increased the extent to which they must be altered decreases. For a more quantitative assessment of this tradeoff, we consider watermarks of the form $v_i' = v_i + \alpha x_i$ and model a white noise attack by $v_i' = v_i + r_i$, where r_i are chosen according to independent normal distributions with standard deviation σ . For the watermarking procedure we described below, one can recover the watermark when α is proportional to σ/\sqrt{n} . That is, by quadrupling the number of components used, one can halve the magnitude of the watermark placed into each component. Note that the sum of squares of the deviations will be essentially unchanged.

Note that the number of bits of information associated with the watermark can be arbitrary—the watermark is simply used as an index to a database entry associated with the watermark.

D. Evaluating the Similarity of Watermarks

It is highly unlikely that the extracted mark X^* will be identical to the original watermark X . Even the act of requantizing the watermarked document for delivery will cause X^* to deviate from X . We measure the similarity of X and X^* by

$$\text{sim}(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}} \quad (4)$$

Many other measures are possible, including the standard correlation coefficient. Further variations on this basic metric are discussed in IV-D2. To decide whether X and X^* match, one determines whether $\text{sim}(X, X^*) > T$, where T is some threshold. Setting the detection threshold is a classical decision estimation problem in which we wish to minimize both the rate of false negatives (missed detections) and false positives (false alarms) [25]. We have chosen our measure so that it is particularly easy to determine the probability of false positives.

1) *Computing the Probability of False Positives:* There is always the possibility that X and X^* will be very similar purely by random chance; hence, any similarity metric will give "significant" values that are spurious. We analyze the probability of such false positives as follows. Suppose that the creators of document D^* had no access to X (either through the seller or through a watermarked document). Then, even conditioned on any fixed value for X^* , each x_i will be independently distributed according to $N(0, 1)$. That is, X is independent of X^* .

The distribution on $X^* \cdot X$ may be computed by first writing it as $\sum_{i=1}^n x_i^* x_i$, where x_i^* is a constant. Using the well-known formula for the distribution of a linear combination of variables that are independent and normally distributed, $X^* \cdot X$ will be distributed according to

$$N\left(0, \sum_{i=1}^n x_i^{*2}\right) = N(0, X^* \cdot X^*)$$

Thus, $\text{sim}(X, X^*)$ is distributed according to $N(0, 1)$. We can then apply the standard significance tests for the normal distribution. For example, if X^* is created independently from X then the probability that $\text{sim}(X, X^*) > 6$ is the probability of a normally distributed random variable exceeding its mean by more than six standard deviations.

Hence, for a small number of documents, setting the threshold at T equal to six will cause spurious matchings to be extremely rare. Of course, the number of tests to be performed must be considered in determining what false positive probability is acceptable. For example, if one tests an extracted watermark X^* against 10^6 watermarks, then the probability of a false positive is increased by a multiplicative factor of 10^6 as well.

We note that our similarity measure and the false-positive probability analysis does not depend on n , the size of the watermark. However, n implicitly appears, since for example, $\text{sim}(X, X)$ is likely to be around \sqrt{n} when X is generated in the prescribed manner. As a rule of thumb, larger values of n tend to cause larger similarity values when X and X^* are genuinely related (e.g., X^* is a distorted version of X),



Fig. 4. Bavarian couple image courtesy of Corel Stock Photo Library.



Fig. 5. Watermarked version of Bavarian couple

without causing larger similarity values when X and X^* are independent. This benefit must be balanced against the tendency for the document to be more distorted when η is larger.

a) *A remark on quantization:* In the above analysis, we treated all of the vectors as consisting of ideal real numbers. In practice, the actual values inserted will be quantized to some extent. Nevertheless, it is simpler to view the watermarks as real numbers and the quantization process as yet another form of distortion. Our analysis of false positives does not depend on the distribution or even the domain of possible X^* , and hence holds regardless of quantization effects.

There is an additional, extremely low-order quantization effect that occurs because X is generated with only finite precisions. However, this effect is caused only by the arithmetic precision, and not on the constraints imposed by the document. If each $x_i \in X$ is stored as a double-precision real number, the difference between the calculated value of $\text{sim}(X, X^*)$ and its "ideal" value will be quite small for any reasonable η and any reasonable bound on the dynamic range of X^* .

2) *Robust Statistics:* The above analysis required only the independence of X from X^* , and did not rely on any specific properties of X^* itself. This fact gives us further flexibility when it comes to preprocessing X^* . We can process X^* in a number of ways to potentially enhance our ability to extract a watermark. For example, in our experiments on images we encountered instances where the average value of x_i^* , denoted $E_i(X^*)$, differed substantially from zero, due to the effects of a dithering procedure. While this artifact could be easily eliminated as part of the extraction process, it provides a motivation for preprocessing extracted watermarks. We found that the simple transformation $x_i^* \leftarrow x_i^* - E_i(X^*)$ yielded superior values of $\text{sim}(X, X^*)$. The improved performance resulted from the decreased value of $X^* \cdot X^*$; the value of $X^* \cdot X$ was only slightly affected.

In our experiments, we frequently observed that x_i^* could be greatly distorted for some values of i . One postprocessing

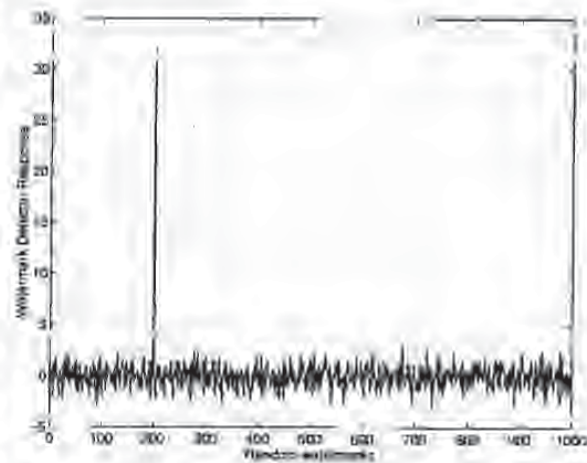


Fig. 6. Watermark detector response to 1000 randomly generated watermarks. Only one watermark (the one to which the detector was set to respond) matches that present in Fig. 5.

option is to simply ignore such values, setting them to zero. That is

$$x_i^* \leftarrow \begin{cases} x_i^* & \text{if } |x_i^*| \leq \text{tolerance} \\ 0 & \text{otherwise.} \end{cases}$$

Again, the goal of such a transformation is to lower $X^* \cdot X^*$. A less abrupt version of this approach is to normalize the X^* values to be either $-1, 0$ or 1 , by

$$x_i^* \leftarrow \text{sign}(x_i^* - E_i(X^*)).$$

This transformation can have a dramatic effect on the statistical significance of the result. Other robust statistical techniques could also be used to suppress outlier effects [11].

A natural question is whether such postprocessing steps run the risk of generating false positives. Indeed, the same potential risk occurs whenever there is any latitude in the



(a)



(b)

Fig. 7. (a) Lowpass filtered, 0.5-scaled image of Bavarian couple. (b) Rescaled image showing noticeable loss of fine detail.

procedure for extracting X^* from D^* . However, as long as the method for generating a set of values for X^* depends solely on D and D^* , our statistical significance calculation is unaffected. The only caveat to be considered is that the bound on the probability that one of X_1^*, \dots, X_k^* generates a false positive is the sum of the individual bounds. Hence, to convince someone that a watermark is valid, it is necessary to have a published and rigid extraction and processing policy that is guaranteed to only generate a small number of candidate X^* .

E. Resilience to Multiple-Document (Collusion) Attacks

The most general attack consists of using t multiple watermarked copies D_1^*, \dots, D_t^* of document D to produce an unwatermarked document D^* . We note that most schemes proposed seem quite vulnerable to such attacks. As a theoretical exception, Boneh and Shaw [5] propose a coding scheme for use in situations in which one can insert many relatively weak ± 1 watermarks into a document. They assume that if the i th watermark is the same for all t copies of the document then it cannot be detected, changed or removed. Using their coding scheme, the number of weak watermarks to be inserted scales according to t^4 , which may limit its usefulness in practice.

To illustrate the power of multiple-document attacks, consider watermarking schemes in which v_i^j is generated by either adding 1 or -1 at random to v_i . Then as soon as one finds two documents with unequal values for v_i^j , one can determine v_i and, hence, completely eliminate this component of the watermark. With t documents one can, on average, eliminate all but a 2^{1-t} fraction of the components of the watermark. Note that this attack does not assume anything about the distribution on v_i . While a more intelligent allocation of ± 1 values to the watermarks (following [5] and [17]) will better resist this simple attack, the discrete nature of the watermark components makes them much easier to completely eliminate. Our use of continuous valued watermarks appears to

give greater resilience to such attacks. Interestingly, we have experimentally determined that if one chooses the x_i uniformly over some range, then one can remove the watermark using only five documents.

Use of the normal distribution seems to give better performance than the distributions considered above. We note that the crucial performance measure to consider is the value of $\max_i(X^* \cdot X_i)$, where X^* is the watermark extracted from an document D^* generated by attacking documents D_1, \dots, D_t , with respective watermarks X_1, \dots, X_t . The denominator $\sqrt{X^* \cdot X^*}$ of our similarity measure can always be made larger by, for example, adding noise. This causes the similarity measure to shrink, at the expense of distorting the image. Hence, we can view $\max_i(X^* \cdot X_i)$ as determining a fidelity/undetectability tradeoff curve and the value of $\sqrt{X^* \cdot X^*}$ as picking a point on this curve.

When X_i is inserted into D by a linear update rule, then an averaging attack, which sets

$$D^* = \frac{D_1 + \dots + D_t}{t}$$

will result in

$$X^* = \frac{X_1 + \dots + X_t}{t}.$$

In this case,

$$\max_i(X^* \cdot X_i) \approx \frac{1}{t} \max_i(X_i \cdot X_i) \text{ (assuming } X_i X_j \approx 0).$$

That is, there is a $1/t$ behavior in the detector output.

Note that with a naive averaging attack, the denominator, $\sqrt{X^* \cdot X^*}$, will be a (roughly) $1/\sqrt{t}$ factor smaller, so $\max_i \text{sim}(X_i, X^*)$ will be roughly \sqrt{t}/\sqrt{t} . However, as mentioned before, additional noise can be added so that the extracted watermark, X^* , has the same power as any of the original watermarks X_i . Then $\max_i \text{sim}(X_i, X^*)$ will be



Fig. 8. JPEG encoded version of Bavarian couple with 10% quality and 0% smoothing.



Fig. 9. JPEG encoded version of Bavarian couple with 5% quality and 0% smoothing.

roughly \sqrt{n}/t . Thus, the similarity measure can be struck by a factor of t .

We do not know of any more effective multidocument attack on normally distributed watermarks. In a forthcoming paper (see <http://www.neci.nj.nec.com/tr/index.html>), a more theoretical justification is given for why it is hard to achieve more than an $O(t)$ reduction in the similarity measure.

V. EXPERIMENTAL RESULTS

In order to evaluate the proposed watermarking scheme, we took the Bavarian couple² image of Fig. 4 and produced the watermarked version of Fig. 5. We then subjected the watermarked image to a series of image processing and collusion style attacks. These experiments are preliminary, but show resilience to certain types of common processing. Of note is our method's resistance to compression such as JPEG, and data conversion (printing, xeroxing and scanning). Note that in the case of affine transforms, registration to the original image is crucial to successful extraction.

In all experiments, a watermark length of 1000 was used. We added the watermark to the image by modifying 1000 of the more perceptually significant components of the image spectrum using (2). More specifically, the 1000 largest coefficients of the DCT (excluding the DC term) were used. A fixed scale factor of 0.1 was used throughout.

A. Experiment 1: Uniqueness of Watermark

Fig. 6 shows the response of the watermark detector to 1000 randomly generated watermarks of which only one matches the watermark present in Fig. 5. The positive response due to the correct watermark is very much stronger than the response to

²The common test image Lenna was originally used in our experiments, and similar results were obtained. However, Playboy Inc. refused to grant copyright permission for electronic distribution.



Fig. 10. Dithered version of the Bavarian couple image.

incorrect watermarks, suggesting that the algorithm has very low false positive response rates.

B. Experiment 2: Image Scaling

We scaled the watermarked image to half of its original size, as shown in Fig. 7(a). In order to recover the watermark, the quarter-sized image was rescaled to its original dimensions, as shown in Fig. 7(b), in which it is clear that considerable fine detail has been lost in the scaling process. This is to be expected since subsampling of the image requires a lowpass spatial filtering operation. The response of the watermark detector to the original watermarked image of Fig. 5 was 32.0, which compares to a response of 13.4 for the rescaled version of Fig. 7(b). While the detector response is down by over 50%, the response is still well above random chance



(a)



(b)

Fig. 11. (a) Clipped version of watermarked Bavarian couple. (b) Restored version of Bavarian couple in which missing portions have been replaced with imagery from the original unwatermarked image of Fig. 4.

levels suggesting that the watermark is robust to geometric distortions. Moreover, it should be noted that 75% of the original data is missing from the scaled down image of Fig. 7.³

C. Experiment 3: JPEG Coding Distortion

Fig. 8 shows a JPEG encoded version of the Bavarian couple image with parameters of 10% quality and 0% smoothing, which results in clearly visible distortions of the image. The response of the watermark detector is 22.8, again suggesting that the algorithm is robust to common encoding distortions. Fig. 9 shows a JPEG encoded version of Bavarian couple with parameters of 5% quality and 0% smoothing, which results in very significant distortions of the image. The response of the watermark detector in this case is 13.9, which is still well above random.

D. Experiment 4: Dithering Distortion

Fig. 10 shows a dithered version of Bavarian couple. The response of the watermark detector is 5.2, again suggesting that the algorithm is robust to common encoding distortions. In fact, more reliable detection can be achieved simply by removing any nonzero mean from the extracted watermark, as discussed in Section IV-D2. In this case the detection value is 10.5.

E. Experiment 5: Cropping

Fig. 11(a) shows a cropped version of the watermarked image of Fig. 5 in which only the central quarter of the image remains. In order to extract the watermark from this image, the missing portions of the image were replaced with portions from the original unwatermarked image of Fig. 4, as shown

³ However, subsequent experiments have revealed that if small changes of scale are not considered, then the response of the watermark detector is severely degraded.

in Fig. 11(b). In this case, the response of the watermark is 14.6. Once again, this is well above random even though 75% of the data has been removed.

Fig. 12(a) shows a clipped version of the JPEG encoded image of Fig. 8 in which only the central quarter of the image remains. As before, the missing portions of the image were replaced with portions from the original unwatermarked image of Fig. 4, as shown in Fig. 12(b). In this case, the response of the watermark is 10.6. Once more, this is well above random even though 75% of the data has been removed and distortion is present in the clipped portion of the image.

F. Experiment 6: Print, Xerox, and Scan

Fig. 13 shows an image of the Bavarian Couple after 1) printing, 2) xeroxing, then 3) scanning at 300 dpi using a UMAX PS-2400X scanner, and finally 4) rescaling to a size of 256×256 . Clearly, this image suffers from several levels of distortion that accompany each of the four stages. High-frequency pattern noise is especially noticeable. The detector response to the watermark is 4.0. However, if the nonzero mean is removed and only the sign of the elements of the watermark are used, then the detector response is 7.0, which is well above random.

G. Experiment 7: Attack by Watermarking Watermarked Images

Fig. 14 shows an image of Bavarian Couple after five successive watermarking operations, i.e., the original image is watermarked, the watermarked image is watermarked, etc. This may be considered another form of attack in which it is clear that significant image degradation eventually occurs as the process is repeated. This attack is equivalent to adding noise to the frequency bins containing the watermark. Interestingly, Fig. 15 shows the response of the detector to



(a)



(b)

Fig. 12. (a) Clipped version of JPEG encoded (10% quality, 0% smoothing) Bavarian couple. (b) Restored version of Bavarian couple in which missing portions have been replaced with imagery from the original unwatermarked image of Fig. 4.



Fig. 13. Printed, xeroxed, scanned, and rescaled image of Bavarian couple.

1000 randomly generated watermarks, which include the five watermarks present in the image. Five spikes clearly indicate the presence of the five watermarks and demonstrate that successive watermarking does not unduly interfere with the process.

H. Experiment 8: Attack by Collusion

In a similar experiment, we took five separately watermarked images and averaged them to form Fig. 16 in order to simulate a simple collusion attack. As before, Fig. 17 shows the response of the detector to 1000 randomly generated watermarks, which include the five watermarks present in the image. Once again, five spikes clearly indicate the presence of the five watermarks and demonstrate that simple collusion based on averaging a few images is an ineffective attack.



Fig. 14. Image of Bavarian couple after five successive watermarks have been added.

VI. CONCLUSION

A need for electronic watermarking is developing as electronic distribution of copyright material becomes more prevalent. Above, we outlined the necessary characteristics of such a watermark. These are: fidelity preservation, robustness to common signal and geometric processing operations, robustness to attack, and applicability to audio, image and video data.

To meet these requirements, we propose a watermark whose structure consists of k i.i.d. random numbers drawn from a $N(0, 1)$ distribution. We rejected a binary watermark because it is far less robust to attacks based on collusion of several independently watermarked copies of an image. The length of the watermark is variable and can be adjusted to suit the characteristics of the data. For example, longer watermarks

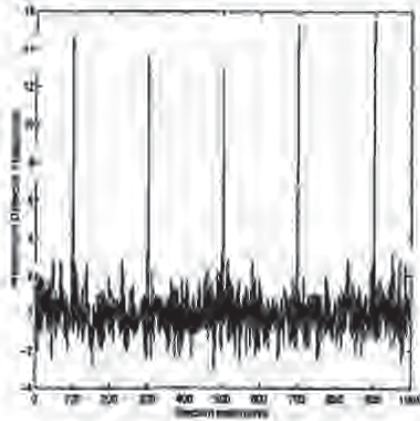


Fig. 16. Watermark detector response to 1000 randomly generated watermarks (including the five specific watermarks) for the watermarked image of Fig. 14. Each of the five watermarks is clearly indicated.

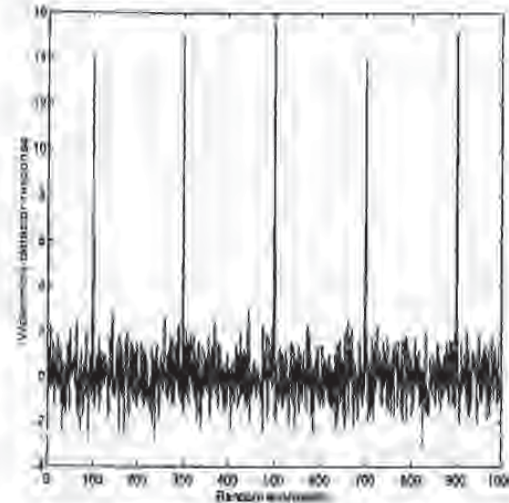


Fig. 17. Watermark detector response to 1000 randomly generated watermarks (including the five specific watermarks) for the watermarked image of Fig. 16. Each of the five watermarks is clearly detected, indicating that collusion by averaging is ineffective.



Fig. 18. Image of Bavarian couple after averaging together five independently watermarked versions of the Bavarian couple image.

may be used for an image that is especially sensitive to large modifications of its spectral coefficients, thus requiring weaker scaling factors for individual components.

We recommend that the watermark be placed in the perceptually most significant components of the image spectrum. This maximizes the chances of detecting the watermark even after common signal and geometric distortions. Further, modification of these spectral components results in severe image degradation long before the watermark itself is destroyed. Of course, to insert the watermark, it is necessary to alter these very same coefficients. However, each modification can be extremely small and, in a manner similar to spread spectrum communication, a strong narrowband watermark may be distributed over a much broader image (channel) spectrum. We have not performed an objective evaluation of the image quality, in part because the image quality can be adjusted to any desired quality by altering the relative power of the watermark using the scale factor term. Of course, as the

watermark strength is reduced to improve the image quality, the robustness of the method is also reduced. It will ultimately be up to content owners to decide what image degradation and what level of robustness is acceptable. This will vary considerably from application to application.

Detection of the watermark then proceeds by adding all of these very small signals, and concentrating them once more into a signal with high SNR. Because the magnitude of the watermark at each location is only known to the copyright holder, an attacker would have to add much more noise energy to each spectral coefficient in order to be sufficiently confident of removing the watermark. However, this process would destroy the image fidelity.

In our experiments, we added the watermark to the image by modifying the 1000 largest coefficients of the DCT (excluding the DC term). These components are heuristically perceptually more significant than others. An important open problem is the construction of a method that would identify perceptually significant components from an analysis of the image and the human perceptual system. Such a method may include additional considerations regarding the relative predictability of a frequency based on its neighbors. The latter property is important in combating attacks that may use statistical analyzes of frequency spectra to replace components with their maximum likelihood estimate. For example, the choice of the DCT is not critical to the algorithm and other spectral transforms, including wavelet type decompositions, are also possible.

We showed, using the Bavarian couple image, that our algorithm can extract a reliable copy of the watermark from imagery that we degraded with several common geometric and signal processing procedures. An important caveat here is that any affine geometric transformation must first be inverted. These procedures include translation, rotation, scale

change, and cropping. The algorithm displays strong resilience to lossy operations such as aggressive scale changes, JPEG compression, dithering and data conversion. The experiments presented are preliminary, and should be expanded in order to validate the results. We are conducting ongoing work in this area. Further, the degree of precision of the registration procedures used in undoing affine transforms must be characterized precisely across a large test set of images.

Application of the method to color images is straightforward. The most common transformation of a color image is to convert it to black and white. Color images are therefore converted into a YIQ representation and the brightness component Y is then watermarked. The color image can then be converted to other formats, but must be converted back to YIQ prior to extraction of the watermark. We therefore expect color images to be robust to the signal transformations we applied to gray-level images. However, robustness to certain color image processing procedures should be investigated. Similarly, the system should work well on text images, however, the binary nature of the image together with its much more structured spectral distribution need more work. We expect that our watermarking methodology should extend straightforwardly to audio and video data. However, special attention must be paid to the time-varying nature of these data.

Broader systems issues must be also addressed in order for this system to be used in practice. For example, it would be useful to be able to prove in court that a watermark is present without publicly revealing the original, unmarked document. This is not hard to accomplish using secure trusted hardware; an efficient purely cryptographic solution seems much more difficult. It should also be noted that the current proposal only allows the watermark to be extracted by the owner, since the original unwatermarked image is needed as part of the extraction process. This prohibits potential users from querying the image for ownership and copyright information. This capability may be desirable but appears difficult to achieve with the same level of tamper resistance. However, it is straightforward to provide if a much weaker level of protection is acceptable and might therefore be added as a secondary watermarking procedure. Finally, we note that while the proposed methodology is used to hide watermarks in data, the same process can be applied to sending other forms of message through media data.

ACKNOWLEDGMENT

I. Cox and T. Shanon thank L. O'Gorman of AT&T Bell Laboratories for bringing this problem to their attention, and S. Roy for testing the robustness of the algorithm. I. Cox thanks H. Stone for advice on image transforms.

REFERENCES

- [1] E. H. Adelson, "Digital signal encoding and decoding apparatus," U.S. Patent 4939 515, 1990.
- [2] G. W. Brunkaway, K. A. Maguire, and F. C. Mintzer, "Color correct digital watermarking of images," U.S. Patent 5530 759, 1996.
- [3] W. Bender, D. Gröll, and N. Morimoto, "Techniques for data hiding," in *Proc. SPIE*, vol. 2420, p. 40, Feb. 1994.
- [4] J. Drossi, S. Low, M. Masamchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," in *Proc. Infocom '94*, pp. 1278-1287.
- [5] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in *Advances in Cryptology: Proc. CRYPTO'95*. New York: Springer-Verlag, 1995.
- [6] G. Caronni, "Assuring ownership rights for digital images," in *Proc. Reliable IT Systems, VIS'95*.
- [7] I. J. Cox, S. Roy, and S. L. Hingorani, "Dynamic histogram warping of images pairs for constant image brightness," in *IEEE Int. Conf. Image Processing*, 1995.
- [8] O. Faugeras, *Three-Dimensional Computer Vision: A Geometric Viewpoint*. Cambridge, MA: MIT Press, 1993.
- [9] A. Gersho and R. Gray, *Vector Quantization and Signal Compression*. Boston, MA: Kluwer, 1992.
- [10] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. New York: Addison-Wesley, 1993.
- [11] P. J. Huber, *Robust Statistics*. New York: Wiley, 1981.
- [12] H. Jayant, J. Johanson, and R. Safranek, "Signal compression based on models of human perception," in *Proc. IEEE*, vol. 81, no. 10, 1993.
- [13] J. Kilian et al., "Resistance of watermarked documents to collusional attacks," in preparation.
- [14] E. Koeh, J. Radford, and J. Zhao, "Copyright protection for multimedia data," in *Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994.
- [15] E. Koeh and J. Zhao, "Toward robust and hidden image copyright labeling," in *Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, June 1995.
- [16] J. S. Lim, *Two-Dimensional Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1990.
- [17] F. T. Leighton and S. Micali, "Secret-key agreement without public-key cryptography," in *Proc. Cryptology*, 1993.
- [18] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," in *Proc. IEEE*, vol. 83, pp. 944-957, 1995.
- [19] K. Mitsu and K. Tanaka, "Video-sineography," in *Proc. IMA Intellectual Property Project*, 1994, vol. 1, pp. 187-206.
- [20] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications—A tutorial," *IEEE Trans. Commun.*, vol. COM-30, pp. 855-884, 1982.
- [21] G. B. Rhoads, "Identification/authentication coding method and apparatus," Rep. WIPO/WO 95/14289, World Intellectual Property Org., 1995.
- [22] W. F. Schreiber, A. E. Lippman, E. H. Adelson, and A. N. Netravali, "Receiver-compatible enhanced definition television system," U.S. Patent 5010 405, 1991.
- [23] C. W. Therrien, *Decision Estimation and Classification: An Introduction to Pattern Recognition and Related Topics*. New York: Wiley, 1989.
- [24] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. 1990 IEEE Military Communications Conf.*, 1990, pp. 216-220.
- [25] L. F. Turner, "Digital data security system," Patent 409 WO 8900013, 1989.
- [26] R. O. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Int. Conf. Image Processing*, 1994, vol. 2, pp. 86-90.



Ingemar J. Cox (S'79-M'83-SM'95) received the Ph.D. degree from Oxford University, Oxford, U.K., in 1983.

From 1984 to 1989, he was a principal investigator in the Robotics Principles Department, AT&T Bell Laboratories, Murray Hill, NJ, where his research interests focused on issues of autonomous mobile robots. He joined NEC Research Institute, Princeton, NJ, as a senior research scientist in 1989. His principal research interests are broadly in computer vision, specifically tracking, stereo and 3-D estimation, and multimedia, especially image database retrieval and electronic watermarking for copyright protection.



Joe Killian received the B.S. degree in computer science and in mathematics in 1985, and the Ph.D. in mathematics in 1989, both from the Massachusetts Institute of Technology, Cambridge.

He is a Research Scientist with NEC Research Institute, Princeton, NJ. His research interests are in complexity theory and cryptography.



Talal Shamoon (S'84-M'95) received the Ph.D. degree in electrical engineering from Cornell University, Ithaca, NY, in January 1995.

He joined the NEC Research Institute (NECI), Princeton, NJ, in December of 1994, where he held the title of Scientist. He joined the InterTrust STAR Laboratory, Sunnyvale, CA, in 1997, where he is currently a Member of the Research Staff working on problems related to trusted rights management of multimedia content. His research interests include algorithms for audio, image and video coding and

processing, multimedia security, data compression, and acoustic transducer design. He has worked on high-fidelity audio coding and fast search algorithms for large image data bases. Since joining NECI, he has been actively involved in research on watermarking for multimedia systems.



F. Thomson Leighton received the B.S.E. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1978, and the Ph.D. degree in applied mathematics from the Massachusetts Institute of Technology (MIT), Cambridge, in 1981.

He is a Professor of applied mathematics and a member of the Laboratory for Computer Science (LCS) at MIT. He was a Bantrell Postdoctoral Research Fellow at LCS from 1981 to 1983, and he joined the MIT faculty as an Assistant Professor

of applied mathematics in 1982. He is a leader in the development of networks and algorithms for message routing in parallel machines, particularly in the use of randomness in wiring to overcome problems associated with congestion, blocking, and faults in networks. He has published over 100 research papers on parallel and distributed computing and related areas. He is the author of two books, including a leading text on parallel algorithms and architectures.

A Public Key Watermark for Image Verification and Authentication

Ping Wah Wong
Hewlett Packard Company
11000 Wolfe Road
Cupertino, CA 95014

Abstract

We propose in this paper a public key watermarking algorithm for image integrity verification. This watermark is capable of detecting any change made to an image, including changes in pixel values and image size. This watermark is important for several imaging applications, including trusted camera, legal usage of images, medical archiving of images, news reporting, commercial image transaction, and others. In each of these applications, it is important to verify that the image has not been manipulated and that the image was originated by either a specific camera or a specific user. The verification (the watermark extraction) procedure uses a public key as in public key cryptography, and hence it can be performed by any person without the secure exchange of a secret key. This is very important in many applications (e.g., trusted camera, news reporting) where the exchange of a secret key is either not possible or undesirable.

1 Introduction

Digital watermarking is a technique to insert a digital signature into an image so that the signature can be extracted for the purposes of ownership verification and/or authentication. This type of technology is becoming increasingly important due to the popularity of the usage of digital images on the World Wide Web and in electronic commerce.

There are different types of watermarking schemes that are designed for different applications [1, 2]. One type of watermark is designed to ensure the integrity of images, i.e., it can detect any change to an image as well as localizing the areas that have been changed. Since digital images can be altered or manipulated with ease, the ability to detect changes to digital images is very important for many applications such as news reporting, medical archiving, or legal usages. Another need for image authentication arises in, for example, electronic commerce where a buyer purchases a digital image from a seller, and then the seller transmits the digital image to the buyer over the

network. In this case the buyer wants to ensure that the received image is indeed the genuine image sent by the seller. Here we not only want to verify the integrity of an image, we also want to check the original ownership.

Previously, the idea of a trusted camera [3] was proposed. This scheme computes for each captured image a standard digital signature. The digital signature is stored and transmitted along with the image. The integrity of the output digital image can be checked using standard digital signature techniques. Recently Yeung and Mintzer [4] propose a verification watermarking method based on indexing to a random sequence. This method detects changes to the pixel values, but it does not detect changes in image size due to scaling or cropping. Wong [5] proposes a secret key watermarking method where a user can detect any change to the pixel values and to the size of the image. The security of this method resides in a secret user key used in conjunction with a cryptographic hash function. Since this is a secret key scheme, only the user who has possession of the secret key can carry out the verification procedure. There is also the undesirable requirement whereby the secret key must be communicated through a separate secure channel.

In this paper, we extend the secret key verification watermark into a public key scheme so that the integrity and ownership of the image can be verified using a public key. In such a system, the owner of the image inserts a watermark using a private key K' . In the watermark extraction procedure, any person can use the public key K (corresponding to the private key K') to extract a watermark. Any change made to the watermarked image can be detected by a visual inspection of the extracted watermark. As in public key cryptographic systems [6, 7], the public key in this watermarking scheme can be published without compromising the security of the system.

2 Watermark Insertion and Extraction

We describe in this section our public key authentication watermarking algorithm for grayscale images. For color images, the same technique can be applied independently to the color planes of the image, either in the RGB color space or in any other color space such as YUV.

Consider a grayscale image $x_{m,n}$ of size M by N pixels. We want to insert a binary watermark image $b_{m,n}$ to $x_{m,n}$ to obtain the watermarked image $y_{m,n}$. To this end, we partition the image into blocks of size I by J pixels, and insert a block of the watermark into each block of image data.

Let $a_{m,n}$ be a bi-level image that we will use as our watermark, to be embedded in $x_{m,n}$. Note that $a_{m,n}$ need not be of the same size as $x_{m,n}$. From $a_{m,n}$, we form another bi-level image $b_{m,n}$ of size M by N (same size as $x_{m,n}$). In our example, we form $b_{m,n}$ by tiling $a_{m,n}$, i.e., periodically replicating $a_{m,n}$ to the desired size. We then partition $b_{m,n}$ into blocks of I by J pixels. Each block of $b_{m,n}$ is then inserted into the corresponding block $x_{m,n}$ to give a watermarked block of $y_{m,n}$.

The watermark insertion and extraction procedures for each block are shown in Figs. 1 and 2, respectively.

2.1 Watermark Insertion

Let X_r denote the r^{th} block of data within the image $x_{m,n}$. We form the corresponding block \tilde{X}_r , where each element in \tilde{X}_r equals the corresponding element in X_r , except that the least significant bit is set to zero. Let $H(\cdot)$ be a cryptographic hash function such as the MD5 [8]. We compute the hash

$$H(M, N, \tilde{X}_r) = (p_1^r, p_2^r, \dots, p_s^r) \quad (1)$$

where p_i^r denotes the output bits from the hash function, and s is size of the output bits that is dependent on the specific hash function used. For example, $s = 128$ for MD5. In our algorithm we need to make sure to select a block size such that $IJ \leq s$. Let P_r be the first IJ bits from the bit stream, i.e.,

$$P_r \hat{=} (p_1^r, p_2^r, \dots, p_{IJ}^r).$$

We combine P_r with a corresponding block B_r in $b_{m,n}$ using an exclusive or function. That is, we compute $W_r = P_r \oplus B_r$, where \oplus denotes the element-wise exclusive OR operation between the two blocks. Finally we encrypt W_r with a public key cryptographic system [7] to give

$$G_r = E_{K'}(W_r)$$

where $E(\cdot)$ is the encryption function of the public key system, and K' is the private key. The binary block of

data G_r is then embedded into the least significant bit of \tilde{X}_r to form a block Y_r of the watermarked image.

2.2 Watermark Extraction

In the extraction procedure, we split the input image block Z_r into two pieces; the first piece G_r contains the least significant bits, and the other piece \tilde{Z}_r contains the pixel values except that the least significant bits have been zeroed out. We then calculate the hash of M , N and \tilde{Z}_r , and denote the first 64 bits of the output by Q_r . We use a public key decryption algorithm [7] to decrypt G_r with the public key K that corresponds to the private key K' used in the watermark insertion procedure. That is, we calculate

$$U_r = D_K(Z_r).$$

Finally, we compute the output block $O_r = Q_r \oplus U_r$ using an element-wise exclusive or procedure.

3 Experimental Results

We implemented both the public key watermark insertion and extraction procedures as described in the previous section. For the experiments, we used the MD5 [8] as our hash function, and the RSA public key encryption algorithm [7] for encryption and decryption. A vase image shown in Fig. 3 is used for testing the validity and properties of the algorithm. The binary watermark image is the logo image shown in the upper right hand corner of Fig. 3.

Note from the algorithm that if both the watermarked image block and the image size had not been changed since the insertion of a watermark, i.e., if $X_r = Y_r$, then $\tilde{X}_r = \tilde{Z}_r$ and $G_r = C_r$. This implies $P_r = Q_r$ and $U_r = W_r$. Hence the output binary image O_r is identical to the block B_r . If the watermarked image was changed, the output block O_r will appear similar to random noise due to the nature of the hash function. As a result, this algorithm can detect any change to the pixel values to the block level. Since the block sizes are relatively small (we used 8 by 8 in our experiments), we consider this detection to be sufficiently localized.

Since the image size parameters M and N are used in the watermark insertion and extraction procedures of every block, any change in image size will result in the detection of changes in every block of the image. Hence the entire extracted watermark appears like random noise as shown in Fig. 3. In summary, this public key algorithm allows an authentication of image integrity as it can detect any change to an image including changes in pixel values and image size.

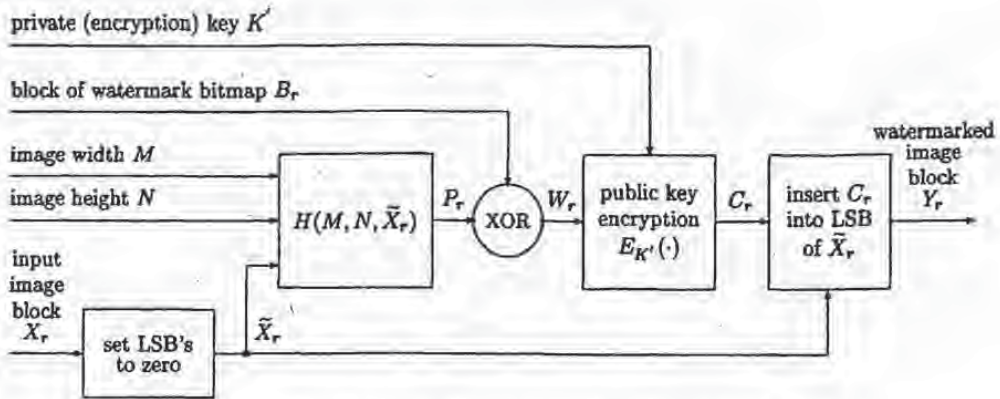


Figure 1: Public key verification watermark insertion procedure.

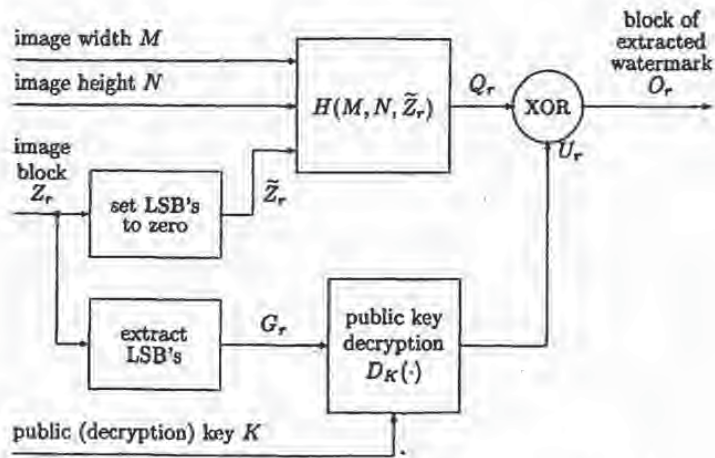


Figure 2: Public key verification watermark extraction procedure.

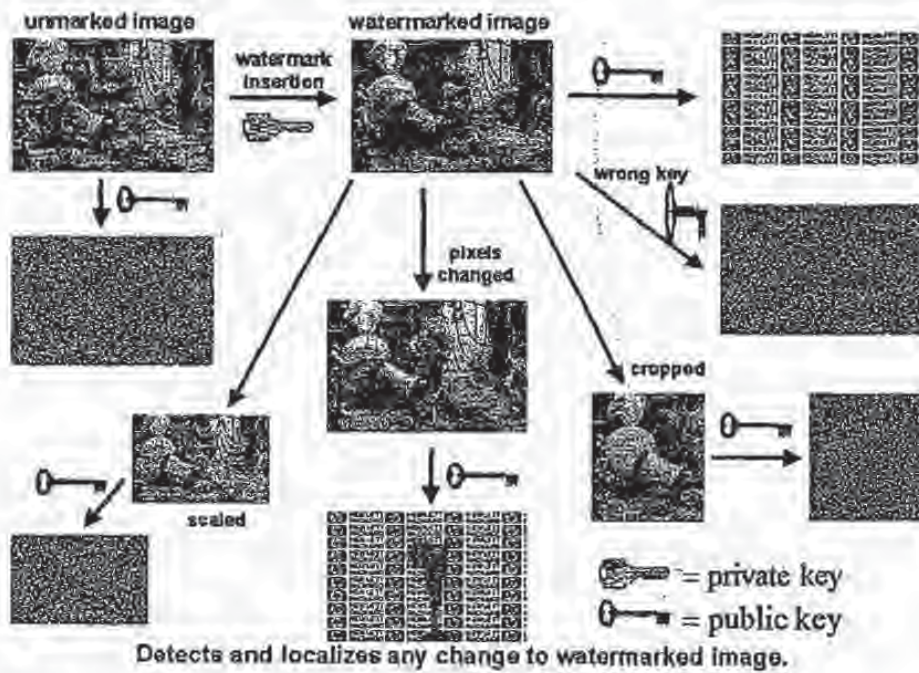


Figure 3: Experimental results summarizing the properties of the public key verification watermark.

4 Properties

As described in the previous section, this public key authentication watermark can detect any change to an image. The verification is performed using the public key of the owner, which also implies the original ownership of the image. Experimental results indicating the properties of this public key verification watermark is summarized in Fig. 3. Here we summarize the properties of the public key authentication watermark.

- The watermark is invisible.
- If one uses the correct public key K in the watermark extraction procedure, one obtains an appropriate watermark.
- If an image is unmarked, i.e., if it does not contain a watermark, the watermark extraction procedure returns an output that resembles random noise as shown in Fig. 3.
- If one applies an incorrect key (for example, if one uses the public key of different owner), then the watermark extraction procedure returns an output that resembles random noise.
- If a watermarked image is cropped or scaled, then the watermark extraction procedure returns an output that resembles random noise.
- If one changes certain pixels in the watermarked image, then the specific locations of the changes are reflected at the output of the watermark extraction procedure. This is shown in the middle and bottom part of Fig. 3 where a glass is painted onto a watermarked image and the extracted watermark indicates the location of the glass.
- Despite embedding the watermark in the least significant bit of the image, the watermark is still secure. Recall that this watermark is designed for authentication purposes, i.e., to detect any change to the image. If someone attempts to remove the watermark by changing some bit planes of the image, the watermark extraction procedure will detect the changes.

5 Conclusion

We described a public key watermarking algorithm in this paper for image verification and authentication purposes. This is an extension of our previous work [5] on a secret key watermarking algorithm for image verification. The importance of the public key extension is that while a private key (secret) is used in watermark insertion, the watermark can be checked using

a public key. As a result, any person can perform the integrity check using a public key without the secure exchange of a secret key.

References

- [1] F. Mintzer, G. Braudaway, and M. M. Yeung, "Effective and ineffective digital watermarks," in *Proceedings of ICIP*, (Santa Barbara, CA), October 1997.
- [2] N. Memon and P. W. Wong, "Protecting digital media content: Watermarks for copyrighting and authentication," *Communications of ACM*, July 1998.
- [3] G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image," *IEEE Transactions on Consumer Electronics*, vol. 39, pp. 905-910, November 1993.
- [4] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proceedings of ICIP*, (Santa Barbara, CA), October 1997.
- [5] P. W. Wong, "A watermark for image integrity and ownership verification," in *Proceedings of IS&T PIC Conference*, (Portland, OR), May 1998.
- [6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 67, pp. 644-654, November 1976.
- [7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, February 1978.
- [8] R. L. Rivest, "The MD5 message digest algorithm." Internet RFC 1321, April 1992.

Attacks on Copyright Marking Systems

Fabien A.P. Petitcolas*, Ross J. Anderson, and Markus G. Kuhn**

University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, UK
{fapp2,rja14,mgk25}@cl.cam.ac.uk
<<http://www.cl.cam.ac.uk/Research/Security/>>

Abstract. In the last few years, a large number of schemes have been proposed for hiding copyright marks and other information in digital pictures, video, audio and other multimedia objects. We describe some contenders that have appeared in the research literature and in the field; we then present a number of attacks that enable the information hidden by them to be removed or otherwise rendered unusable.

1 Information Hiding Applications

The last few years have seen rapidly growing interest in ways to hide information in other information. A number of factors contributed to this. Fears that copyright would be eroded by the ease with which digital media could be copied led people to study ways of embedding hidden copyright marks and serial numbers in audio and video; concern that privacy would be eroded led to work on electronic cash, anonymous remailers, digital elections and techniques for making mobile computer users harder for third parties to trace; and there remain the traditional 'military' concerns about hiding one's own traffic while making it hard for the opponent to do likewise.

The first international workshop on information hiding [3] brought these communities together and a number of hiding schemes were presented there; more have been presented elsewhere. We formed the view that useful progress in steganography and copyright marking might come from trying to attack all these first generation schemes. In the related field of cryptology, progress was iterative: cryptographic algorithms were proposed, attacks on them were found, more algorithms were proposed, and so on. Eventually, theory emerged: fast correlation attacks on stream ciphers and differential and linear attacks on block ciphers, now help us understand the strength of cryptographic algorithms in much more detail than before. Similarly, many cryptographic protocols were proposed and almost all the early candidates were broken, leading to concepts of protocol robustness and techniques for formal verification [7].

* The first author is grateful to Intel Corporation for financial support under the grant 'Robustness of Information Hiding Systems'

** The third author is supported by a European Commission Marie-Curie grant

So in this paper, we first describe the copyright protection context in which most recent schemes have been developed; we then describe a selection of these schemes and present a number of attacks, which break most of them. We finally make some remarks on the meaning of robustness in the context of steganography in general and copyright marking in particular.

1.1 Copyright Protection Issues

Digital recording media offer many new possibilities but their uptake has been hindered by widespread fears among intellectual property owners such as Hollywood and the rock music industry that their livelihoods would be threatened if users could make unlimited perfect copies of videos, music and multimedia works.

One of the first copy protection mechanisms for digital media was the serial copy management system (SCMS) introduced by Sony and Phillips for digital audio tapes in the eighties [34]. The idea was to allow consumers to make a digital audio tape of a CD they owned in order to use it (say) in their car, but not to make a tape of somebody else's tape; thus copies would be limited to first generation only. The implementation was to include a Boolean marker in the header of each audio object. Unfortunately this failed because the hardware produced by some manufacturers did not enforce it.

More recently the Digital Video Disk, also known as Digital Versatile Disk (DVD) consortium called for proposals for a copyright marking scheme to enforce serial copy management. The idea is that the DVD players sold to consumers will allow unlimited copying of home videos and time-shifted viewing of TV programmes, but cannot easily be abused for commercial piracy [21,46]. The proposed implementation is that videos will be unmarked, or marked 'never copy', or 'copy once only'; compliant players would not record a video marked 'never copy' and when recording one marked 'copy once only' would change its mark to 'never copy'. Commercially sold videos would be marked 'never copy', while TV broadcasts and similar material would be marked 'copy once only' and home videos would be unmarked.

Electronic copyright management schemes have also been proposed by European projects such as Imprimatur and CITED [47, 68, 69], and American projects such as the proposed by the Working Group on Intellectual Property Rights [71].

1.2 Problems

Although these schemes might become predominant in areas where they can be imposed from the beginning (such as DVD and video-on-demand), they suffer from a number of drawbacks. Firstly, they rely on the tamper-resistance of consumer electronics – a notoriously unsolved problem [5]. The tamper-resistance mechanisms being built into DVD players are fairly rudimentary and the history of satellite TV piracy leads us to expect the appearance of 'rogue' players which will copy everything. Electronic copyright management schemes also conflict with applications such as digital libraries, where 'fair use' provisions are

strongly entrenched. According to Samuelson, '*Tolerating some leakage may be in the long run of interest to publishers [...] For educational and research works, pay-per-use schemes may deter learning and deep scholarship*' [58]. A European legal expert put it even more strongly: that copyright laws are only tolerated because they are not enforced against the large numbers of petty offenders [35].

Similar issues are debated within the software industry; some people argue, for example, that a modest level of amateur software piracy actually enhances revenue because people may 'try out' software they have 'borrowed' from a friend and then go on to buy it (or the next update).

For all these reasons, we may expect leaks in the primary copyright protection mechanisms and wish to provide independent secondary mechanisms that can be used to trace and prove ownership of digital objects. It is here that marking techniques are expected to be most important.

2 Copyright Marks

There are two basic kinds of mark: fingerprints and watermarks. One may think of a fingerprint as an embedded serial number while a watermark is an embedded copyright message. The first enables us to trace offenders, while the second can provide some of the evidence needed to prosecute them. It may also, as in the DVD proposal, form part of the primary copy management system; but it will more often provide an independent back-up to a copy management system that uses overt mechanisms such as digital signatures.

In [8], we discussed the various applications of fingerprinting and watermarking, their interaction, and some related technologies. Here, we are concerned with the robustness of the underlying mechanisms. What sort of attacks are possible on marking schemes? What sort of resources are required to remove marks completely, or to alter them so that they are read incorrectly? What sort of effect do various possible removal techniques have on the perceptual quality of the resulting audio or video?

We will use the terminology agreed at the first international workshop on Information Hiding [54]. The information to be hidden (watermark, fingerprint, or in the general case of steganography, a secret message) is *embedded* in a *cover* object (a cover CD, a cover video, a cover text, etc.) giving a *stego* object, which in the context of copyright marking we may also call a *marked* object (CD, video, etc.). The embedding is performed with the help of a *key*, a secret variable that is in general known to the object's owner. Recovery of the embedded mark may or may not require a key; if it does the key may be equal to, or derived from, the key used in the embedding process.

In the rest of this section, we will first discuss simple hiding methods and the obvious attacks on them. We will then present, as an example of the 'state of the art', robustness requirements that appeared in a recent music industry request for proposals [1]. We will then present the main contending techniques used in currently published and fielded systems. Attacks on these systems will then be presented.

2.1 Simple Hiding Methods

The simplest schemes replace all the bits in one or more of the less significant bit planes of an image or audio sample with the 'hidden' information [12, 26, 39, 67]. This is particularly easy with pictures: even when the four least significant bits of the cover image are replaced with the four most significant bits of the embedded image, the eye cannot usually tell the difference [39]. Audio is slightly harder, as the randomisation of even the least significant bit of 8-bit audio adds noise that is audible during quiet passages of music or pauses in speech. Nonetheless, several systems have been proposed: they include embedding, in the regular channels of an audio CD, another sound channel [27, 70] and a steganographic system in which secret messages are hidden in the digitised speech of an ISDN telephone conversation [26].

However, bit-plane replacement signals are not only easy to detect. They violate Kerckhoffs' principle that the security of a protection system should not rely on its method of operation being unknown to the opponent, but rather on the choice of a secret key [36]. Better approaches use a key to select some subset of pixels or sound samples which then carry the mark.

An example of this approach is Chameleon [6], a system which enables a broadcaster to send a single ciphertext to a large population of users, each of which is supplied with a slightly different decryption key; the effect of this is to introduce a controlled number of least-significant-bit errors into the plaintext that each user decrypts. With uncompressed digital audio, the resulting noise is at an acceptably low level and then Chameleon has the advantage that the decrypted audio is fingerprinted automatically during decryption without any requirement that the consumer electronic device be tamper-resistant.

In general, schemes which use a key to choose some subset of least significant bits to tweak may provide acceptable levels of security in applications where the decrypted objects are unlikely to be tampered with. However, in many applications, a copyright pirate may be able and willing to perform significant filtering operations and these will destroy any watermark, fingerprint or other message hidden by simple bit tweaking. So we shall now consider what it means for a marking scheme to be robust.

2.2 Robustness Requirements

The basic problem is to embed a mark in the digital representation of an analogue object (such as a film or sound recording) in such a way that it will not reduce the perceived value of the object while being difficult for an unauthorised person to remove. A first pass at defining robustness in this context may be found in a recent request for proposals for audio marking technology from the International Federation for the Phonographic Industry, IFPI [1]. The goal of this exercise was to find a marking scheme that would generate evidence for anti-piracy operations, track the use of recordings by broadcasters and others and control copying. The IFPI robustness requirements are as follows:

- the marking mechanism should not affect the sonic quality of the sound recording;
- the marking information should be recoverable after a wide range of filtering and processing operations, including two successive D/A and A/D conversions, steady-state compression or expansion of 10%, compression techniques such as MPEG and multi-band nonlinear amplitude compression, adding additive or multiplicative noise, adding a second embedded signal using the same system, frequency response distortion of up to 15 dB as applied by bass, mid and treble controls, group delay distortions and notch filters;
- there should be no other way to remove or alter the embedded information without sufficient degradation of the sound quality as to render it unusable;
- given a signal-to-noise level of 20 dB or more, the embedded data channel should have a bandwidth of 20 bits per second, independent of the signal level and type (classical, pop, speech).

Similar requirements could be drawn up for marking still pictures, videos and multimedia objects in general. However, before rushing to do this, we will consider some systems recently proposed and show attacks on them that will significantly extend the range of distortions against which designers will have to provide defences, or greatly reduce the available bandwidth, or both.

2.3 General Techniques

We mentioned schemes that modify the least significant bits of digital media; by repeating such marks, or employing more robust encoding methods, we can counter some filtering attacks. We can also combine coding with various transform techniques (DCT, wavelet and so on).

The *Patchwork* algorithm [11], for instance, successively selects random pairs of pixels; it makes the brighter pixel brighter and the duller pixel duller and the contrast change in this pixel subset encodes one bit. To maintain reasonable robustness against filtering attacks, the bandwidth of such systems has to be limited to at most a few hundred bits per image [40, 41]. In a similar way, marks can be embedded in audio by increasing the amplitude contrast of many pairs of randomly chosen sound samples and using a suitable filter to minimise the introduction of high-frequency noise.

More sophisticated variants on this theme involve spread-spectrum techniques. Although these have been used since the mid-fifties in the military domain because of their anti-jamming and low-probability-of-intercept properties [61], their applicability to image watermarking has only been noticed recently by Tirkel *et al.* [66]. Since then a number of systems based on this technique have been proposed [67, 72, 73]: typically a maximal length sequence is added to the signal in the spatial domain and the watermark is detected by using the spatial cross-correlation of the sequence and the watermarked image.

Another kind of marking technique embeds the mark in a transform domain, typically one that is widely used by compression algorithms. Thus when marking sound one could add a pseudorandom sequence to the excitation signal in

an LPC or CELP coded audio signal [45] and when marking an image one could use the DCT domain. Langelaar *et al.* remove certain high frequency DCT coefficients [41]; Cox *et al.* modulate the 1000 largest DCT coefficients of an image with a random vector [19]; Koch *et al.* change the quantisation of the DCT coefficients and modify some of them in such a way that a certain property (order in size) is verified [37]; while Ó Ruanaidh *et al.* modulate the DCT coefficient with a bi-directional coding [49].

Techniques of this kind are fairly robust against various kinds of signal processing and may be combined with exploitation of the perceptual masking properties of the human auditory system in [16, 17] and of the human vision system in [28, 65, 64]. The basic idea here is to amplify the mark wherever the changes will be less noticeable and also to embed it in the *perceptually significant* components of the signal [20]. Masking may also be used to avoid placing marks in places such as the large expanses of pure colour found in cartoons; the colour histogram of such images has sharp peaks, which are split into twin peaks by some naïve marking methods as the colour value c is replaced by $c - \delta$ and $c + \delta$, thus allowing the mark to be identified and removed [44].

3 Attacks

This leads us to the topic of attacks and here we present some quite general kinds of attack that destroy, or at least reveal significant limitations of, several marking schemes: PictureMarc 1.51 [24, 56], SysCoP [37, 74, 75], JK_PGS (EPFL algorithm, part of the European TALISMAN project), SureSign [63], EIKONA-mark [25, 55], Echo Hiding, and the NEC method [19]. We suspect that systems that use similar techniques are also vulnerable to our attacks.

3.1 The Jitter Attack

Our starting point in developing a systematic attack on marking technology was to consider audio marking schemes that tweak low order bits whose location is specified by a key. A simple and devastating attack on these schemes is to add jitter to the signal. In our first implementation, we split the signal into chunks of 500 samples, either duplicated or deleted a sample at random in each chunk (resulting in chunks of 499 or 501 samples long) and stuck the chunks back together. This turned out to be almost imperceptible after filtering, even in classical music; but the jitter prevents the marked bits from being located.

In a more sophisticated implementation, we resample these chunks at a lower or higher frequency. This relies on the properties of the ear's pitch resolution:

In pitch perception experiments in the mid-audio frequency range, subjects are able to perceive changes in frequency of pure tones of approximately 0.1%. [...] At frequencies above 4 kHz pitch discrimination reduces substantially. [...] In the case of complex signals, such as speech, it is very much less clear what the capabilities and processes of the auditory system are. [...] There is evidence that peaks in the spectrum of

the audio signal are detected more easily than features between spectral peaks. *J.N. Holmes* [33]

If n_i is the number of samples in the i th chunk, n'_i the number of samples after resampling and α the maximum relative change of frequency allowed then, in the mid-audio range, we are roughly limited, for pure tones, by $|\Delta n_i| \leq \alpha n_i$ (because α is small), where $\Delta n_i := n'_{i+1} - n'_i$. This can be simplified as $0 < k \leq \frac{\alpha n}{v}$ when the n_i are equal and when the number k of removed or added samples is constant for each chunk. This is the approach we chose; it allowed us to introduce a long jitter. Then the strategy for choosing k and n depends on the input signal. With this technique we were able to tweak up to one sample in 50 of a 44 kHz sampled voice recording without any perceptible effect.

We also applied a similar attack to SysCoP Demo 1.0. In that case we simply deleted columns of pixels and duplicated others in order to preserve the image size. Fig. 1 gives an example of this attack.

Of course, there are much more subtle distortions that can be applied. For instance, in [30], Hamdy *et al.* present a way to increase or decrease the length of a music performance without changing the pitch; this was developed to enable radio broadcasters to slightly increase or decrease the playing time of a musical track. As such tools become widely available, attacks involving sound manipulation will become easy. Most simple spread-spectrum based techniques are subject to this kind of attacks. Indeed, although spread-spectrum signals are very robust to distortion of their amplitude and to noise addition, they do not survive timing errors: synchronisation of the chip signal is very important and simple systems fail to recover this synchronisation properly.

3.2 StirMark

Following this attack and after evaluating some watermarking software, it became clear that although many of the seriously proposed schemes could survive basic manipulations – that is, manipulations that can be done easily with standard tools, such as rotation, shearing, resampling, resizing and lossy compression – they would not cope with combinations of them. This motivated us to implement StirMark.

StirMark is a generic tool developed for simple robustness testing of image marking algorithms and other steganographic techniques. In its simplest version, StirMark simulates a resampling process, i.e. it introduces the same kind of errors into an image as printing it on a high quality printer and then scanning it again with a high quality scanner. It applies a minor geometric distortion: the image is slightly stretched, sheared, shifted and/or rotated by an unnoticeable random amount¹ (Fig. 2 – middle drawing) and then resampled using either bi-linear or

¹ If A , B , C and D are the corners of the image, a point M of the said image can be expressed as $M = \alpha[\beta A + (1 - \beta)D] + (1 - \alpha)[\beta B + (1 - \beta)C]$ where $0 \leq \alpha, \beta \leq 1$ are the coordinates of M relatively to the corners. The distortion is done by moving the corners by a small random amount in both directions. The new coordinates of M are given by the previous formula, keeping (α, β) constant.

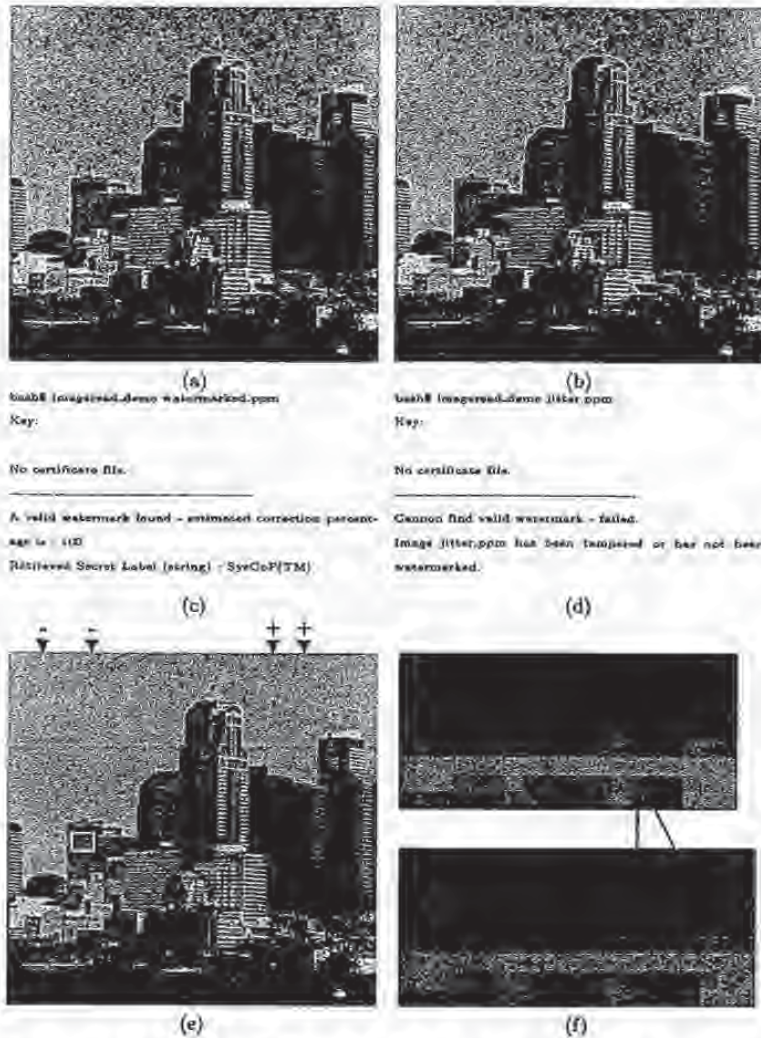


Fig. 1. A successful jitter attack on SysCoP. We used the demo software release 1.0 available on SysCoP's Web site [76]. (a) shows an image watermarked with SysCoP and (b) the same image but after the attack. In the first case the software detects the watermark correctly (c) but the check fails on the modified image (d). Here, the attack simply consists in deleting and duplicating some columns of pixels such that the original size of the picture is conserved. (e) shows the columns which have been deleted (-) and duplicated (+). Finally, (f) is a magnified view of the white rectangle in (e); the bottom part corresponds to the original image.

Nyquist interpolation. In addition, a transfer function that introduces a small and smoothly distributed error into all sample values is applied. This emulates the small non-linear analog/digital converter imperfection typically found in scanners and display devices. StirMark introduces a practically unnoticeable quality loss in the image if it is applied only once. However after a few iterated applications, the image degradation becomes noticeable.

With these simple geometrical distortions we could confuse most marking systems available on the market. More distortions - still unnoticeable - can be applied to a picture. We applied a global 'bending' to the image: in addition to the general bi-linear property explained previously a slight deviation is applied to each pixel, which is greatest at the center of the picture and almost null at the borders. On top of this a higher frequency displacement of the form $\lambda \sin(\omega_x x) \sin(\omega_y y) + n(x, y)$ - where n is a random number - is added. In order for these distortions to be most effective, a medium JPEG compression is applied at the end.



Fig. 2. We exaggerate here the distortion applied by StirMark to still pictures. The first drawing corresponds to the original picture; the others show the picture after StirMark has been applied - without and with bending and randomisation.

For those unfamiliar with digital image signal processing we shall now summarise briefly the main computation steps. Apart from a few simple operations such as rotations by 90 or 180 degrees, reflection and mirroring, image manipulation usually requires resampling when destination pixels do not line up with source pixels. In theory, one first generates a continuous image from the digital one, then modifies the continuous image, finally samples this to create a new digital image. In practice, however, we compute the inverse transform of a new pixel and evaluate the reconstruction function at that point.

There are numerous reconstruction filters. In a first version of the software we simply used a linear interpolation but, as foreseen, this tended to blur the image too much, making the validity of the watermark removal arguable. Then we implemented the sine function as a reconstruction filter, which gives theoretically perfect reconstruction for photo images and can be described as follows. If (z, y) are the coordinates of the inverse transform - which, in our case is a distortion of the picture - of a point in the new image and f the function to be reconstructed,

then, an estimate of f at (x, y) is given by $\hat{f}(x, y) = \sum_{i=-n}^n \sum_{j=-n}^n \text{sinc}(x - i) \text{sinc}(y - j) f_{i,j}$. This gives very much better results than the simple filter; an example of the removal of an NEC watermark is given in Fig. 3.

We suggest that image watermarking tools which do not survive StirMark – with default parameters – should be considered unacceptably easy to break. This immediately rules out the majority of commercial marking schemes.

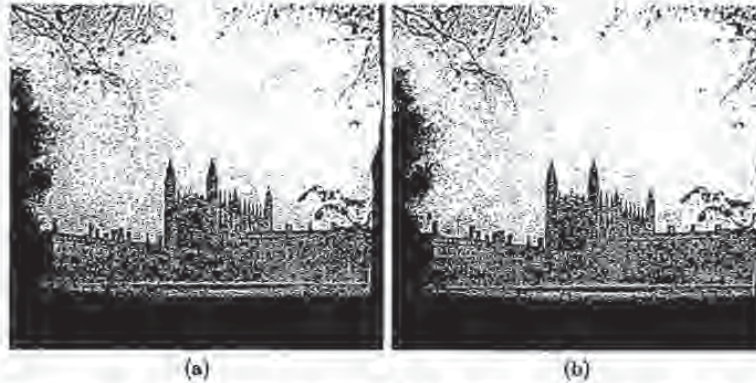


Fig. 3. Kings' College Chapel, courtesy of John Thompson, JetPhotographic, Cambridge. For this example we watermarked a picture with NEC's algorithm [19]. We used the default parameters suggested by their paper ($N = 1000$ and $\alpha = 0.1$). (a) is the watermarked image. We then applied StirMark (b) and tested the presence of the watermark. The similarity between the original watermark and the extracted watermark was 3.74 instead of 21.08. This is well below the decision threshold.

One might try to increase the robustness of a watermarking system by trying to foresee the possible transforms used by pirates; one might then use techniques such as embedding multiple versions of the mark under suitable inverse transforms; for instance Ó Ruanaidh and Pereira suggest to use the Fourier-Mellin transform² to cope with rotation and scaling [50]. However, the general theme of the attacks we have developed and described above is that given a target marking scheme, we invent a distortion (or a combination of distortions) that will remove it or at least make it unreadable, while leaving the perceptual value of the previously marked object undiminished. We are not limited in this process to the distortions produced by common analogue equipment, or considered in the IFPI request for proposals cited above.

² The Fourier-Mellin transform is equivalent to the Fourier transform on a log-polar map: $(x, y) \rightarrow (\mu, \theta)$ with $x = e^{\mu} \cos \theta$ and $y = e^{\mu} \sin \theta$.

As an analogy, one might consider the 'chosen protocol attack' on authentication schemes [60]. It is an open question whether there is any marking scheme for which a chosen distortion attack cannot be found.

3.3 The Mosaic Attack

This point is emphasised by a 'presentation' attack, which is of quite general applicability and which possesses the initially remarkable property that a marked image can be unmarked and yet still rendered pixel for pixel in exactly the same way as the marked image by a standard browser.

The attack was motivated by a fielded automatic system for copyright piracy detection, consisting of a watermarking scheme plus a web crawler that downloads pictures from the net and checks whether they contain a watermark.

It consists of chopping an image up into a number of smaller subimages, which are embedded in a suitable sequence in a web page. Common web browsers render juxtaposed subimages stuck together, so they appear identical to the original image (Fig. 4). This attack appears to be quite general; all marking schemes require the marked image to have some minimal size (one cannot hide a meaningful mark in just one pixel). Thus by splitting an image into sufficiently small pieces, the mark detector will be confused [53]. The best that one can hope for is that the minimal size could be quite small and the method might therefore not be very practical.

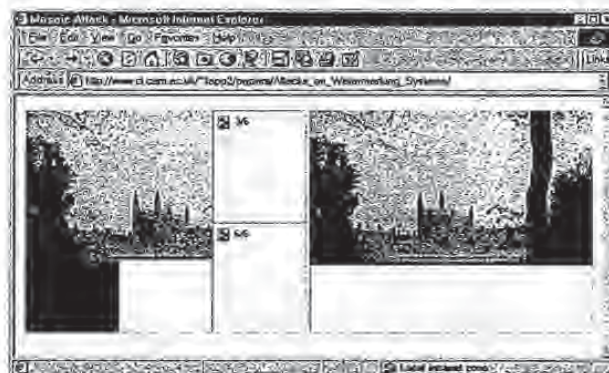


Fig. 4. Screen-shot of a web browser while downloading an image after the mosaic attack. This attack chops a watermarked image into smaller images which are stuck back together when the browser renders the page. We implemented software that reads a JPEG picture and produces a corresponding mosaic of small JPEG images as well as the necessary HTML code automatically [53]. In some cases downloading the mosaic is even faster than downloading the full image! In this example we used a 350 × 280-pixel image watermarked using PictureMarc 1.51.

There are other problems with such 'crawlers'. Java applets, ActiveX controls, etc. can be embedded to display a picture inside the browser; the applet could even de-scramble the picture in real time. Defeating such techniques would entail rendering the web page, detecting pictures and checking whether they contain a mark. An even more serious problem is that much current piracy is of pictures sold via many small services, from which the crawler would have to purchase them using a credit card before it could examine them. A crawler that provided such 'guaranteed sales' would obviously become a target.

3.4 Attack on *Echo Hiding*

One of the few marking schemes to be robust against the jitter attack is echo hiding, which hides information in sound by introducing echoes with very short delays. *Echo hiding* [29] relies on the fact that we cannot perceive short echoes (say 1 ms) and embeds data into a cover audio signal by introducing an echo characterised by its delay τ and its relative amplitude α . By using two types of echo it is possible to encode ones and zeros. For this purpose the original signal is divided into chunks separated by spaces of pseudo-random length; each of these chunks will contain one bit of information.

The echo delays are chosen between 0.5 and 2 milliseconds and the best relative amplitude of the echo is around 0.8. According to its creators, decoding involves detecting the initial delay and the auto-correlation of the cepstrum of the encoded signal is used for this purpose.

The 'obvious' attack on this scheme is to detect the echo and then remove it by simply inverting the convolution formula; the problem is to detect the echo without knowledge of either the original object or the echo parameters. This is known as 'blind echo cancellation' in the signal processing literature and is known to be a hard problem in general.

We tried several methods to remove the echo. Frequency invariant filtering [51, 59] was not very successful. Instead we used a combination of cepstrum analysis and 'brute force' search.

The underlying idea of cepstrum analysis is presented in [15]. Suppose that we are given a signal $y(t)$ which contains a simple single echo, i.e. $y(t) = x(t) + \alpha x(t - \tau)$. If we note Φ_{xx} the power spectrum of x then $\Phi_{yy}(f) = \Phi_{xx}(f)[1 + 2\alpha \cos(2\pi f\tau) + \alpha^2]$ whose logarithm is approximately $\log \Phi_{yy}(f) \approx \log \Phi_{xx}(f) + 2\alpha \cos(2\pi f\tau)$. This is a function of the frequency f and taking its power spectrum raises its 'quefrequency' τ , that is the frequency of $\cos(2\pi\tau f)$. The auto-covariance of this later function emphasises the peak that appears at 'quefrequency' τ (Fig. 5).

To remove the echoes, we need a method to detect the echo delay τ . For this, we used a slightly modified version of the cepstrum: $C \circ \Phi \circ \ln \circ \Phi$ where C is the auto-covariance function³, Φ the power spectrum density function and \circ the composition operator. Experiments on random signals as well as on music show that this method returns quite accurate estimators of the delay (Fig. 6) when an artificial echo has been added to the signal. In the detection function we only

³ $C(x) = E[(x - \bar{x})(x - \bar{x})^*]$.

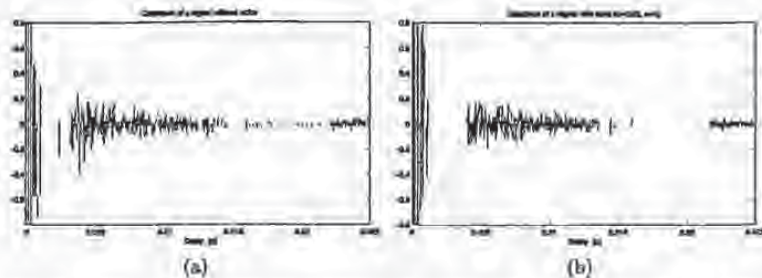


Fig. 5. Graph (a) represents the cepstrum of a signal without echo. Graph (b) is the cepstrum of the same signal with a 20 ms echo which is emphasised by the very clear peak at 0.02 s.

consider echo delays between 0.5 and 3 milliseconds. Below 0.5 ms the function does not work properly and above 3 ms the echo becomes too audible.

Our first attack was to remove an echo with random relative amplitude, expecting that this would introduce enough modification in the signal to prevent watermark recovery. Since echo hiding gives best results for α greater than 0.7 we could use $\hat{\alpha}$ – an estimation of α – drawn from, say a normal distribution centred on 0.8. It was not really successful so our next attack was to iterate: we re-apply the detection function and vary $\hat{\alpha}$ to minimise the residual echo. We could obtain successively better estimators of the echo parameters and then remove this echo. When the detection function cannot detect any more echo, we have got the correct value of $\hat{\alpha}$ (as this gives the lowest output value of the detection function). Results obtained using this algorithm are presented in Fig. 6.

3.5 Protocol Considerations

The main threat addressed in the literature is an attack by a pirate who tries to remove the watermark directly. As a consequence, the definition commonly used for robustness includes only resistance to signal manipulation (cropping, scaling, resampling, etc.). Craver *et al.* show that this is not enough by exhibiting a 'protocol' level attack [22].

The basic idea is that many schemes provide no intrinsic way of detecting which of two watermarks was added first: the process of marking is often additive, or at least commutative. So if the owner of the document d encodes a watermark w and publishes the marked version $d + w$ and has no other proof of ownership, a pirate who has registered his watermark as w' can claim that the document is his and that the original unmarked version of it was $d + w - w'$. Their paper ([23]) extends this idea to defeat a scheme which is non-invertible (an inverse needs only be approximated).

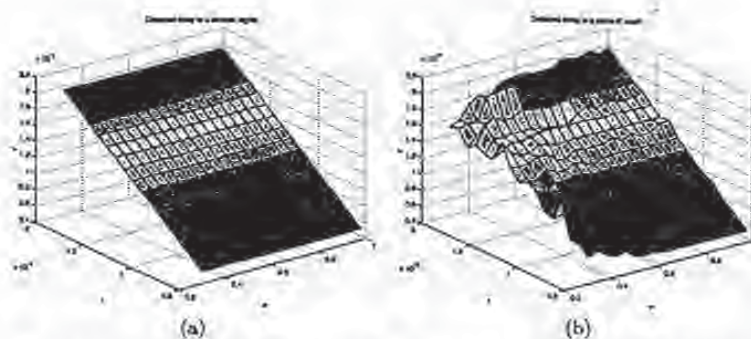


Fig. 6. Performances of the echo detector. We added different echoes characterised by their relative amplitude α and their delay τ to a signal and each time we used our echo detector to find an estimation $\hat{\tau}$ of τ . These graphs show the detected echo delay as a function of α and τ for random signals (a) and for a piece of music (b).

Craver *et al.* argue for the use of information-losing marking schemes whose inverses cannot be approximated closely enough. However, our alternative interpretation of their attack is that watermarking and fingerprinting methods must be used in the context of a larger system that may use mechanisms such as timestamping and notarisation to prevent attacks of this kind.

Registration mechanisms have not received very much attention in the copyright marking literature to date. The existing references such as [18, 32, 31, 52] mainly focus on protecting the copyright holder and do not fully address the rights of the consumers who might be fooled by a crooked reseller.

3.6 Implementation Considerations

The robustness of embedding and retrieving techniques is not the only issue. Most attacks on fielded cryptographic systems have come from the opportunistic exploitation of loopholes that were found by accident; cryptanalysis was rarely used, even against systems that were vulnerable to it [2].

We cannot expect copyright marking systems to be any different and the pattern was followed in the first attack to be made available on the Internet against the most widely used picture marking scheme, PictureMarc, which is bundled with Adobe Photoshop and Corel Draw. This attack [13] exploited weaknesses in the implementation rather than the underlying marking algorithms, even although these are weak (the marks can be removed using StirMark).

Each user has an ID and a two-digit password, which are issued when she registers with Digimarc and pays for a subscription. The correspondence between IDs and passwords is checked using obscure software in the implementation and although the passwords are short enough to be found by trial and error, the

attack first uses a debugger to break into the software and disable the password checking mechanism.

We note in passing that IDs are public, so either password search or disassembly can enable any user to be impersonated.

A deeper examination of the program also allows a villain to change the ID, thus the copyright, of an already marked image as well as the type of use (such as adult versus general public content). Before embedding a mark, the program checks whether there is already a mark in the picture, but this check can be bypassed fairly easily using the debugger with the result that it is possible to overwrite any existing mark and replace it with another one.

Exhaustive search for the personal code can be prevented by making it longer, but there is no obvious solution to the disassembly attack. If tamper resistant software [9] cannot give enough protection, then one can always have an online system in which each user shares a secret embedding key with a trusted party and uses this key to embed some kind of digital signature. Observe that there are two separate keyed operations here; the authentication (which can be done with a signature) and the embedding or hiding operation.

Although we can do public-key steganography – hiding information so that only someone with a certain private key can detect its existence [4] – we still do not know how to do the hiding equivalent of a digital signature; that is, to enable someone with a private key to embed marks in such a way that anyone with the corresponding public key can read them but not remove them. One problem is that a public decoder can be used by the attacker; he can remove a mark by applying small changes to the image until the decoder cannot find it anymore. This was first suggested by Perrig in [52]. In [42] a more theoretical analysis of this attack is presented as well as a possible countermeasure: randomising the detection process. One could also make the decoding process computationally expensive. However neither approach is really satisfactory in the absence of tamper-resistant hardware.

Unless a breakthrough is made, applications that require the public verifiability of a mark (such as DVD) appear doomed to operate within the constraints of the available tamper resistance technology, or to use a central 'mark reading' service. This is evocative of cryptographic key management prior to the invention of public key techniques.

4 Conclusion

We have demonstrated that the majority of copyright marking schemes in the literature are vulnerable to attacks involving the introduction of sub-perceptual levels of distortion. In particular, many of the marking schemes in the marketplace provide only a limited measure of protection against attacks. Most of them are defeated by StirMark, a simple piece of software that we have placed in the public domain [38]. We have also shown a specific attack on the one serious exception to this rule (echo hiding).

This experience confirms our hypothesis that steganography would go through the same process of evolutionary development as cryptography, with an iterative process in which attacks lead to more robust systems.

Our experience in attacking the existing marking schemes has convinced us that any system which attempted to meet all the accepted requirements for marking (such as those set out by IFPI) would fail: if it met the robustness requirements then its bandwidth would be quite insufficient. This is hardly surprising when one considers that the information content of many music recordings is only a few bits per second, so to expect to embed 20 bits per second against an opponent who can introduce arbitrary distortions is very ambitious.

Our more general conclusion from this work is that the 'marking problem' has been over-abstracted; there is not one 'marking problem' but a whole constellation of them. We do not believe that any general solution will be found. The trade-offs and in particular the critical one between bandwidth and robustness, will be critical to designing a specific system.

We already remarked in [8] on the importance of whether the warden was active or passive - that is, whether the mark needed to be robust against distortion. In general, we observe that most real applications do not require all of the properties in the IFPI list. For example, when auditing radio transmissions, we only require enough resistance to distortion to deal with naturally occurring effects such as multipath. Many applications will also require supporting protocol features, such as the timestamping service that we mentioned in the context of reversible marks.

So we do not believe that the intractability of the 'marking problem' is a reason to abandon this field of research. On the contrary, practical schemes for most realistic application requirements are probably feasible and the continuing process of inventing schemes and breaking them will enable us to advance the state of the art rapidly.

Finally, we suggest that the real problem is not so much inserting the marks as recognising them afterwards. Thus progress may come not just from devising new marking schemes, but in developing ways to recognise marks that have been embedded using the obvious combinations of statistical and transform techniques and thereafter subjected to distortion. The considerable literature on signal recognition may provide useful starting points.

Acknowledgements

Some of the ideas presented here were clarified by discussion with Roger Needham, David Wheeler, John Daugman, Peter Rayner, David Aucsmith, Stewart Lee, Scott Craver, Brian Moore, Mike Roe, Peter Wayner, Jon Honeyball, Scott Moskowitz and Matt Blaze.

References

1. Request for proposals - Embedded signalling systems issue 1.0. International Federation of the Phonographic Industry, 54 Regent Street, London W1R 5PJ, June 1997.
2. Ross J. Anderson. Why cryptosystems fail. *Communications of the ACM*, 37(11):32-40, November 1994.
3. Ross J. Anderson, editor. *Information hiding: first international workshop*, volume 1174 of *Lecture Notes in Computer Science*, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany.
4. Ross J. Anderson. Stretching the limits of steganography. In IH96 [3], pages 39-48.
5. Ross J. Anderson and Markus G. Kuhn. Tamper resistance - A cautionary note. In *Second USENIX Workshop on Electronic Commerce*, pages 1-11, Oakland, CA, USA, November 1996.
6. Ross J. Anderson and Charalampos Maniavas. Chameleon - a new kind of stream cipher. In Bibam [14], pages 107-113.
7. Ross J. Anderson and Roger M. Needham. Programming satan's computer. In J. van Leeuwen, editor, *Computer Science Today - Commemorative Issue*, volume 1000 of *Lecture Notes in Computer Science*, pages 426-441. Springer-Verlag, Berlin, Germany, 1995.
8. Ross J. Anderson and Fabien A. P. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 15(4):474-481, May 1998. Special Issue on Copyright & Privacy Protection.
9. David Aucsmith. Tamper resistant software: An implementation. In Anderson [3], pages 317-333.
10. David Aucsmith, editor. *Information Hiding: Second International Workshop*, volume 1525 of *Lecture Notes in Computer Science*, Portland, Oregon, USA, 1998. Springer-Verlag, Berlin, Germany.
11. Walter Bender, Daniel Gruhl, and Norishige Morimoto. Techniques for data hiding. In Niblack and Jain [48], pages 164-173.
12. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3 & 4):313-336, 1996.
13. Anonymous (<zguan.bbs@bbs.ntu.edu.tw>). Learn cracking IV - another weakness of PictureMarc. <news:tv.bbs.comp.hacker> mirrored on <http://www.cl.cam.ac.uk/~Tapp2/watermarking/image_watermarking/diginarc_crack.html>, August 1997. Includes instructions to override any Diginarc watermark using PictureMarc.
14. Eli Bibam, editor. *Fast Software Encryption - 4th International Workshop, FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, Haifa, Israel, January 1997. Springer-Verlag, Germany.
15. Bruce P. Bogert, M.J.R. Healy, and John W. T. Englandey. The quefrency analysis of time series for echoes: Cepstrum, pseudo-autocovariance, cross-cepstrum and saphe cracking. In M. Rosenblatt, editor, *Symposium on Time Series Analysis*, pages 209-243, New York, NY, USA, 1963. John Wiley & Sons, Inc.
16. Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy. Digital watermarks for audio signals. In *European Signal Processing Conference, EUSIPCO '96*, Trieste, Italy, September 1996.
17. Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy. Digital watermarks for audio signals. In *International Conference on Multimedia Computing and Systems*, pages 473-480, Hiroshima, Japan, 17-23 June 1996. IEEE.

18. Marc Cooperman and Scott A. Moskowitz. Steganographic method and device. US Patent 5,613,004, March 1995.
19. Ingemar J. Cox, Joe Kilian, Tam Leighton, and Talal Shamooh. A secure, robust watermark for multimedia. In Anderson [3], pages 183-206.
20. Ingemar J. Cox and Matt L. Miller. A review of watermarking and the importance of perceptual modeling. In Rogowitz and Pappas [57].
21. Ingemar J. Cox and Kazuyoshi Tanaka. NEC data hiding proposal. Technical report, NEC Copy Protection Technical Working Group, July 1997. Response to call for proposal issued by the Data Hiding SubGroup.
22. Scott Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. Can invisible watermark resolve rightful ownerships? In Sethin and Jain [62], pages 310-321.
23. Scott Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *IEEE Journal of Selected Areas in Communications*, 16(4):573-586, May 1998. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.
24. Digimarc home page. <<http://www.digimarc.com/>>, April 1997.
25. Eliconmark. Alpha Tec Ltd., <<http://www.generation.net/~pitcas/sign.html>>, October 1997.
26. Elke Frans, Anja Jerichow, Steffen Möller, Andreas Pfitzmann, and Ingo Stierand. Computer based steganography: how it works and why therefore any restriction on cryptography are nonsense, at best. In Anderson [3], pages 7-21.
27. Michael A. Gerzon and Peter G. Graven. A high-rate buried-data channel for audio CD. *Journal of the Audio Engineering Society*, 43(1/2):3-22, January-February 1995.
28. François Goffin, Jean-François Delaigle, Christophe De Vleeschouwer, Benoît Macq, and Jean-Jacques Quisquater. A low cost perceptible digital picture watermarking method. In Sethin and Jain [62], pages 264-277.
29. Daniel Gruhl, Walter Bender, and Anthony Lu. Echo hiding. In Anderson [3], pages 295-315.
30. Khaled N. Hamdy, Ahmed H. Tewfik, Ting Chen, and Satoshi Takagi. Time-scale modification of audio signals with combined harmonic and wavelet representations. In *International Conference on Acoustics, Speech and Signal Processing - ICASSP '97*, volume 1, pages 439-442, Munich, Germany, April 1997. IEEE, IEEE Press, Session on Hearing Aids and Computer Music.
31. Alexander Herrigel, Joseph J. K. Ó Ruanaidh, Holger Petersen, Shelby Pereira, and Thierry Pun. Secure copyright protection techniques for digital images. In Aucsmith [10], pages 169-190.
32. Alexander Herrigel, Adrian Perrig, and Joseph J. K. Ó Ruanaidh. A copyright protection environment for digital images. In *Verlässliche IT-Systeme '97*, Albert-Ludwigs Universität, Freiburg, Germany, October 1997.
33. J.N. Holmes. *Speech Synthesis and Recognition*, chapter 3.6 Analysis of simple and complex signals, pages 47-48. Aspects of Information Technology. Chapman & Hall, London, England, 1986.
34. International Electrotechnical Commission, Geneva, Switzerland. *Digital audio interface, IEC 60958*, February 1989.
35. Alastair Kelman. Electronic copyright management - the way ahead. Security Seminars, University of Cambridge, February 1997.
36. A. Kerckhoffs. La Cryptographie Militaire. *Journal des Sciences Militaires*, 9:5-38, January 1883.

37. E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *Workshop on Nonlinear Signal and Image Processing*, pages 452–455, Neos Marmaras, Greece, June 1995. IEEE.
38. Markus G. Kuhn and Fabien A. P. Petitcolas. StirMark. <<http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmerk/>>, November 1997.
39. Charles Kuruk and John McHugh. A cautionary note on image downgrading. In *Computer Security Applications Conference*, pages 153–159, San Antonio, TX, USA, December 1992.
40. Gerrit C. Langelaar, Jan C.A. van der Lubbe, and J. Biemond. Copy protection for multimedia data based on labeling techniques. In *17th Symposium on Information Theory in the Benelux*, Enschede, The Netherlands, May 1996.
41. Gerrit C. Langelaar, Jan C.A. van der Lubbe, and Reginald L. Lagendijk. Robust labeling methods for copy protection of images. In *Setlin and Jain [62]*, pages 298–309.
42. Jean-Paul M.G. Linnartz and Marten van Dijk. Analysis of the sensitivity attack against electronic watermarks in images. In *Aucsmith [10]*, pages 258–272.
43. Mark Lomas, Bruno Crispo, Bruce Christianson, and Mike Roe, editors. *Security Protocols: Proceeding of the 5th International Workshop*, volume 1361 of *Lecture Notes in Computer Science*, Ecole Normale Supérieure, Paris, France, April 1997. University of Cambridge, Isaac Newton Institute, Springer-Verlag, Berlin, Germany.
44. Maurice Maes. Twin peaks: The histogram attack on fixed depth image watermarks. In *Aucsmith [10]*, pages 290–305.
45. Kinen Matsui and Kiyoshi Tanaka. Video-steganography: How to secretly embed a signature in a picture. *Journal of the Interactive Multimedia Association Intellectual Property Project*, 1(1):187–205, January 1994.
46. Norishige Morimoto and Daniel Sullivan. IBM DataHiding proposal. Technical report, IBM Corporation, September 1997. Response to call for proposal issued by the Data Hiding SubGroup.
47. Peter Naccarrow. Digital technology – Bane or boon for copyright? *Computer Laboratory Seminars*, University of Cambridge, November 1997.
48. Wayne Niblack and Ramesh C. Jain, editors. *Storage and Retrieval for Image and Video Database III*, volume 2420, San Jose, California, USA, February 1995. IS&T, The Society for Imaging Science and Technology and SPIE, The International Society for Optical Engineering, SPIE.
49. Joseph J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Watermarking digital images for copyright protection. *IEE Proceedings on Vision, Signal and Image Processing*, 143(4):250–256, August 1996.
50. Joseph J. K. Ó Ruanaidh and Shelby Pereira. A secure robust digital image watermark. In *International Symposium on Advanced Imaging and Network Technologies - Conference on Electronic Imaging: Processing, Printing and Publishing in Colour*, Europto, Zürich, Switzerland, May 1998. International Society for Optical Engineering, European Optical Society, Commission of the European Union, Directorate General XII.
51. Alan V. Oppenheim and Ronald W. Schaffer. *Discrete-Time Signal Processing*, chapter 12, pages 768–834. Prentice-Hall International, Inc., Englewood Cliffs, NJ, USA, international edition, 1989.
52. Adrian Perrig. A copyright protection environment for digital images. Diploma dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, February 1997.

53. Fablen A. P. Petitcolas. Weakness of existing watermarking schemes. <http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/>, October 1997.
54. Birgit Pfizmann. Information hiding terminology. In Anderson [3], pages 347-350. Results of an informal plenary meeting and additional proposals.
55. I. Pitas. A method for signature casting on digital images. In *International Conference on Image Processing*, volume 3, pages 215-218, September 1996.
56. Geoffrey B. Rhoads. Steganography methods employing embedded calibration data. US Patent 5,636,292, June 1997.
57. Bernice E. Rogowitz and Thrasyvoulos N. Pappas, editors. *Human Vision and Electronic Imaging II*, volume 3018, San Jose, CA, USA, February 1997. IS&T, The Society for Imaging Science and Technology and SPIE, The International Society for Optical Engineering, SPIE.
58. Pamela Samuelson. Copyright and digital libraries. *Communications of the ACM*, 38(4):15-21, 110, April 1995.
59. Ronald W. Schaefer. Echo removal by discrete generalized linear filtering. Technical Report 466, Massachusetts Institute of Technology, February 1969.
60. Bruce Schneier. Protocol interactions and the chosen protocol attack. In Lomas et al. [43], pages 91-104.
61. Robert A. Scholtz. The origins of spread-spectrum communications. *IEEE Transactions on Communications*, 30(5):822-853, May 1982.
62. Ishwar K. Sethin and Ramesh C. Jain, editors. *Storage and Retrieval for Image and Video Database V*, volume 3022, San Jose, CA, USA, February 1997. IS&T, The Society for Imaging Science and Technology and SPIE, The International Society for Optical Engineering, SPIE.
63. Sigma Technologies - SureSign digital fingerprinting. <<http://www.sigumtech.com/>>, October 1997.
64. Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik. Transparent robust image watermarking. In *International Conference on Image Processing*, volume III, pages 211-214. IEEE, 1996.
65. Mitchell D. Swanson, Bin Zu, and Ahmed H. Tewfik. Robust data hiding for images. In *7th Digital Signal Processing Workshop (DSP 96)*, pages 37-40, Loen, Norway, September 1996. IEEE.
66. A.Z. Tirkel, G.A. Rankin, R.M. van Schyndel, W.J. Ho, N.R.A. Mee, and C.F. Osborne. Electronic watermark. In *Digital Image Computing, Technology and Applications - DICTA '93*, pages 666-673, Macquarie University, Sydney, 1993.
67. R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne. A digital watermark. In *International Conference on Image Processing*, volume 2, pages 86-90, Austin, Texas, USA, 1994. IEEE.
68. Georges Van Slype. Natural language version of the generic CITED model - ECMS (Electronic Copyright Management System) design for computer based applications. Report 2, European Commission, ESPRIT II Project, Bureau Van Dijk, Brussel, Belgium, May 1995.
69. Georges Van Slype. Natural language version of the generic CITED model - Presentation of the generic model. Report 1, European Commission, ESPRIT II Project, Bureau Van Dijk, Brussel, Belgium, May 1995.
70. A. Werner, J. Oomen, Marc E. Groenewegen, Robbert G. van der Waal, and Raymond N.J. Veldhuis. A variable-bit-rate buried-data channel for compact disc. *Journal of the Audio Engineering Society*, 43(1/2):23-28, January-February 1995.
71. The Working Group on Intellectual Property Rights in part of the US Information Infrastructure Task Force, formed in February 1993.

72. Raymond B. Wolfgang and Edward J. Delp. A watermark for digital images. In *International Conference on Images Processing*, pages 219-222, Lausanne, Switzerland, September 1996. IEEE.
73. Raymond B. Wolfgang and Edward J. Delp. A watermarking technique for digital imagery: further studies. In *International Conference on Imaging, Systems, and Technology*, pages 279-287, Las Vegas, NV, USA, 30 June-3 July 1997. IEEE.
74. J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. In *International Congress on Intellectual Property Rights for Specialised Information, Knowledge and New Technologies*, Vienna, Austria, August 1995.
75. Jian Zhao. A WWW service to embed and prove digital copyright watermarks. In *European Conference on Multimedia Applications, Services and Techniques*, pages 695-710, Louvain-la-Neuve, Belgium, May 1996.
76. Jian Zhao. The syscop home page. <<http://syscop.igd.fhg.de/>> or <<http://www.crcg.edu/syscop/>>, February 1997.

Lecture Notes in Computer Science

1174

W. A. R. ...

W. A. R. ...

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without permission in writing from the publisher. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, and in connection with the previous general permission for use must always be obtained from Springer-Verlag. Violations are subject to prosecution under the German Copyright Law.

Printed in Germany, 1996

Printed on acid-free paper

Stretching the Limits of Steganography

Ross Anderson

Cambridge University Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, UK
Email rja14@c1.cam.ac.uk

Abstract. We present a number of insights into information hiding. It was widely believed that public key steganography was impossible; we show how to do it. We then look at a number of possible approaches to the theoretical security of hidden communications. This turns out to hinge on the inefficiency of practical compression algorithms, and one of the most important parameters is whether the opponent is active or passive (i.e., whether the censor can add noise, or will merely allow or disallow a whole message). However, there are coartexts whose compression characteristics are such that even an active opponent cannot always eliminate hidden channels completely.

1 Introduction

Steganography is about concealing the existence of messages, and it goes back to ancient times. Kahn tells of a classical Chinese practice of embedding a code ideogram at a prearranged place in a dispatch; of the warning the Greeks received of Xerxes' intentions from a message underneath the wax of a writing tablet; and a trick of dotting successive letters in a coartext with secret ink, due to Aeneas the Tactician [8].

The opponent may be passive, and merely observe the coartext, but he may also be active. In the US post office during the second world war, postal censors deleted lovers' X's, shifted watch hands, and replaced items such as loose stamps and blank paper. They also rephrased telegrams; in one case, a censor changed 'father is dead' to 'father is deceased', which elicited the reply 'is father dead or deceased?'

The study of this subject in the open scientific literature may be traced to Simmons, who in 1983 formulated it as the prisoners' problem [16]: Alice and Bob are in jail, and wish to hatch an escape plan. All their communications pass through the warden, Willy. If Willy sees any encrypted messages, he will frustrate their plan by putting them into solitary confinement. So they must find some way of hiding their ciphertext in an innocuous looking coartext. As in the related field of cryptography, we assume that the mechanism in use is known to the warden, and so the security must rely solely on a secret key.

There are many real life applications of steganography. Apparently, during the 1980's, British Prime Minister Margaret Thatcher became so irritated at

press leaks of cabinet documents that she had the word processors programmed to encode their identity in the word spacing of documents, so that disloyal ministers could be traced. Similar techniques are now undergoing trials in an electronic publishing project, with a view to hiding copyright messages and serial numbers in documents [10].

Simmons' real application was more exotic — the verification of nuclear arms control treaties. The US and the USSR wanted to place sensors in each others' nuclear facilities that would transmit certain information (such as the number of missiles) but not reveal other kinds of information (such as their location). This forced a careful study of the ways in which one country's equipment might smuggle out the forbidden information past the other country's monitoring facilities [17, 19].

Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to a person who intercepts it. Such protection is often not enough: the detection of enciphered message traffic between a soldier and a hostile government, or between a known drug-smuggler and someone not yet under suspicion, has obvious implications.

However, we still have no comprehensive theory of steganography, in the way that Shannon gave us a theory of encryption [15] and Simmons of authentication [18]. In this article, we will try to move a few small steps towards such a theory.

2 The State of the Art

A number of computer programs are available that will embed a ciphertext file in an image. The better systems assume that both sender and receiver share a key and use a conventional cryptographic keystream generator [13] to expand this into a long pseudo-random keystream. The keystream is then used to select pixels in which the bits of the ciphertext are embedded.

Of course, not every pixel may be suitable for encoding ciphertext: changes to pixels in large fields of monochrome colour, or that lie on sharply defined boundaries, might be visible. So some systems have an algorithm that determines whether a candidate pixel can be used by checking that the variance in luminosity of the eight surrounding pixels is neither very high (as on a boundary) nor very low (as in a monochrome field). A bit can be embedded in a pixel that passes this test by some rule such as setting its low order bit to the parity of the surrounding pixels (though in practice one might use something slightly more complicated to avoid leaving telltale statistics).

Of course, the more bits per pixel, the less correlated the low order bits will be with neighbouring bits and with higher order bits in the same pixel. Some quantitative measurements of the correlations between pixels on different bit planes in digital video may be found in [20]. In effect, the bits that Alice can use to embed covert data are redundant in that Willy will be unaware that they have been altered. It follows that they might be removed by an efficient compression scheme, if one exists for the image or other covertext in use.

So when the image is to be subjected to compression (whether before or after the insertion of covert material), things become more complicated, and we have to tailor the embedding method. For example, with .gif files one can swap colours for similar colours that are adjacent in the current palette [7], while if we want to embed a message in a file that may be subjected to JPEG compression and filtering, we can embed it in multiple locations [9] or in the frequency domain by altering components of the image's discrete cosine transform [3] [23]. Further papers on the topic may be found in this volume.

So the general model is that Alice embeds information by tweaking some bits of some transform of the coartext. The transform enables her to get at one or more bits which are redundant in the sense that tweaking them cannot be detected easily or at all. In a first approximation, we will expect that such transforms will be similar to those used for compression, and that there are many low-bandwidth stego channels arising from redundancy whose elimination, by compression or otherwise, is uneconomic for normal users of the cover system. We will not expect to find many high bandwidth channels, as these would normally correspond to redundancy that could economically be removed.

3 Public Key Steganography

So far, we have merely stated the general intuition of people who have thought about these topics. They generally assume that steganography, in the presence of a capable motivated opponent who is aware of the general methods that might be used, requires the pre-existence of a shared secret so that the two communicating parties can decide on which bits to tweak. So there has been a general assumption that public-key steganography is impossible.

However, this is not the case. We will now show how a hidden message can be sent to a recipient with whom the sender has no shared secret, but for whom an authentic public key is available.

Given a coartext in which any ciphertext at all can be embedded, then there will usually be a certain rate at which its bits can be tweaked without the warden noticing (we will discuss this more fully below). So suppose that Alice can modify at least one out of every hundred bits of the coartext. This means that Willy cannot distinguish the parity of each successive block of a hundred bits from random noise, and it follows that she can encode an arbitrary pseudorandom string in these parities.

This pseudorandom material will lie in plain sight; anyone will be able to read it. So Willy cannot simply check a coartext by seeing whether a pseudorandom string can be found in it. Indeed, a suitable parity check function will extract pseudorandom-looking data from any message in which covert information can be inserted at all.

Now suppose that Alice and Bob did not have the opportunity to agree a secret key before they were imprisoned, but that Bob has a public key that is known to Alice. She can take her covert message, encrypt it under his public key,

and embed it as the parity of successive blocks. Each possible recipient will then simply try to decrypt every message he sees, and Bob alone will be successful. In practice, the value encrypted under a public key could be a control block consisting of a session key plus some padding, and the session key would drive a conventional steganographic scheme as described elsewhere in this volume.

Normal public key cryptography means that users can communicate confidentially in the absence of previously shared secrets; our construction of public key steganography shows that they can also communicate covertly (if this is at all possible for people with previously shared secrets). Public key stego scales less well than public key crypto, as every recipient has to try to decrypt every message. However, this appears to be an intrinsic property of anonymous communications.

4 Theoretical Limits

Can we get a scheme that gives unconditional covertness, in the sense that the one-time pad provides unconditional secrecy?

Suppose that Alice uses an uncompressed digital video signal as the covertext, and encodes ciphertext at a very low rate. For example, the k th bit of ciphertext might become the least significant bit of one of the pixels of the k th frame of video, with the choice of pixel being specified by the k th word of a shared one time pad. Then we intuitively expect that attacks will be impossible: the ciphertext will be completely swamped in the covertext's intrinsic noise. Is there any way this intuitively obvious fact could be rigorously proved?

This leads us to ask what a proof of perfect covertness would look like. A working definition of a secure stegosystem might be one for which Willy cannot differentiate between raw covertext and the stegotext containing embedded information, unless he has knowledge of the key. As in the case of cryptography, we might take Willy to be a probabilistic polynomial Turing machine in the case where we require computational security, and assume that he can examine all possible keys in the case where we require unconditional security.

In the latter case, he will see the actual message, so the system must generate enough plausible messages from any given stegotext, and the number of such messages must not vary in any usable way between the stegotext and a wholly innocent covertext.

This much is straightforward, but what makes the case of steganography more difficult than secrecy or authenticity is that we are dependent on the model of the source. There are a number of ways in which we can tackle this dependence, and we will present three of them. It is an open question whether any of them will yield useful results in any given application.

4.1 Selection channel

Our first idea is inspired by the correction channel that Shannon uses to prove his second coding theorem. This is the channel which someone who can see both the transmitted and received signals uses to tell the receiver which bits to tweak, and produces various noise and error correction bounds [14].

In a similar way, when Alice and Bob use a shared one-time pad to decide which covertext bit will contain the next ciphertext bit, we can think of the pad as a selection channel. If Willie is computationally unbounded, he can try all possible pads (including the right one), so the number of them which yield a plausible ciphertext must be large enough that he cannot reasonably accuse Alice of sending stegotext rather than an innocent message.

It may be useful at this point to recall the book cipher: The sender and receiver share a book and encipher a message as a series of pointers to words. So the cipher group '78216' might mean page 78, paragraph 2 and the 16th word. Book codes can be secure provided that the attacker does not know which book is in use, and care is taken not to reuse a word (or a word close enough to it) [8]. The book cipher is just a selection channel. The model of computation may be different, in that with a book cipher we start off with the book and then generate the ciphertext, whereas in a stegosystem, we start off with the text to be embedded and then create the stegotext; but they are clearly related.

A repetitive book will have a lower capacity, as we will be able to use a smaller percentage of its words before inference attacks from the context become possible. Similarly, if the covertext to be used in a stegosystem has unusual statistics (such as an unequal number of zeros and ones) then its stego capacity will be lower, as only a small proportion of candidate ciphertexts would look random enough.

We mentioned systems that generate a number of candidate locations for a ciphertext bit and then filter out the locations where actually embedding a bit would have a significant effect on the statistics thought to be relevant (in the case of hiding in an image, this could mean avoiding places where the local variance in luminosity is either very low or very high).

Our information theoretic approach suggests a better way. We will use our *lazy* stream generator to select not one pixel but a set of them, and embed the ciphertext bit as their parity. This way, the information can be hidden by changing whichever of the pixels can be changed least obtrusively.

From the information theoretic point of view, if the covertext is '1' with probability 0.5, and we encode in bit pairs, then the probability that a bit pair will have parity 1 is 0.52; if we move to triples, the parity is 1 with probability 0.504, and so on. As the improvement is geometric, we can with little difficulty get the discrepancy as low as we like and thus — provided that our selection channel is broad enough — we can hide information quite efficiently.

Indeed, there is a tradeoff: the more bits in the selection channel, the more bits we can hide in the covertext. In practice our selection channel will be a

cryptographic pseudorandom number generator, and we can draw from it as many bits as we like.

But clearly there is an ultimate limit to the amount of information that can be hidden.

For example, suppose that there is an allowed set of cover texts M (we might be using the cover of a news agency; we have to report a reasonably truthful version of events, and transmit photographs — perhaps slightly doctored — of events that actually took place). Suppose also that there is an allowed set of encodings E . Then the covert capacity will be at most $H(E) - H(M)$. Can we tighten this upper bound or — better still — get any kind of lower bound?

4.2 Equivalence classes

We can consider equivalence classes of messages. Suppose Alice uses a keyed cryptographic hash function to derive one bit from each sentence of a letter. As she prepares her stegotext letter to Bob, she has a routine which checks this bit and beeps if it is wrong. This will go off about every other sentence, which she can then rewrite.

Of course, if she uses standard changes such as [is able ↔ can], then clearly she must not alter their statistics to the point that Willy can detect the change. It is even an open question whether a computer can alter a natural language text in a way that is undetectable to a human [21] — that is, embed a ciphertext using the technique described above — and the problem is commended to the research community as a weak form of the Turing test.

The converse is that writing a program to scan for human inserted steganography might be rather hard. This is an area in which competitive research might prove interesting!

Equivalence classes can also arise naturally. For example, when making a map from a larger scale map, many arbitrary decisions have to be taken about which features to incorporate, especially with features such as coastlines that are to some extent fractal [12]. Also, when software is written, it contains 'birthmarks' such as the order in which registers are pushed and popped, and these were used by IBM in litigation against software pirates who had copied their PC-AT ROM [6].

Equivalence classes of messages are tied up with compression. If coverttext C_1 means the same as coverttext C_2 , then a compression algorithm need only select one representative from this equivalence class. However, if $C_1 \neq C_2$, then this choice throws away information, and so the compression is lossy.

Information theorists assume that any signal can in theory be completely compressed. But if this could ever be done in practice, then the steganography problem would become trivial: Alice can just 'uncompress' her ciphertext getting a comprehensible message, and Willy would have to pass the result. So Willy can only do his job at all because perfect compression is unfeasible. So regardless of whether we talk in terms of compression or of equivalence classes, Willy's

performance of his job depends on his having a model of the source, and the danger to Alice and Bob is that his model might be better than theirs.

4.3 Conditional entropy

If Alice does not trust her ability to spot which bits of the covertext (or some transform of it) will appear noise-like to Willy, she might try to use conditional entropy. If the ciphertext is random, its mutual information with the covertext will be zero, and entropy will be additive — the entropy of the loaded covertext will be exactly equal to the entropy of the pure covertext plus that of the ciphertext.

Thus the maximum amount of ciphertext that she can hide from Willy depends on the uncertainty of the covertext entropy. Confidence levels can be computed in the obvious way: if the ciphertext rate is R_1 , then the warden must not be able to detect with probability P a change of R_1 in the covertext rate R_2 .

Thanks to the Central Limit Theorem, the more covertext we give the warden, the better he will be able to estimate its statistics, and so the smaller the rate at which Alice will be able to tweak bits safely. The rate might even tend to zero, as was noted in the context of covert channels in operating systems [11]. However, as a matter of empirical fact, there do exist channels in which ciphertext can be inserted at a positive rate [4], so measuring entropy may be useful in a number of applications.

However, it still does not give us a way to prove the unconditional covertness of a system. The reason for this is that once Alice assumes that Willy is smarter than she is, she has no way of estimating the variance in his estimates of the entropy of her covertext. A purist might conclude that the only circumstance in which she can be certain that Willy cannot detect her messages is when she uses a subliminal channel in the sense of Simmons; that is, a channel in which she chooses some random bits (as in an ElGamal digital signature) and these bits can be recovered by the message recipient [1].

5 Active and Passive Wardens

The applications discussed above include both passive wardens, who monitor traffic and signal to some process outside the system if unauthorised message traffic is detected, and active wardens who try to remove all possible covert messages from coverttexts that pass through their hands. A good example of the latter was the world war two postal censor described in the introduction, and a highly topical example is given by software piracy.

Software birthmarks, as mentioned above, have been used to prove the authorship of code so that pirates could be prosecuted. They were serviceable with hand assembled system software, but might be harder to find now that

most code is produced by a compiler. A possible remedy is to embed copyright information by mangling the object code in some way. The automatic, random replacement of code fragments with equivalent ones is used by Intel to customise security code [2]. This may be adequate in that application, where the goal is to prevent a single patch defeating all instances of a protective mechanism; but copyright marking is harder. One could imagine a contest between software authors and pirates to see who can mangle code most thoroughly without affecting its performance too much. If the author has the better mangler, then some of the information he adds will be left untouched by the pirate.

In fact, the World Intellectual Property Organisation has proposed a system of numbering for all digital works, including books, sound and video recordings, and computer programs; it claims that the boundaries between these are breaking down. Software publishers are sceptical; they claim to have had no difficulty yet in establishing ownership [5]. But whatever the legal value of copyright marking, the software pirate is a good example of an active warden.

In such a case, the simple public key scheme described in section two above will not work. Even in the shared-key model, there are cases where an active warden can completely block the stego channel. For example, if (a) his model of the communication is at least as good as the prisoners' (b) the covertext information separates cleanly from the covert information, then he can replace the latter with noise. This is the case of a software pirate who has a better code mangler than the software author.

6 Limits on Active Wardens

However, there are many other cases where the stego channel is highly bound up with the covertext. For example, Jaggal [7] measured the noise that can be added to a .gif file before the image quality is degraded, while Möller and others have done the same for digitised speech [4].

The point here is that if Alice can add an extra X% of noise without affecting the picture, then so can Willy; but she can stop him finding out which X% carries the covert message by using a keystream to select which bits of covertext to tweak. In this case, all Willy will be able to do is to cut the bandwidth of the channel — a scenario that Trostle and others have explored in the context of covert channels in operating systems [22].

This bandwidth limitation will also be effective against systems that embed each ciphertext bit as a parity check of a number of covertext bits. When the warden is active, the more covertext bits we use in each parity check, the more easily he will be able to inject noise into our covertext.

> It is an open question whether public key steganography can be made to work against an active warden who can add only a limited amount of noise. It may also be of interest to consider whether one can implement other cryptographic primitives, such as the wiretap channel and bit commitment [13]. If it turns out that the kind of public key steganography that we have described here cannot be

made to work, then key exchange well might be possible by combining techniques like these.

7 Conclusions

We have stretched the limits of steganography somewhat. Firstly, we have shown how to do public key steganography. Secondly, we have discussed a number of possible approaches to a theory of the subject, which suggest various practical techniques for improving the covertness of existing steganographic schemes. Thirdly, we have highlighted one of the most important topics, namely whether the warden is active or passive, and shown how this interacts with both the public key and theoretical approaches to the subject.

Acknowledgements: Some of the ideas presented here were clarified by discussion with David Wheeler, John Daugman, Roger Needham, Gus Simmons, Markus Kuhn, John Kelsey, Ian Jackson, Mike Roe, Mark Lomas, Stewart Lee, Peter Wayner and Matt Blaze. I am also grateful to the Isaac Newton Institute for hospitality while this paper was being written.

References

1. "The Newton Channel", RJ Anderson, S Vaudeauy, B Preneel, K Nyberg, *this volume*
2. "Tamper Resistant Software: An Implementation", D Aucsmith, *this volume*
3. "Watermarking Digital Images for Copyright Protection", FM Boland, JJK Ó Ruanaidh, C Dautzenberg, *Proceedings, IEEE International Conference on Image Processing and its Applications, Edinburgh 1995*
4. "Computer Based Steganography", E Franz, A Jerichow, S Maeller, A Pfitzmann, I Stierand, *this volume*
5. "A voluntary international numbering system — the latest WIPO proposals", R Hart, *Computer Law and Security Report* v 11 no 3 (May-June 95) pp 127-129
6. Talk on software birthmarks, counsel for IBM Corporation, BCS Technology of Software Protection Special Interest Group, London 1985
7. 'Steganography in Digital Images', G Jagpal, Thesis, Cambridge University Computer Laboratory, May 1995
8. 'The Codebreakers', D Kahn, Macmillan 1967
9. "Towards Robust and Hidden Image Copyright Labeling", E Koch, J Zhao, *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing (Neos Marmaras, Halkidiki, Greece, June 20-22, 1995)*
10. "Electronic Document Distribution", NF Maxemchuk, *AT & T Technical Journal* v 73 no 5 (Sep/Oct 94) pp 73-80
11. "Covert Channels — Here to Stay?", IS Maskowitz, MH Kang, *Compass* 94 pp 235-243
12. RM Needham, *private conversation*, December 1995
13. 'Applied Cryptography — Protocols, Algorithms and Source Code in C' B Schneier (second edition), Wiley 1995

14. "A Mathematical Theory of Communication", CE Shannon, in *Bell Systems Technical Journal* v 27 (1948) pp 379-423, 623-656
15. "Communication theory of secrecy systems", CE Shannon, in *Bell Systems Technical Journal* v 28 (1949) pp 656-715
16. "The Prisoners' Problem and the Subliminal Channel", GJ Simmons, in *Proceedings of CRYPTO '83*, Plenum Press (1984) pp 51-67
17. "How to Insure that Data Acquired to Verify Treaty Compliance are Trustworthy", GJ Simmons, *Proceedings of the IEEE* v 76 (1984) p 5
18. "A survey of information authentication", GJ Simmons, in *Contemporary Cryptology — the Science of information Integrity*, IEEE Press 1992, pp 379-419
19. "The History of Subliminal Channels", GJ Simmons, *this volume*
20. 'High Quality De-interlacing of Television Images', N van Someren, PhD Thesis, University of Cambridge, September 1994
21. K Spärck Jones, *private communication*, August 1995
22. "Modelling a Fuzzy Time System", JT Trostle, *Proc. IEEE Symposium in Security and Privacy 93* pp 82 - 89
23. "Embedding Robust Labels Into Images For Copyright Protection", J Zhao, E Koch, *Proc. Int. Congr. on IPR for Specialized-Information, Knowledge and New Technologies* (Vienna, Austria, August 21-25, 1995)

Rotation, Scale and Translation Invariant Digital Image Watermarking

Joseph J.K. Ó Ruanaidh

Thierry Pun

Groupe de Vision par Ordinateur,
Centre Universitaire d'Informatique,
Université de Genève,
CH-1211 Genève 4, Switzerland

Abstract

A digital watermark is an invisible mark embedded in a digital image which may be used for Copyright Protection. This paper proposes that Fourier-Mellin transform-based invariants can be used for digital image watermarking. The embedded marks may be designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required for extracting the embedded mark.

1 Introduction

Computers, printers and high rate digital transmission facilities are becoming less expensive and more widespread. Digital networks provide an efficient cost-effective means of distributing digital media. Unfortunately however, digital networks and multimedia also afford virtually unprecedented opportunities to pirate copyrighted material. The idea of using a robust digital watermark to detect and trace copyright violations has therefore stimulated significant interest among artists and publishers. As a result, digital image watermarking has recently become a very active area of research. Techniques for hiding watermarks have grown steadily more sophisticated and increasingly robust to lossy image compression and standard image processing operations, as well as to cryptographic attack.

Many of the current techniques for embedding marks in digital images have been inspired by methods of image coding and compression. Information has been embedded using the Discrete Cosine Transform (DCT) [6, 2] Discrete Fourier Transform magnitude and phase [5], Wavelets [6], Linear Predictive Coding and Fractals. The key to making watermarks robust has been the recognition that in order for a watermark to be robust it must be embedded in the perceptually

significant components of the image [6, 2]. The term "perceptually significant" is somewhat subjective but it suggests that a good watermark is one which takes account of the behaviour of human visual system. Objective criteria for measuring the degree to which an image component is significant in watermarking have gradually evolved from being based purely on energy content [6, 2] to statistical [7] and psychovisual [3] criteria.

The ability of humans to perceive the salient features of an image regardless of changes in the environment is something which humans take for granted [10]. We can recognize objects and patterns independently of changes in image contrast, shifts in the object or changes in orientation and scale. It seems clear that an embedded watermark should have the same invariance properties as the image it is intended to protect.

Digital watermarking is also fundamentally a problem in digital communications [6, 9, 2]. In parallel with the increasing sophistication in modelling and exploiting the properties of the human visual system, there has been a corresponding development in communication techniques. Tirkel and Osborne [11] were the first to note the applicability of spread spectrum techniques to digital image watermarking. Since then there has been an increasing use of spread spectrum communications in digital watermarking. It has several advantageous features such as cryptographic security [11, 2], and is capable of achieving error free transmission of the watermark near or at the limits set by Shannon's noisy channel coding theorem [6, 9]. Note that the shorter is the core information or "payload" contained in a watermark then the greater is the chances of the watermark being communicated reliably. Spread spectrum is also an example of a symmetric key [8] cryptosystem where system security is based on proprietary knowledge of the keys (or the

seeds for pseudorandom generators) required to embed, extract or remove an image watermark.

Synchronisation of the watermark signal is of the utmost importance during watermark extraction. If watermark extraction is carried out in the presence of the original image then synchronisation is relatively trivial. The problem of synchronising the watermark signal is much more difficult to solve in the case where there is no original image. If the watermarked image is translated, rotated and scaled then synchronisation necessitates a search over a four dimensional parameter space (X -offset, Y -offset, angle of rotation and scaling factor). The search space grows even larger if one takes into account the possibility of shear and a change of aspect ratio. In this paper, the aim is to investigate the possibility of using invariant representations of a digital watermark to help avoid the need to search for synchronisation during the watermark extraction process. A digital watermark that is invariant to these transformations requires no such search. The tradeoff here is between using a fully invariant representation which may be numerically unstable and expensive to compute with the expense of carrying out a search.

2 Integral Transform Invariants

There are many different kinds of image invariant such as moment, algebraic and projective invariants. In this section we will briefly outline the development of several integral transform based invariants [1].

The invariants described below depend on the properties of the Fourier transform. There are a number of advantages in using a transform based representation. First, using integral transform-based invariants is a relatively simple generalisation of transform domain watermarking. Second, the number of robust invariant components is relatively large which makes it suitable for spread spectrum techniques. Third, as we shall see, mapping to and from the invariant domain to the spatial domain is well-defined and it is, in general, not computationally expensive.

2.1 The Fourier Transform

Let the image be a real valued continuous function $f(x_1, x_2)$ defined on an integer-valued Cartesian grid $0 \leq x_1 < N_1, 0 \leq x_2 < N_2$. Let the two dimensional Discrete Fourier Transform (DFT) $F(k_1, k_2)$ where $0 \leq k_1 < N_1, 0 \leq k_2 < N_2$ be defined in the usual way [4].

2.1.1 The Translation Property

Shifts in the spatial domain cause a linear shift in the phase component:

$$F(k_1, k_2) \exp\{-j(a k_1 + b k_2)\} \leftrightarrow f(x_1 + a, x_2 + b) \quad (1)$$

Note that both $F(k_1, k_2)$ and its dual $f(x_1, x_2)$ are periodic functions so it is implicitly assumed that translations cause the image to be "wrapped around". We shall refer to this as a *circular translation*.

2.1.2 Reciprocal Scaling

Scaling the axes in the spatial domain causes an inverse scaling in the frequency domain:

$$\frac{1}{\rho} F\left(\frac{k_1}{\rho}, \frac{k_2}{\rho}\right) \leftrightarrow f(\rho x_1, \rho x_2) \quad (2)$$

2.1.3 The Rotation Property

Rotating the image through an angle θ in the spatial domain causes the Fourier representation to be rotated through the same angle:

$$F(k_1 \cos \theta - k_2 \sin \theta, k_1 \sin \theta + k_2 \cos \theta) \leftrightarrow f(x_1 \cos \theta - x_2 \sin \theta, x_1 \sin \theta + x_2 \cos \theta) \quad (3)$$

2.2 Translation Invariance

From the translation property of the Fourier transform it is clear that spatial shifts affect only the phase representation of an image. This leads to the well known result that the DFT magnitude is a circular translation invariant. An ordinary translation can be represented as a cropped circular translation.

2.3 Rotation and Scale Invariance

The basic translation invariants described in section 2.2 may be converted to rotation and scale invariants by means of a *log-polar mapping*. Consider a point $(x, y) \in \mathbb{R}^2$ and define:

$$\begin{aligned} x &= r^\mu \cos \theta \\ y &= r^\mu \sin \theta \end{aligned} \quad (4)$$

where $\mu \in \mathbb{R}$ and $0 \leq \theta < 2\pi$. One can readily see that for every point (x, y) there is a point (μ, θ) that uniquely corresponds to it. Note that in the new coordinate system *scaling* and *rotation* are converted to a translation of the μ and θ coordinates respectively. At this stage one can implement a rotation and scale invariant by applying a translation invariant in the log-polar coordinate system. Taking the Fourier transform of a log-polar map (LPM) is equivalent to computing the Fourier-Mellin transform [1].

2.4 Rotation, Scale and Translation Invariance

Consider two invariant operators: \mathcal{F} which extracts the modulus of the Fourier transform and \mathcal{F}_M which extracts the modulus of the Fourier-Mellin transform.

Applying the hybrid operator $\mathcal{F}_M \circ \mathcal{F}$ to an image $f(x, y)$ we obtain:

$$I_1 = [\mathcal{F}_M \circ \mathcal{F}] f(x, y) \quad (5)$$

Let us also apply this operator to an image that has been translated, rotated and scaled:

$$\begin{aligned} I_2 &= \{\mathcal{F}_M \circ \mathcal{F} \circ \mathcal{R}(\theta) \circ \mathcal{S}(\rho) \circ \mathcal{T}(\alpha, \beta)\} f(x, y) \\ &= \{\mathcal{F}_M \circ \mathcal{R}(\theta) \circ \mathcal{F} \circ \mathcal{S}(\rho) \circ \mathcal{T}(\alpha, \beta)\} f(x, y) \\ &= \left[\mathcal{F}_M \circ \mathcal{R}(\theta) \circ \mathcal{S}\left(\frac{1}{\rho}\right) \circ \mathcal{F} \circ \mathcal{T}(\alpha, \beta) \right] f(x, y) \\ &= [\mathcal{F}_M \circ \mathcal{F}] I(x, y) \\ &= I_1 \end{aligned} \quad (6)$$

Hence $I_1 = I_2$ and the representation is rotation, scale and translation invariant. The rotation, scale and translation (RST) invariant just described is sufficient to deal with any combination of rotation, scale and translation transformations in any order [1].

3 Watermarking Implementation

Figure 1 illustrates the process of obtaining the RST transformation invariant from a digital image. Figure 1 is for illustrative purposes only since the process used in practice is more complicated; the main difficulty being that the time and frequency domain are both discretely sampled spaces. The watermark takes the form of a two dimensional spread spectrum signal in the RST transformation invariant domain. Note that the size of the RST invariant representation depends on the resolution of the log-polar map which can be kept the same for all images. This is a convenient feature of this approach which helps to standardise the embedding and detection algorithms.

4 Examples

Figure 2 is a standard image which contains a 104 bit rotational and scale invariant watermark. The watermark is encoded as a spread spectrum signal which was embedded in the RS invariant domain. Figure 2 was rotated by 143° and scaled by a factor of 75% along each axis. The embedded mark which read "The watermark" in ASCII code was recovered from this watermarked image. It was also found that the watermark survived lossy image compression using JPEG at normal settings (75% quality factor). Other methods exist that tolerate JPEG compression down to 5% quality factor [2, 6]; work is underway to combine these with this approach. In addition, the mark is also reasonably resistant to cropping and could be recovered from a segment approximately 50% of the size of the original image.

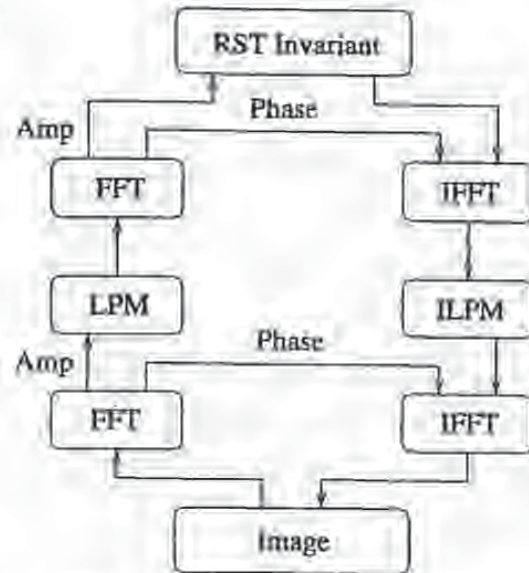


Figure 1: A diagram of a prototype RST invariant watermarking scheme.

5 Conclusion

This paper has outlined the theory of integral transform invariants and proposed that this can be used to produce watermarks that are resistant to translation, rotation and scaling. The importance of invertibility of the invariant representation was emphasised. One of the significant points is the application of the Fourier-Mellin transform¹ to digital image watermarking.

An example of a rotation and scale invariant watermark was presented. As one might expect, this proved to be robust to changes in scale and rotation. It was also found to be weakly resistant to lossy image compression and cropping. The robustness of the embedded mark to these attacks will be greatly improved with future work.

On its own, the invariant watermark discussed in this paper cannot resist changes in aspect ratio or shear transformations. There is no obvious means

¹ Digimarc Corporation have independently produced their PictureMarc software which uses the Fourier-Mellin transformation to achieve invariance to rotation and scale transformations. The technical details, which are included in a patent application, are not available to the authors at the time that this paper is being written.



Figure 2: A watermarked image of a hand-drill that has been rotated by 143 degrees and scaled by 75%. The embedded mark was recovered from this image.

of constructing an integral transform-based operator that is invariant to these transformations. However, work is currently in progress to find a means of searching for the most likely values of aspect ratio and shear factor, and then to apply the necessary corrections during watermark extraction.

Acknowledgments

This work is supported by the Swiss National Science Foundation (grant no. 5003-45334). We wish to thank Dr David McG. Squire, Sergei Starchik and Dr Feng-Lin for their extremely helpful advice on the theory of invariants and Dr A. Z. Tirkel for many stimulating conversations and for exchanging many ideas. We are also grateful to Dr Alexander Herrigel and Adrian Perrig for their useful comments. Thanks also to Geoff Rhoads for answering our queries about PictureMarc.

References

- [1] R. D. Brandt and F. Lin. Representations that uniquely characterize images modulo translation, rotation and scaling. *Pattern Recognition Letters*, 17:1001-1015, August 1996.

- [2] I. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for images, audio and video. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 243-246, Lausanne, Switzerland, September 16-19 1996.
- [3] J.F. Delaigle, C. De Vleeschouwer, and B. Macq. Digital Watermarking. In *Conference 2659 - Optical Security and Counterfeit Deterrence Techniques*, San José, February 1996. SPIE Electronic Imaging: Science and Technology, pp. 99-110.
- [4] Joo S. Lim. *Two-Dimensional Signal and Image Processing*. Prentice-Hall International, 1990.
- [5] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Phase watermarking of digital images. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 239-242, Lausanne, Switzerland, September 16-19 1996.
- [6] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Watermarking digital images for copyright protection. *IEE Proceedings on Vision, Image and Signal Processing*, 143(4):250-256, August 1996. Invited paper, based on the paper of the same title at the IEE Conference on Image Processing and Its Applications, Edinburgh, July 1995.
- [7] I Pitas. A method for signature casting on digital images. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 215-218, Lausanne, Switzerland, September 16-19 1996.
- [8] B. Schneier. *Applied Cryptography*. Wiley, 2nd edition, 1995.
- [9] J. Smith and B. Comiskey. Modulation and information hiding in images. In Ross Anderson, editor, *Proceedings of the First International Workshop in Information Hiding*, Lecture Notes in Computer Science, pages 207-226, Cambridge, UK, May/June 1996. Springer Verlag.
- [10] D. McG. Squire. *Model-based Neural Networks for Invariant Pattern Recognition*. PhD thesis, Curtin University of Technology, Perth, Western Australia, October 1996.
- [11] A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne. Electronic watermark. In *Diata-95*, pages 666-672, Macquarie University, Sydney, December 1993.

Rotation, Scale and Translation Invariant Digital Image Watermarking

Joseph J.K. Ó Ruanaidh and Thierry Pun

*Centre Universitaire d'Informatique, Université de Genève, 24 rue Général
Dufour, CH-1211 Genève 4, Switzerland*

A digital watermark is an invisible mark embedded in a digital image which may be used for Copyright Protection. This paper describes how Fourier-Mellin transform-based invariants can be used for digital image watermarking. The embedded marks are designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required for extracting the embedded mark.

1 Introduction

Computers, printers and high rate digital transmission facilities are becoming less expensive and more widespread. Digital networks provide an efficient cost-effective means of distributing digital media. The popularity of the World Wide Web has clearly demonstrated the commercial potential of the digital multimedia market. Unfortunately however, digital networks and multimedia also afford virtually unprecedented opportunities to pirate copyrighted material. The idea of using a robust digital watermark to detect and trace copyright violations has therefore stimulated significant interest among artists and publishers. As a result, digital image watermarking has recently become a very active area of research. Techniques for hiding watermarks have grown steadily more sophisticated and increasingly robust to lossy image compression and standard image processing operations, as well as to cryptographic attack.

Many of the current techniques for embedding marks in digital images have been inspired by methods of image coding and compression. Information has been embedded using the Discrete Cosine Transform (DCT) [16,34,5,6] Discrete Fourier Transform magnitude and phase [15], Wavelets [16], Linear Predictive Coding [13] and Fractals [9,22]. The key to making watermarks robust has been the recognition that in order for a watermark to be robust it must be embedded in the *perceptually significant* components of the image [16,5,6]. The term "perceptually significant" is somewhat subjective but it suggests that a

* This work is supported by the Swiss National Science Foundation (grant no. 5003-45334)

good watermark is one which takes account of the behaviour of human visual system. Objective criteria for measuring the degree to which an image component is significant in watermarking have gradually evolved from being based purely on energy content [16,5,6] to statistical [20] and psychovisual [27,10] criteria.

Digital watermarking is also fundamentally a problem in digital communications [16,25,5,6]. In parallel with the increasing sophistication in modelling and exploiting the properties of the human visual system, there has been a corresponding development in communication techniques. Early methods of encoding watermarks were primitive and consisted of no more than incrementing an image component to encode a binary '1' and decrementing to encode a '0' [3,16]. Tirkel and Osborne [29] were the first to note the applicability of spread spectrum techniques to digital image watermarking. Since then there has been an increasing use of spread spectrum communications in digital watermarking. It has several advantageous features such as cryptographic security [29,30,6], and is capable of achieving error free transmission of the watermark near or at the limits set by Shannon's noisy channel coding theorem [16,25].

Spread spectrum is an example of a symmetric key [24] cryptosystem. System security is based on proprietary knowledge of the keys (or the seeds for pseudo-random generators) which are required to embed, extract or remove an image watermark. One proviso in the use of a spread spectrum system is that it is important that the watermarking process incorporate some non-invertible step which may depend on a private key or a hash function of the original image. Only in this way can true ownership of the copyright material be resolved [8].

The ability of humans to perceive the salient features of an image regardless of changes in the environment is something which humans take for granted [26,14]. We can recognise objects and patterns independently of changes in image contrast, shifts in the object or changes in orientation and scale. Gibson [12] makes the hypothesis that the human visual system is strongly tied to the ability to recognize invariants. It seems clear that an embedded watermark should have the same invariance properties as the image it is intended to protect. In this paper, we propose that an image watermark should be, so far as possible, encoded to be *invariant* to image transformations. We shall also demonstrate how image invariants can be used to construct watermarks that are unaltered by some of the most basic operations encountered in image processing; namely rotation, translation and changes of scale.

1.1 Nomenclature

This paper will make use of terms agreed during the 1996 Workshop on Information Hiding [18]. The term "cover image" will be used to describe the unmarked original image and "stegoimage" for an image with one or more hidden embedded marks. One significant deviation from the recommended steganographic nomenclature is the frequent use of the term "watermark" to describe the embedded mark. The authors believe this usage is perfectly acceptable because it has become the norm.

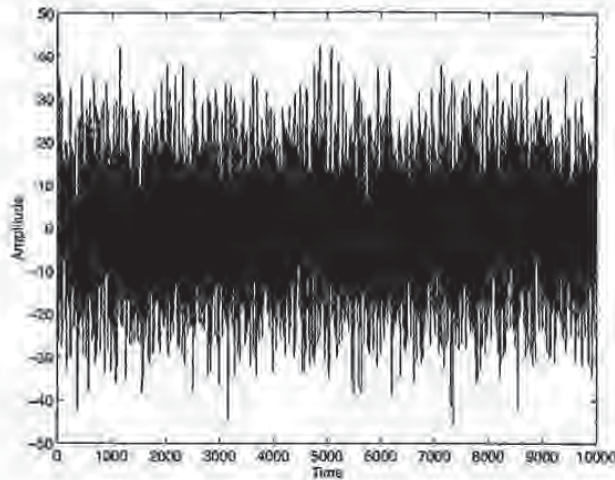


Fig. 1. An example of a spread spectrum signal used as a digital watermark.

2 Spread Spectrum

Pickholtz et al. [19] define spread spectrum communications as follows:

Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for despreading and subsequent data recovery.

Spread spectrum systems are also capable of approaching the Shannon limit for reliable communication. The fundamental information theoretic limits to reliable communication and its implications to digital watermarking have been discussed by some authors [16,25]. Note that the smaller is the number of bits of core information or "payload" contained in a watermark, the greater the chance of it being communicated without error.

Cox et al [7,6] recover a watermark by explicitly computing the correlation between the (noise corrupted) watermark recovered from the image with the perfect watermarks stored in a database. This is a very robust technique for watermark recovery but it is not very useful in practice because of the need for access to the database of marks and the large amount of computation required. In this paper the approach is similar to other spread spectrum approaches in that the watermark is embedded in the form of a pseudorandom sequence. However the approach is different to that of Cox in that it does not require access to a database of watermarks and is not particularly expensive computationally. In common with other spread spectrum techniques, in order

to embed a mark or to extract it, it is important to have access to the key which is simply the seed used to generate pseudo-random sequences. In the case of a public watermarking scheme the key is generally available and may even be contained in publically available software. In a private watermarking scheme the key is proprietary. A mark may be embedded or extracted by the key owner which in our model is the Copyright Holder. In this form spread spectrum is a symmetric key cryptosystem. The infrastructure required to generate, issue and store the keys is not described here.

From the point of view of embedding watermarks in documents given the keys or seeds the sequences themselves can be generated with ease. A good spread spectrum sequence is one which combines desirable statistical properties such as uniformly low cross correlation with cryptographic security. Examples of sequences used in spread spectrum systems used in digital watermarking include m-sequences, Gold codes, Kasami codes and Legendre sequences.

2.1 CDMA coding of digital watermarks

A method for encoding binary messages which can later be recovered given knowledge of the key used is described here. Suppose we are given a message which, without loss of generality, is in binary form b_1, b_2, \dots, b_L where b_i are the bits. This can be written in the form of a set of symbols s_1, s_2, \dots, s_M , most generally by a change in a number base from 2 to B with $L \leq M \log_2 B$. The conversion from base 2 to a base which is a power of two is trivial. The next stage is to encode each symbol s_i in the form of a pseudorandom vector of length N . To encode the first symbol a pseudorandom sequence \vec{v} of length $N + B - 1$ is generated. To encode a symbol of values where $0 \leq s < B$ the elements $v_s, v_{s+1}, \dots, v_{s+B}$ are extracted as a vector \vec{r}_1 of length N . For the next symbol another independent pseudorandom sequence is generated and the symbol encoded as a random vector \vec{r}_2 . Each successive symbol is encoded in the same way. Note that even if the same symbol occurs in different positions in the sequence that no collision is possible because the random sequences used to encode them are different - in fact they are statistically independent. Finally the entire sequence of symbols is encoded as the summation

$$\vec{m}(t_i) = \sum_{j=1}^L \vec{r}_j(t_i) \quad (1)$$

The pseudo-random vector \vec{m} is decoded by generating all of the random vectors \vec{r}_j in turn and recovering the symbols which the largest value of cross correlation. In this example the pseudo-random generator (PRG) is an m-sequence generator but this is not material to the issue since any "good" generator will do. In addition, one may use two dimensional or higher dimensional arrays in place of the pseudorandom vectors described in the communications system above. One interesting point is that for M sufficiently large the statistical distribution of the message m should approach a Gaussian. This follows from the Central Limit Theorem. A Gaussian distributed watermark has the advantage that it is more difficult to detect. The variance increases with order M - in other words, the expected peak excursion of the sequence is only order

M . One can expect that a message with $M = 100$ symbols will only have ten times the amplitude of a message with $M = 1$ symbols. This is very good from the point of view of minimising the visibility of the watermark.

Figure 1 shows a spread spectrum signal $s(t)$ composed of a linear combination of L random vectors $r_l(t)$ as given by equation 1. Each random vector is specifically chosen to represent a particular symbol occupying a position in the message. A symbol may be composed of any number of bits. In our case each symbol is eight bits long and the number of random vectors L is nineteen. This is a form of Direct Sequence Code Division Multiple Access (DS-SS) spread spectrum communications. The encoded message in Figure 1 reads "This is a watermark".

This form of spread spectrum is resistant to cropping (providing it is resynchronised), non-linear distortions of amplitude and additive noise. Also, if it has good statistical properties it should be mistaken for noise and go undetected by an eavesdropper. The specific choice of method for generating the pseudorandom sequence has direct implications for reliability and cryptographic security of the embedded mark. Pseudorandom number generators described in watermarking literature include Gold Codes, Kasami codes, m-sequences [32,29,33,30] and perfect maps [31].

There are however some drawbacks to using direct sequence spread spectrum. Although a spread spectrum signal as described above is extremely resistant to non-linear distortion of its amplitude and additive noise it is also intolerant of timing errors. Synchronization is of the utmost importance during watermark extraction. If watermark extraction is carried out in the presence of the cover image then synchronization is relatively trivial. The problem of synchronizing the watermark signal is much more difficult to solve in the case where there is no cover image. If the stegoimage is translated, rotated and scaled then synchronization necessitates a search over a four dimensional parameter space (X-offset, Y-offset, angle of rotation and scaling factor). The search space grows even larger if one takes into account the possibility of shear and a change of aspect ratio.

In this paper, the aim is to investigate the possibility of using invariant representations of a digital watermark to help avoid the need to search for synchronization during the watermark extraction process.

2.2 Error control codes

It is desirable to incorporate some form of error control coding into the above scheme. The method is symbol based rather than binary bit based as in normal error codes. Because in this implementation each symbol may be correctly received or not, one finds that errors in the bit stream after despreading will occur in bursts, where each burst is due to an incorrectly decoded symbol. Reed Solomon (RS) codes [4,28,1] are powerful codes which are particularly suited to this application. RS codes can correct both errors (the locations of which are unknown) and erasures (the locations of which are exactly known). The probability of a false detection is extremely low. Reed Solomon codes are

particularly suited to this application for the following reasons : RS codes correct symbol errors rather than bit errors. RS codes can correct erasures as well as errors. Erasures can be factored out of the key equation which means that "erased symbols can be ignored. They do not play any role in the error control mechanism - an erasure is useless redundancy. We recognise that this property of being able to discard erased symbols has two advantages : If the posterior probability of a received symbol is low then it may be ignored. RS codes only come in standard sizes. For example a 255x8 bit code is common. Most commonly used RS error control codes appear to be too large to be used in watermarking. However, it is possible to make almost any RS code fit a watermarking application by judiciously selecting symbols as being erased (because they were never embedded in the document in the first place). For a symbol length of eight bits the corresponding RS code (based on a Galois extension field $GF(2^8)$) will be 255 symbols long. This is considerably longer than a watermark (typically approximately 100 bits only). However, this is not a problem since the unneeded symbols can be flagged as erasures and they play no part in the decoding process.

3 Integral Transform Invariants

There are many different kinds of image invariant such as moment, algebraic and projective invariants [23,26]. In this section we will briefly outline the development of several integral transform based invariants [26].

The invariants described below depend on the properties of the Fourier transform. There are a number of reasons for this. First, using integral transform-based invariants is a relatively simple generalization of transform domain watermarking. Second, the number of robust invariant components is relatively large which makes it suitable for spread spectrum techniques. Third, as we shall see, mapping to and from the invariant domain to the spatial domain is well-defined and it is in general not computationally expensive.

3.1 The Fourier Transform

Let the image be a real valued continuous function $f(x_1, x_2)$ defined on an integer-valued Cartesian grid $0 \leq x_1 < N_1, 0 \leq x_2 < N_2$.

The Discrete Fourier Transform (DFT) is defined as follows:

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(x_1, x_2) e^{-j2\pi n_1 k_1 / N_1 - j2\pi n_2 k_2 / N_2} \quad (2)$$

The inverse transform is

$$f(x_1, x_2) = \frac{1}{N_1 N_2} \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} F(k_1, k_2) e^{j2\pi k_1 x_1 / N_1 + j2\pi k_2 x_2 / N_2} \quad (3)$$

The DFT of a real image is generally complex valued

This leads to a

magnitude and phase representation for the image:

$$A(k_1, k_2) = |F(k_1, k_2)| \quad (4)$$

$$\Phi(k_1, k_2) = \angle F(k_1, k_2) \quad (5)$$

We now discuss the properties of the Fourier representation that are crucial to the construction of translation, rotation and scaling invariants.

3.1.1 The Translation Property

Shifts in the spatial domain cause a linear shift in the phase component.

$$F(k_1, k_2) \exp[-j(ak_1 + bk_2)] \leftrightarrow f(x_1 + a, x_2 + b) \quad (6)$$

Note that both $F(k_1, k_2)$ and its dual $f(x_1, x_2)$ are periodic functions so it is implicitly assumed that translations cause the image to be "wrapped around". We shall refer to this as a *circular translation*.

3.1.2 Reciprocal Scaling

Scaling the axes in the spatial domain causes an inverse scaling in the frequency domain.

$$\frac{1}{\rho} F\left(\frac{k_1}{\rho}, \frac{k_2}{\rho}\right) \leftrightarrow f(\rho x_1, \rho x_2) \quad (7)$$

An important example of this property is the Fourier transform of a delta function (which is infinitely narrow) which has a uniformly flat amplitude spectrum (and is infinitely wide).

3.1.3 The Rotation Property

Rotating the image through an angle θ in the spatial domain causes the Fourier representation to be rotated through the same angle.

$$\begin{aligned} &F(k_1 \cos \theta - k_2 \sin \theta, k_1 \sin \theta + k_2 \cos \theta) \\ &\leftrightarrow f(x_1 \cos \theta - x_2 \sin \theta, x_1 \sin \theta + x_2 \cos \theta) \end{aligned} \quad (8)$$

Note that the grid is rotated so the new grid points may not be defined. The value of the image at the nearest valid grid point may be estimated by interpolation.

3.2 Translation Invariance

From property 6 of the Fourier transform it is clear that spatial shifts affect only the phase representation of an image. This leads to the well known result that the DFT magnitude is a circular translation invariant. An ordinary translation can be represented as a cropped circular translation.

It is less well known that it is possible to derive invariants based on the phase representation. To do this involves eliminating the translation dependent linear term from the phase representation. Brandt and Lin [2] present two such translation invariants, namely the *Taylor invariant* which removes the linear phase term in the Taylor expansion of the phase and the *Hessian invariant* which removes this linear phase term by double differentiation.

We shall see in section 3.3 that properties 7 and 8 allow one to extend the basic translation invariants to cover changes of rotation and scale.

3.3 Rotation and Scale Invariance

The basic translation invariants described in section 3.2 may be converted to rotation and scale invariants by means of a *log-polar mapping*.

Consider a point $(x, y) \in \mathbb{R}^2$ and define:

$$\begin{aligned} x &= e^\mu \cos \theta \\ y &= e^\mu \sin \theta \end{aligned} \tag{9}$$

where $\mu \in \mathbb{R}$ and $0 \leq \theta < 2\pi$. One can readily see that for every point (x, y) there is a point (μ, θ) that uniquely corresponds to it.

The new coordinate system has the following properties:

Scaling is converted to a translation.

$$(\rho x, \rho y) \leftrightarrow (\mu + \log \rho, \theta) \tag{10}$$

Rotation is converted to a translation.

$$\begin{aligned} (x \cos(\theta + \delta) - y \sin(\theta + \delta), x \sin(\theta + \delta) + y \cos(\theta + \delta)) \\ \leftrightarrow (\mu, \theta + \delta) \end{aligned} \tag{11}$$

At this stage one can implement a rotation and scale invariant by applying a translation invariant in the log-polar coordinate system. Taking the Fourier transform of a log-polar map is equivalent to computing the Fourier-Mellin transform:

$$F_M(k_1, k_2) = \int_{-\infty}^{\infty} \int_0^{2\pi} f(e^\mu \cos \theta, e^\mu \sin \theta) \exp [i(k_1 \mu + k_2 \theta)] d\mu d\theta \quad (12)$$

The modulus of the Fourier-Mellin transform is rotation and scale invariant.

Many useful invariants are derived by finding an alternative coordinate system in which the effect of the transformation is replaced by a translation and applying a translation invariant operator in the new coordinate system. Squire [26] demonstrates how such invariants can be derived formally using the methods of Lie Group algebra.

3.3.1 The Commutative Property

It is interesting to show that the single parameter group of rotation transformations $\mathcal{R}(\theta)$ and the single parameter group of scale transformations $\mathcal{S}(\rho)$ commute.

$$\begin{aligned} \mathcal{R}(\theta) \circ \mathcal{S}(\rho) f(x, y) &= \mathcal{R}(\theta) f(\rho x, \rho y) \\ &= f(\rho x \cos \theta - \rho y \sin \theta, \rho x \sin \theta + \rho y \cos \theta) \\ &= \mathcal{S}(\rho) f(x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta) \\ &= \mathcal{S}(\rho) \circ \mathcal{R}(\theta) f(x, y) \end{aligned} \quad (13)$$

Similarly one can show [2] that the two parameter group of translation transformations $\mathcal{T}(\alpha, \beta)$ commutes neither with $\mathcal{R}(\theta)$, nor with $\mathcal{S}(\rho)$ nor with the joint transformation $\mathcal{RS}(\theta, \rho)$.

3.4 Rotation, Scale and Translation Invariance

Consider two invariant operators: \mathcal{F} which extracts the modulus of the Fourier transform and \mathcal{F}_M which extracts the modulus of the Fourier-Mellin transform. Applying the hybrid operator $\mathcal{F}_M \circ \mathcal{F}$ to an image $f(x, y)$ we obtain:

$$I_1 = [\mathcal{F}_M \circ \mathcal{F}] f(x, y) \quad (14)$$

Let us also apply this operator to an image that has been translated, rotated and scaled:

$$I_2 = [\mathcal{F}_M \circ \mathcal{F} \circ \mathcal{R}(\theta) \circ \mathcal{S}(\rho) \circ \mathcal{T}(\alpha, \beta)] f(x, y)$$

$$= [\mathcal{F}_M \circ \mathcal{R}(\theta) \circ \mathcal{F} \circ \mathcal{S}(\rho) \circ \mathcal{T}(\alpha, \beta)] f(x, y) \quad (15)$$

$$= \left[\mathcal{F}_M \circ \mathcal{R}(\theta) \circ \mathcal{S}\left(\frac{1}{\mu}\right) \circ \mathcal{F} \circ \mathcal{T}(\alpha, \beta) \right] f(x, y) \quad (16)$$

$$= [\mathcal{F}_M \circ \mathcal{F}] f(x, y) \quad (17)$$

$$= I_1 \quad (18)$$

Hence $I_1 = I_2$ and the representation is rotation, scale and translation invariant. Steps 15 and 16 follow from properties 8 and 7 of the Fourier transform respectively. The contraction in equation 17 is due to the invariance properties of \mathcal{F} and \mathcal{F}_M .

The rotation, scale and translation (\mathcal{RST}) invariant just described is sufficient to deal with any combination or permutation of rotation, scale and translation in any order [2].

To give a concrete example of its application, consider a copy of a stegoimage placed on a scanner from which we wish to extract an embedded mark. The image may be reduced or increased in size and will be, more often than not, at an angle of $\pm\epsilon$, $\pm 90 \pm \epsilon$ or even $180 \pm \epsilon$ degrees where $\pm\epsilon$ is some small random angle. The image is also likely to be translated. Using the invariants derived above it should be possible to extract an embedded mark regardless of orientation, scale or position.

3.5 Complete and Strong invariants

Brandt and Lin [2] define the important concept of *completeness*. A complete invariant represents "all the information contained in the image modulo the given transformation". In this sense a complete invariant is *almost* invertible. If two images have the same complete translation invariant then, by the definition of completeness, one must be a shifted version of the other. Such an invariant cannot be inverted uniquely because the mapping to the invariant domain is not a bijective function. Brandt and Lin [2] present an example where a complete Hessian invariant is inverted to yield the original image, albeit with the origin shifted and image wrapped around at the edges.

Ferraro and Caelli [11] in an earlier paper defined the related concept of *strong* invariance. "An integral transform is defined to be invariant in the strong sense if . . ." the amplitude representation is constant for all states of the transformation and different states are uniquely encoded in the phase component. The phase component may therefore be used to invert the invariant representation.

For convenience, the invariants used in this paper are strongly invariant. In image watermarking it is more convenient to use strong invariants because the last stage of the process of *embedding* a mark involves inverting the invariant representation to obtain the (marked) stegoimage. Invertibility is of no concern whatsoever during the extraction process.

4 Watermark Implementations

In this section we describe two different prototype schemes for embedding watermarks in digital images using \mathcal{RST} invariants. Typically, the watermark is embedded in a gray scale image or the luminance component of a colour image.

4.1 General scheme

Figure 2 illustrates the process of obtaining the \mathcal{RST} transformation invariant from a digital image. The watermark takes the form of a two dimensional spread spectrum signal in the \mathcal{RST} transformation invariant domain. Note that the size of the \mathcal{RST} invariant representation depends on the resolution of the log-polar map which can be kept the same for all images. This is a convenient feature of this approach which helps to standardise the embedding and detection algorithms.

4.1.1 Embedding a watermark

A Fourier transform (FFT) is first applied which is then followed by a Fourier-Mellin transform (A log-polar mapping (LPM) followed by a Fourier transform (FFT)). The invariant coefficients preselected for their robustness to image processing are marked using a spread spectrum signal. The inverse mapping is computed as an inverse FFT (IFFT) followed by an inverse Fourier-Mellin transform (An inverse log-polar mapping (ILPM) followed by an inverse FFT) Note that the inverse transformation from \mathcal{RST} invariant domain to the image domain uses the phase computed during the forward transformations from image domain to the \mathcal{RST} invariant domain.

4.1.2 Extracting a watermark

A watermark may be extracted without or without a cover image. In the case where there is no cover image the image is transformed to the \mathcal{RST} invariant domain and the watermark is decoded. This is similar in principle to the scheme described by Smith and Comiskey [25] whose approach is to "treat the image as noise" and overcome the interference from the stegoimage using spread spectrum communication. When a cover image is available it should be subtracted from the stegoimage and the difference transformed to the \mathcal{RST} invariant domain (since the operations in Figure 2 are linear with respect to image amplitude). Subtracting the cover image improves the performance of the detector because, as Smith and Comiskey point out, it eliminates the noise interference due to the stegoimage [25]. In many cases, image contrast may be distorted, for example by a scanner, in which case the effects of change of contrast must be compensated for in some way. Cox et al. [5,6] describe a method known as dynamic histogram warping [7] to carry this out.

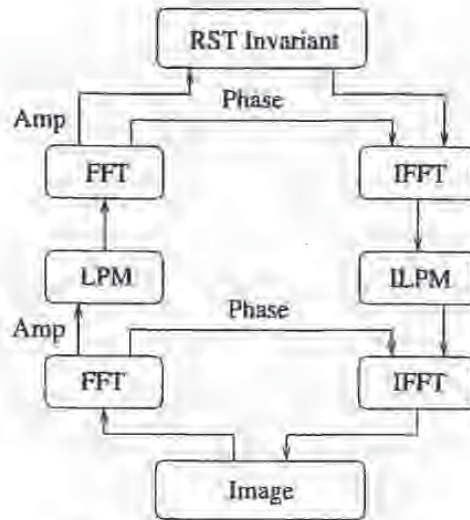


Fig. 2. A diagram of a prototype RST invariant watermarking scheme.

4.1.3 Practical considerations

There are a number of complications in implementing the processing steps depicted in Figure 2. The stegoimage must be real which in turn means that its amplitude spectrum ($A(k, l)$ where $0 \leq k < M$ and $0 \leq l < N$) as well as being positive ($A(k, l) \geq 0$) must also be positively symmetric:

$$A(k, l) = A(M - k, N - l) \quad (19)$$

The log-polar map of a positively symmetric matrix consists of two identical halves. This follows from the fact that the positive symmetry condition in equation 19 is written in polar coordinates as:

$$A(r, \theta) = A(r, \pi + \theta) \quad (20)$$

where $(M/2, N/2)$ is the centre of rotation. Since both halves of the log-polar map are identical then only one half need be used in the upper FFT of Figure 2. The spread spectrum signal is determined from the amplitude spectrum of this FFT. Applying the above in reverse gives an embedding algorithm which yields a real valued watermark.

The scheme described in Figure 2 works in principle but has some serious deficiencies in practice. The first difficulty is that both the log-polar mapping and the inverse log-polar mapping can cause a loss of image quality. The change of coordinate system means that some form of interpolation should be used.

Two simple forms of interpolation, nearest neighbour and bilinear interpolation [21], are in common use. Non-stationary low pass filtering can improve the performance by eliminating frequency aliasing. In practice the resolution of the log-polar map must be at least 512×512 for even a quite poor quality image. The second difficulty is numerical. Interpolation only performs well if neighbouring samples are of the same scale. This makes the computation of the Fourier-Mellin transform of the modulus of a Fourier transform somewhat problematic. A typical Fourier transform representation of an image is quite badly behaved in this respect since there are generally a few components of relatively large magnitude. This difficulty is resolved in the next section.

4.2 Cover Image Independent Scheme

The problems in embedding watermarks using the previous implementation described in Figure 2 can be circumvented by using the method illustrated in Figure 3. In this case the mark must be embedded in the \mathcal{RST} invariant domain independently of the original image. The advantage of using this approach is that the distortions caused by the inverse log-polar map are suffered only by the embedded mark itself and do not affect the stegoimage. Figure 4 shows the corresponding detection process which is relatively straightforward.

Note that when embedding the mark there is no phase component available for the first inverse Fourier transform. The first FFT operates on a random phase signal to keep the amplitude distribution of the inverse FFT reasonably flat. This is beneficial to the inverse log-polar map which performs best when the input is a smooth image. The second FFT uses the phase component directly from the cover image. The advantage in doing this is that matching the phase component of the embedded mark to that of the cover image helps to hide it because the embedded mark resembles the cover image. This follows from the research of Oppenheim and Lim [17] which demonstrates that image phase is far more important to image structure than image amplitude.

5 Examples

Figure 5 depicts a standard image of a mandrill. Figure 6 is the log-polar map of Figure 5. This image was computed using 600 grid points along the θ (angle) axis, 600 grid points along the μ (log-radial) axis and bilinear interpolation. Figure 7 is the inverted log-polar map computed using just 100 angular and 100 log-radial grid points and nearest neighbour interpolation. Note that the restoration grows progressively poorer away from the centre.

Figure 5 is in fact a stegoimage which contains a 104 bit rotational and scale invariant watermark. The watermark is encoded as a spread spectrum signal which was embedded in the RS invariant domain. Figure 5 was rotated by 143° and scaled by a factor of 75% along each axis to give the image shown in Figure 6. The embedded mark which read "The watermark" in ASCII code was recovered from this stegoimage. It was also found that the watermark survived

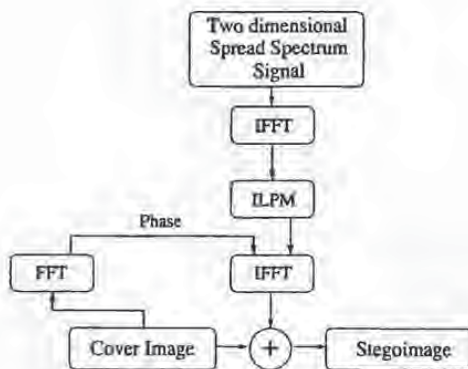


Fig. 3. A method of embedding a mark in an image which avoids mapping the cover image into the RST invariant domain.

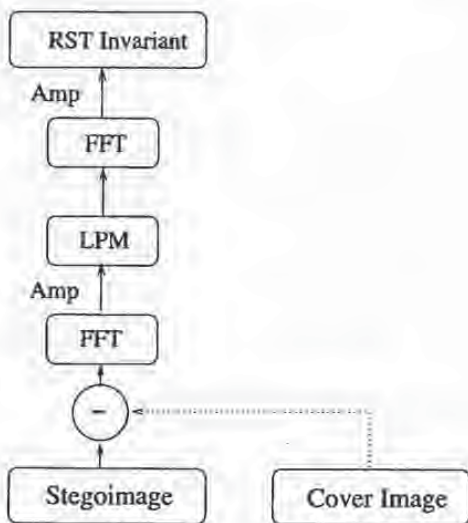


Fig. 4. A scheme to extract a mark from an image.

lossy image compression using JPEG at normal settings (75% quality factor). Other methods exist that tolerate JPEG compression down to 5% quality factor [7,6,16,15]; work is underway to combine these with this approach. In addition, the mark is also reasonably resistant to cropping and could be recovered from a segment approximately 50% of the size of the original image.