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

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

wherein the SECD comprises:

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

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

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

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

wherein the LCS comprises:

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

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

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

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

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

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

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

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

means <u>to</u> receive a copy of the content data set;

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

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

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

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

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

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

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

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

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

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

16. (previously presented) A system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD);

a Local Content Server (LCS);

a communications network interconnecting the SECD to the LCS; and

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

said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise 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), 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

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 6, 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 <u>issued</u> 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.

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.

> **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 <u>reasonable</u> 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.

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. (thereafter "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, 1479, 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. 53-67; 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* 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" 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 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 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 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).

<u>Claim 6 (depending from Claim 4)</u>

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).

<u>Claim 7 (depending from Claim 4)</u>

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).

<u>Claim 8 (depending from Claim 4)</u>

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 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 is 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 5)

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 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 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 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, 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 24)

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

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.

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 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

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

ENCLOSURES *(Check all that apply)*

☑ Fee Transmittal Form
  ☑ Fee Attached
☑ Amendment/Reply
  ☑ After Final
  □ Affidavits/declaration(s)
□ Extension of Time Request
□ Express Abandonment Request
□ Information Disclosure Statement
□ Certified Copy of Priority Document(s)
□ Reply to Missing Parts/ Incomplete Application
  □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

□ Drawing(s)
□ Licensing-related Papers
□ Petition
□ Petition to Convert to a Provisional Application
□ Power of Attorney, Revocation Change of Correspondence Address
□ Terminal Disclaimer
□ Request for Refund
□ CD, Number of CD(s) ____________
  □ Landscape Table on CD

□ After Allowance Communication to TC
□ Appeal Communication to Board of Appeals and Interferences
□ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
□ Proprietary Information
□ Status Letter
☑ Other Enclosure(s) (please identify below):

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. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number 10/049101

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))							
SEARCH FEE (37 CFR 1.16(k), (i), or (m))							
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))							
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X =		OR	X =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X =			X =	
APPLICATION SIZE FEE (37 CFR 1.16(s))	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(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A	RCE 8-9-07	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 31	Minus	** 31	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	* 7	Minus	*** 7	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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 1.

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 amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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	l1 and (safe$ or secur$ or protect$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:28
L3	35	l2 and (store or storage or storing or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
L4	34	l3 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:29
L5	26	l4 and author$	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 orlevel))	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	l7 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:34
L9	41	l8 and (authori$ or allow$ or permit$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:51
L10	37	l9 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

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

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 (qos 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	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
10/29/2007	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.** 10/049,101	**Applicant(s)** MOSKOWITZ, SCOTT A.	
	Examiner Jeremiah Avery	**Art Unit** 2131	

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

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) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ 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.

Claims 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 negatived 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 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").

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 (*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").

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, lies 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, lies 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, lies 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, lies 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, lies 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 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 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 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 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 Guedalia 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. 5,513,126 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.

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	Guedalia 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	08-1997	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, Pertinent Pages)
	U	
	V	
	W	
	X	

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

Index of Claims

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

MAIL DATE	DELIVERY MODE
01/29/2008	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.

8

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

All participants (applicant, applicant's representative, PTO personnel):

(1) *Jeremiah Avery*. (3) *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.

Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

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

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

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

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, differention 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-413A (10-07)
Approved for use through 10/31/2037. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 10/049,101 First Named Applicant: SCOTT MOSKOWITZ
Examiner: JEREMIAH AVERY Art Unit: 2131 Status of Application: PENDING

Tentative Participants:
(1) EXAMINER AVERY (2) EXAMINER
(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)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) RET 112 2nd para	1,3,16	N/A	[ ]	[ ]	[ ]
AFTER FINAL / STANDARD for		"capable of" "such that"			
(2) RET (102 b)	++	CITATION: STRINGER	[ ]	[ ]	[ ]
(3) RET (103a)	1-15/17-31	CITATION: STRINGER CITATION: BUEDALIA	[ ]	[ ]	[ ]
(4) RET of 16 45-A-173 RET	1-15/17-31	STRINGER AS 102b & 103a reference	[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Arguments to be Presented:
– No PRIOR ART OF RECORD FOR "digital watermark"; No PRIOR ART OF RECORD TO ACCEPT CONTENT FROM USERS; 1.104(c) discussing appropriate arguments & answers for TRAVERSED arguments; STRINGER & OFFICIAL NOTICE &/or PRE-APPEAL BRIEF COMMENTS RE: claim features; 770 AFFIDAVIT —

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 Examiner/SPE Signature

SCOTT MOSKOWITZ
Typed/Printed Name of Applicant or Representative

____
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

03-03-08 IFW 2131

Appl'n No. 10/049,101
Amendment/Reply to Office Action of October 29, 2007 dated February 29, 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	: 10/049,101	Confirmation No. 8028
Applicant	: Scott A. MOSKOWITZ, et al.	
Filed	: July 23, 2002	
TC/A.U.	: 2131	
Examiner	: Jeremiah 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:

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; and

said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content.

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

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

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

and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.

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

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

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

c) a rewritable storage medium whereby content received from an SECD and from an SU [[may be]] 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 is it is determined that one exists;

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

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

13. (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 Guedalia 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 Herrmann*, 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, 1195 (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. (thereafter "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 or 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 <u>the examiner must present a convincing line of reasoning</u> 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 <u>all</u> 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 states:

> ... 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 <u>already</u> 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 provie 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 <u>all</u> 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.

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. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | 1 | of | 2

Complete if Known	
Application Number	10/049,101
Filing Date	July 23 2002
First Named Inventor	Moskowitz
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6,088,455	07/11/2000	Logan et al.	
		US- 5,634,040	05/27/1997	Her et al.	
		US- 6,381,747	04/30/2002	Wonfor et al.	
		US- 4,969,204	11/06/1990	Melnychuck et al.	
		US- 6,966,002	11/15/2005	Torrubia-Saez	
		US- 6,263,313	07/17/2001	Milstead, et al.	
		US- 7,093,295	08/15/2006	Saito	
		US- 6,587,837	07/01/2003	Spagna 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	Blakely 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	Haber et al.	
		US- 5,136,647	08/04/1992	Haber 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*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
						□
						□
						□
						□
						□
						□

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete If Known	
Application Number	10/049 101
Filing Date	July 23 2002
First Named Inventor	Moskowitz
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 7,046,808	05/12/2006	Metois et al.	
		US- 6,430,301	08/06/2002	Petrovic	
		US- 2004/0059918	03/25/2004	Xu	
		US- 6,345,100	02/05/2002	Levine	
		US- 2004/0093521	05/13/2004	Hamadeh et al.	
		US- 2007/0083467	04/12/2007	Lindahl et al.	
		US- 7,231,524	06/12/2007	Burns	
		US- 2005/0246554	11/03/2005	Batson	
		US- 6,668,325	02/23/2003	Collberg 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	Michak et al.	
		US- 7,150,003	12/12/2006	Naumovich et al.	
		US- 6,389,538	05/14/2002	Gruse et al.	
		US- 5,513,126	04/30/1996	Harkins et al.	
		US- 5,657,461	08/12/1997	Harkins et al.	
		US- 4,390,898	06/28/1983	Bond et al.	
		US- 5,471,533	11/28/1995	Wang et al.	

FOREIGN PATENT DOCUMENTS

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

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (10-07)
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 persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

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

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		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:	
		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.	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997, 4 pages.	
		Joseph 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 citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1 of 2

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

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		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 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	10/049,101
		Filing Date	July 23 2002
		First Named Inventor	MOSKOWITZ
(Use as many sheets as necessary)		Art Unit	2131
		Examiner Name	AVERY
Sheet 2	of 2	Attorney Docket Number	80408.0001

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 conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/049101
Filing Date	July 23 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		STAIND (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 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

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

(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)

(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).

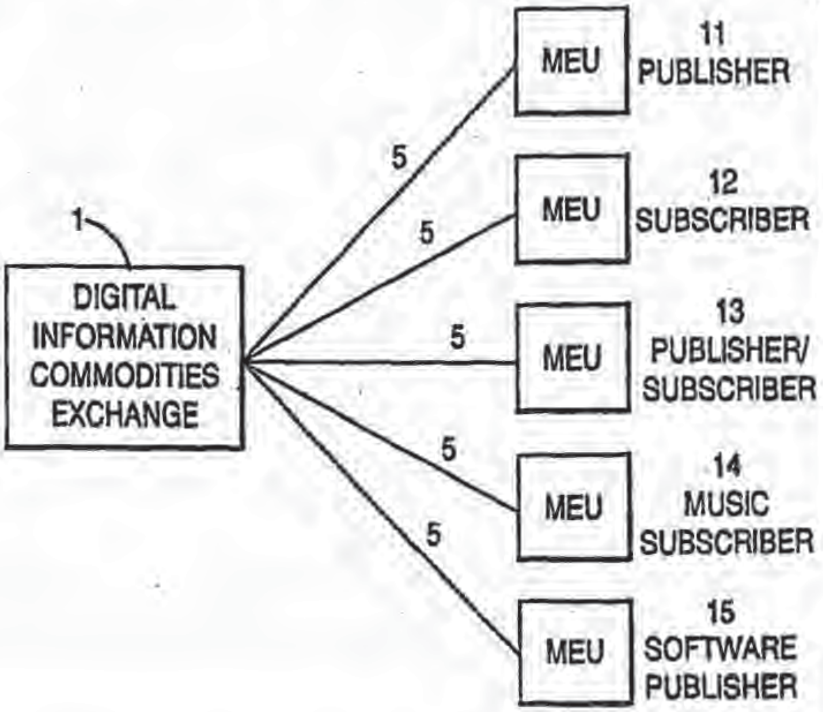
(81) Designated States: CA, CN, JP, KR, SG, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

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

DIGITAL INFORMATION COMMODITIES EXCHANGE WITH VIRTUAL MENUING

FIELD OF THE INVENTION

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.

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 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 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 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.

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. AOL 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 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.

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.

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.

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.

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.

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

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.

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.

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.

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. 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, 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. 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 publisher 11 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 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 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 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 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 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. 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 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, 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 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 unit can then provide any necessary data compression. The signal can then be sent over a telephone line 5 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 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 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-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, 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 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 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 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 22, an apparatus for inputting commands 26 (e.g., a keyboard or a pointing device), and software for user interaction. 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 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 24 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.

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 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 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 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 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 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 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 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 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 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 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 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. 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 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.

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.

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.

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.

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 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 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.

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 the client. The client displays the menu which contained the menu it previously displayed.

SelectCurrent

This signals the host to perform some operation related 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: 1 › = i › = R)

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.

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 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 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.

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 each item.

Menu Update

Data included in this message can be used to alter the display of individual menu items without redrawing a 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, 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 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 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, 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. 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 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 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 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 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.

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 1 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 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 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 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 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,

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 expandable units over two transmission media simultaneously.

2. The system for the exchange of digital information packets of claim 1, wherein said input source 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:

software running on a microprocessor suitable for selecting digital information;

a system for entering commands;

an input;

an output; and

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:

software suitable for selecting digital information;

a system for entering commands; and

a parallel line;

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:

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 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 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 packets, comprising:

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

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

(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 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 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 information packet directory entry and said publisher address;

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

(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.

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

storing said transferred digital information packet on a magnetic medium.

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.

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.

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.

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,

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 utilized to speed said transfer of said digital information packet.

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.

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

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;

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

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,

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,

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 pockets 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.

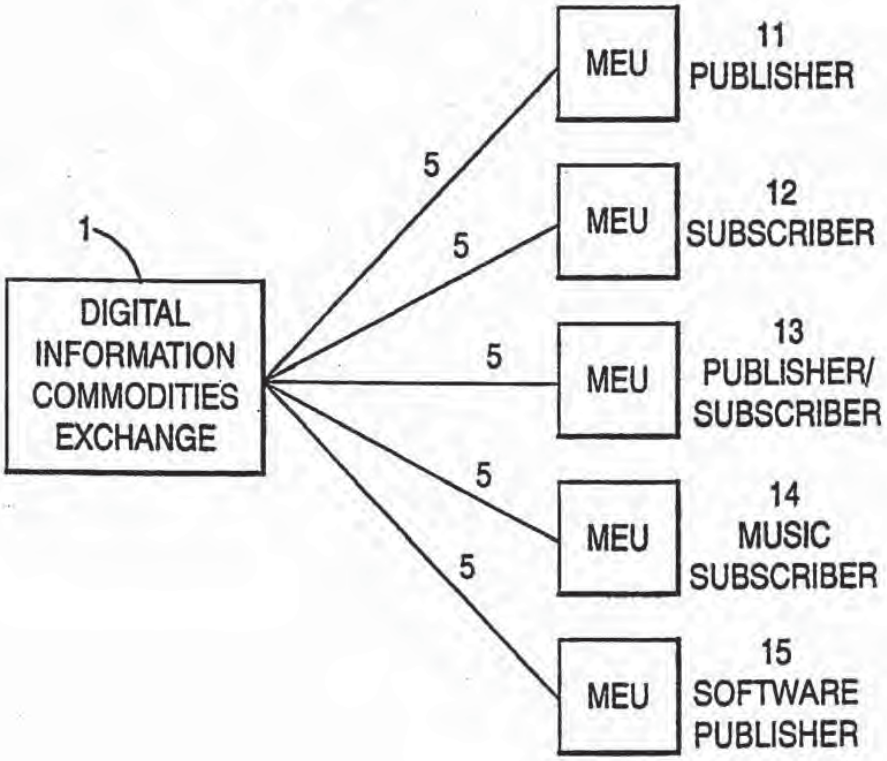
28. The system of claim 21 wherein at least one of said MEUs is connected directly to at least one other of said MEUs over one transmission medium.

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.

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

FIG. 1


1
DIGITAL INFORMATION COMMODITIES EXCHANGE
5
5
5
5
5
MEU
11 PUBLISHER
MEU
12 SUBSCRIBER
MEU
13 PUBLISHER/ SUBSCRIBER
MEU
14 MUSIC SUBSCRIBER
MEU
15 SOFTWARE PUBLISHER

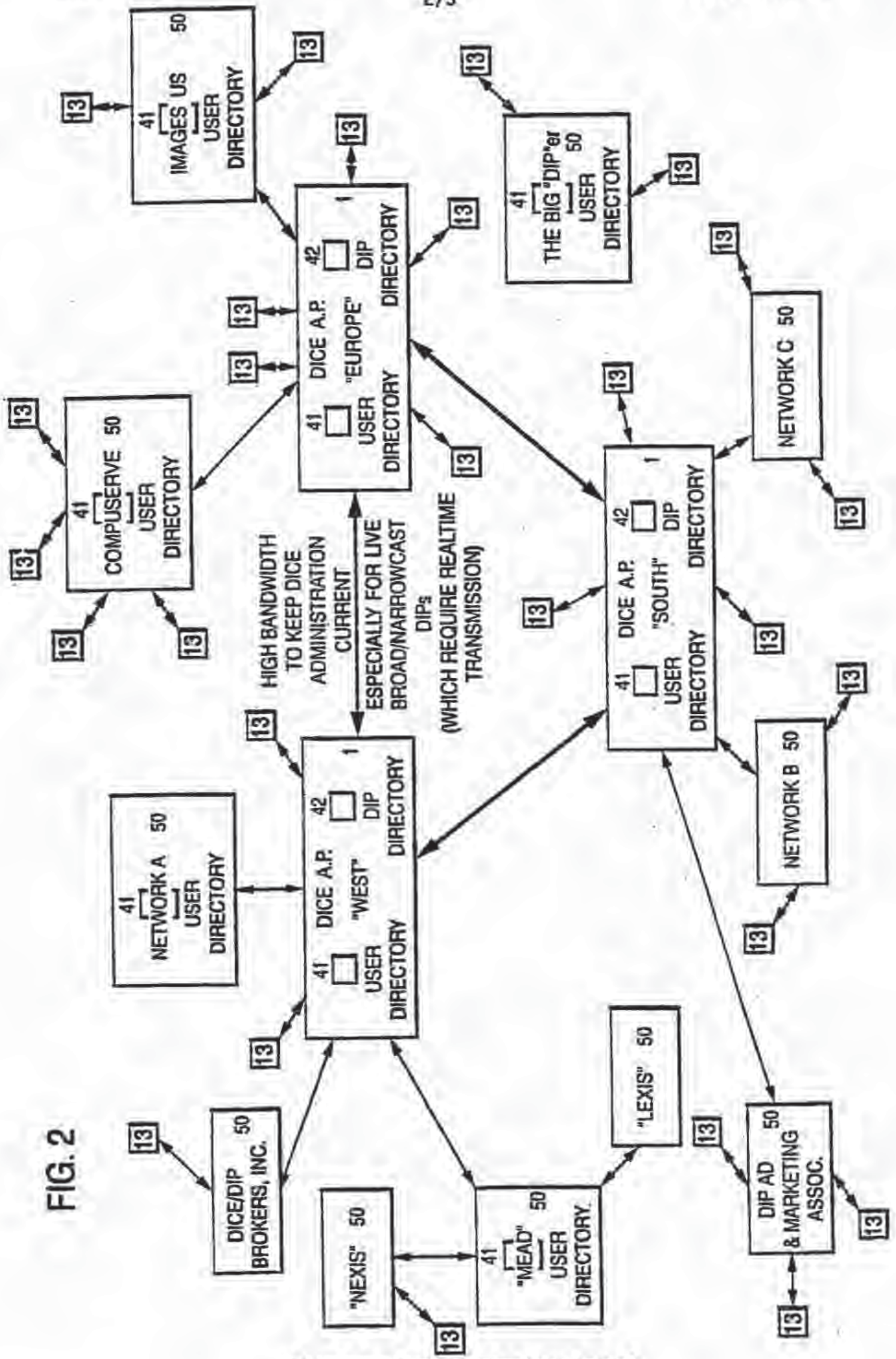

41 IMAGES US USER DIRECTORY 50
13
41 COMPUSERVE USER DIRECTORY 50
41 USER DIRECTORY
DICE A.P. "EUROPE"
42 DIP DIRECTORY 1
THE BIG "DIP"er USER DIRECTORY 41 50
HIGH BANDWIDTH TO KEEP DICE ADMINISTRATION CURRENT ESPECIALLY FOR LIVE BROAD/NARROWCAST DIPs (WHICH REQUIRE REALTIME TRANSMISSION)
NETWORK C 50
41 USER DIRECTORY
DICE A.P. "SOUTH"
42 DIP DIRECTORY 1
41 NETWORK A USER DIRECTORY 50
41 USER DIRECTORY
DICE A.P. "WEST"
42 DIP DIRECTORY 1
NETWORK B 50
DICE/DIP BROKERS, INC. 50
"LEXIS" 50
"NEXIS" 50
41 "MEAD" USER DIRECTORY 50
DIP AD & MARKETING ASSOC. 50

FIG. 2

FIG. 3

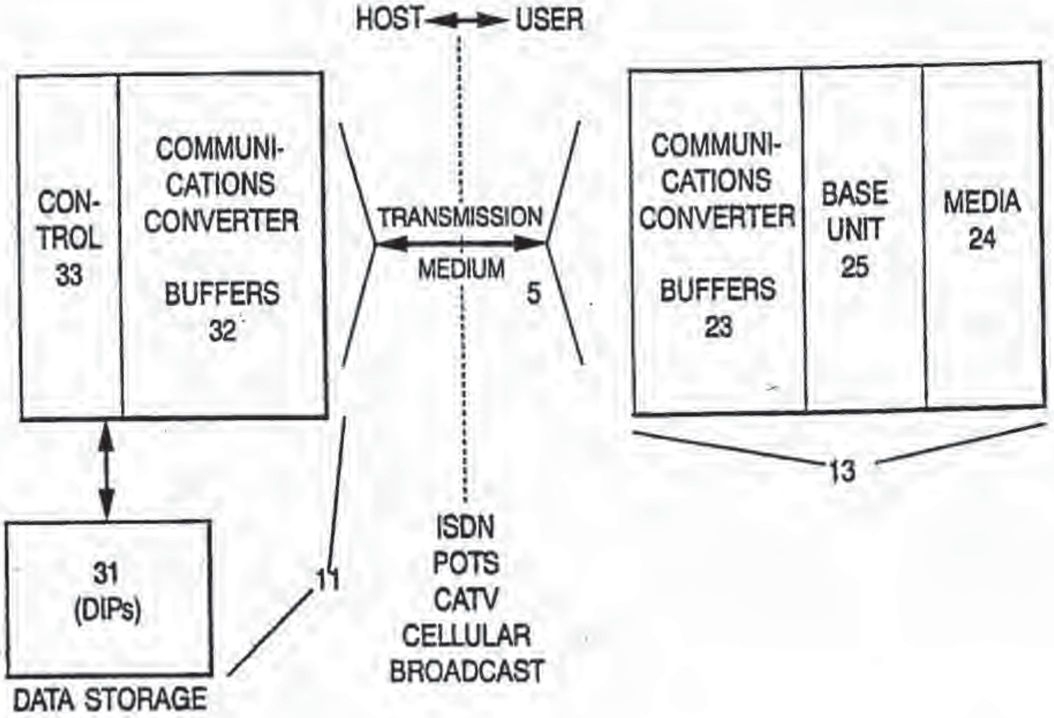
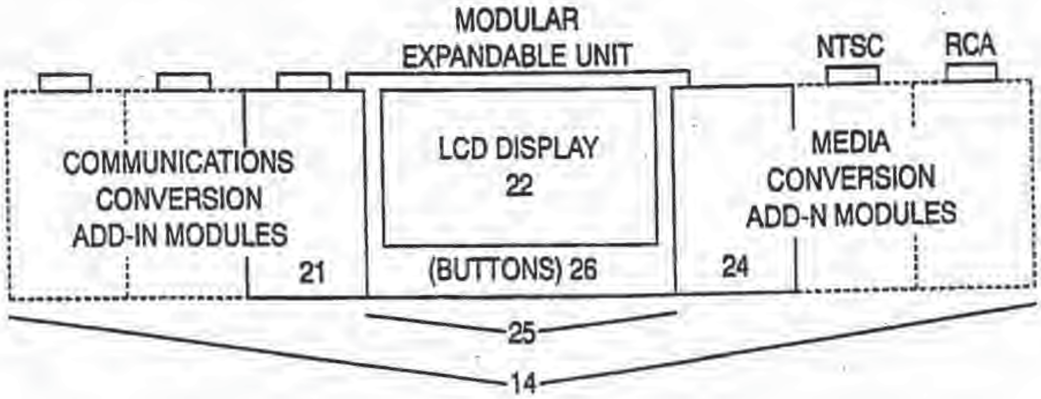

HOST
USER
CON-TROL 33
COMMUNI-CATIONS CONVERTER
BUFFERS 32
TRANSMISSION
MEDIUM
5
COMMUNI-CATIONS CONVERTER
BUFFERS 23
BASE UNIT 25
MEDIA 24
13
31 (DIPs)
DATA STORAGE
11
ISDN
POTS
CATV
CELLULAR
BROADCAST

FIG. 4


MODULAR EXPANDABLE UNIT
NTSC
RCA
COMMUNICATIONS CONVERSION ADD-IN MODULES
21
LCD DISPLAY 22
(BUTTONS) 26
24
MEDIA CONVERSION ADD-N MODULES
25
14

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. : 370/32, 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

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be part of particular relevance		
"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"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	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) 305-3230	Authorized officer B. Harden for HUY D. VU Telephone No. (703) 308-6602

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 modula 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.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L	A2	(11) International Publication Number: WO 96/42151 (43) International Publication Date: 27 December 1996 (27.12.96)

(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).

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

(54) Title: STEGANOGRAPHIC METHOD AND DEVICE

(57) Abstract

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.

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

STEGANOGRAPHIC METHOD AND DEVICE

Definitions

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 specifically refers to digitzed 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.

"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 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

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.

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.

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.

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.

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

1) Encryption
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, my 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 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.

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 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 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.

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.

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.

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 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 "ftp://sumex-aim.stanford.edu/info-mac/cmp/stego10a2.hqx". This application demonstrates a simple steganographic technique to encode a text message into a graphical image without significantly distorting the image.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

Detailed Description

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

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:

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.

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.

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.

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.

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 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 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.

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 audit trail of ownership my 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. 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, 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,

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

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 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.

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 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 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

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

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.

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 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.

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.

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 ½ the sampling rate).

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 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

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.

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.

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.

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 by rotated by a number corresponding to the phase, in bits to the left and XORed with the primary mask to 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.

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 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.

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 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.

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.

The encoder will also prepare the package of additional information so that it contains an easily recognizable start of message delimeter, 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 delimeter 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 delimeters 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 delimeter are used. If each sample is random, then each bit has a 50% probably of matching the delimeter 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.

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.

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.

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 delimeter 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:

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. 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.

Now to account for delimeters 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.

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 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 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 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 greater than the rounding error should work, without significantly degrading the output samples.

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

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 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 delimeter, 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 delimeter. 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 delimeter, bit-by-bit into each consecutive window. As soon as it has processed the last bit of the SOM delimeter 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 then 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 delimeter 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 delimeter. 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 delimeter or it exhausts the sample stream without decoding a message. If the decoder can match completely the start of message delimeter 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 delimeter 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 un-synchronized 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.

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 delimeter 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.

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?

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.

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.

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:

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.

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.

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.

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.

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.

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

(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

the title
the artist
the copyright holder
the body to which royalties should be paid
general terms for publishers' distribution
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 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 transmit a short agreement, the Distribution Agreement to the Publisher, Joe's Online Emporium which lists

the content title
the publisher's identification
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 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 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, 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 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 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 ftp site the Authority should be able to 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.

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-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 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 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

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.

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 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.

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.

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.

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 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.

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. 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.

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 bye, 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, on ebit 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 preceeding encoding windows in the stream.

Once the message is entirely encoded, including its special end of message marker bit stream, encode() resets it 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;

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;

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

i) a clock which generates a clock signal to drive (b) and control the operation of the apparatus.

3. A method of encoding information into a sample stream of data, said method comprising the steps of:

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 stream;

B) obtaining a message to be encoded;

C) generating a message bit steam 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;

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;

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 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;

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 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:

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 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 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 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 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;

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 valves 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≥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 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;

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:

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>1);

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 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;

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 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;

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;

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

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.

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.

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.

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.

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.

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.

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;

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.

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,
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,
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 form 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 data

the content title,
consumer identification,
the terms of distribution,
the consideration paid for the content,
a brief statement of agreement, and

the publisher uses a public key cryptosystem to sign the combined information and finally encodes the signed information.

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.

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.

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.

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 valves 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.

28. The method of claim 8, wherein the decoding of the message bit in step J includes mapping a range of supply values onto a particular message bit value.

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 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 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 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.--

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/00

A1

(11) International Publication Number: WO 97/26732

(43) International Publication Date: 24 July 1997 (24.07.97)

(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).

(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).

Published
With international search report.

(54) Title: METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

(57) Abstract

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.

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	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

FIELD OF INVENTION

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, video games, and computer software. One method of protecting copyrights in the digital 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 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 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.

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 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 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 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 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 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 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 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 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.

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 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 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 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 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 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 authorization of the copy in possession by the user. Without such verification, the functions sought out by the user in 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.

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 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 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 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 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, 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 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 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, 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 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 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 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 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 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 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 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 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.

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. 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 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 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 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 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 types, unless special care is taken to prevent work-a-rounds.

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 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 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. 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 "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 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 into one or several data resources using the stega-cipher 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 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 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 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 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 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. 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. 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 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 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 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 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 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 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' 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 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 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 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.

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. A method of associating executable object code with a digital sample stream by means of a digital watermark wherein the digital watermark contains executable object code and is encoded into the digital sample stream.

2. The method of claim 1 wherein a key to access the digital watermark is a function of a collection of license information pertaining to the software which is accessing the watermark

where license information consists of one or more of the following items:

Owning Organization name;
Personal Owner name;
Owner Address;
License code;
Software serialization number;
Distribution parameters;
Appropriate executable general computing device architecture;
Pricing; and
Software Metering details.

3. The method of claim 1 further comprising the step of transmitting the digital sample stream, via a transmission means, from a publisher to a subscriber

wherein transmission means can selected from the group of

soft sector magnetic disk media;
hard sector magnetic disk media;
magnetic tape media;
optical disc media;
Digital Video Disk media;
magneto-optical disk media;
memory cartridge;
telephone lines;

SCSI;
Ethernet or Token Ring Network;
ISDN;
ATM network;
TCP/IP network;
analog cellular network;
digital cellular network;
wireless network;
digital satellite;
cable network;
fiber optic network; and
electric powerline network.

4. The method of claim 1 where the object code to be encoded is comprised of series of executable machine instructions which perform the function of

processing a digital sample stream for the purpose of modifying it or playing the digital sample stream.

5. The method of claim 3 further comprising the steps of:

decoding said digital watermark and extracting object code;

loading object code into computer memory for the purpose of execution;

executing said object code in order to process said digital sample stream for the purpose of playback.

6. A method of assembling an application to be protected by watermark encoding of essential resources comprising the steps of:

assembling a list of identifiers of essential code resources of an application where identifiers allow the code resource to be accessed and loaded into memory;

providing license information on the licensee who is to receive an individualized copy of the application;

storing license information in a personalization resource which is added to the list of application data resources;

generating a digital watermark key from the license information; using the key as a pseudo-random number string to select a list of suitable digital sample data resources, the list of essential code resources, and a mapping of which essential code resources are to be watermarked into which data resources;

storing the map, which is a list of paired code and data resource identifiers, as a data resource, which is added to the application;

adding a digital watermark decoder code resource to the application, to provide a means for extracting essential code resource from data resources, according to the map;

processing the map list and encoding essential code resources into digital sample data resources with a digital watermark encoder;

removing self-contained copies of the essential code resources which have been watermarked into data resources; and

combining all remaining code and data resources into a single application or installer.

7. A method of intermittently relocating application code resources in computer memory, in order to prevent, discourage, or complicate attempts at memory capture based code analysis.

8. The method of claim 7 additionally comprising the step of

assembling a list of identifiers of code resources of an application where identifiers allow the code resource to be accessed and loaded into memory.

9. The method of claim 8 additionally comprising the step of modifying application program structure to make all code resource calls indirectly, through the memory scheduler, which looks up code resources in its list and dispatches calls.

10. The method of claim 9 additionally comprising the step of intermittently rescheduling or shuffling all code resources prior to or following the dispatch of a code resource call through the memory scheduler.

11. The method of claim 10 additionally comprised of the step of the memory scheduler copying itself to a new location in memory.

12. The method of claim 11 additionally comprising the step of modifying the stack frame, program counter, and memory registers of the CPU to cause the scheduler to jump to the next instruction comprising the scheduler, in the copy, to erase the previous memory instance of the scheduler, and changing all memory references to the scheduler to reflect its new location, and to return from the copy of the scheduler to the frame which called 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

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"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	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search

04 APRIL 1997

Date of mailing of the international search report

2 9 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
BERNARR EARL GREGORY

Telephone No. (703) 306-4153

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

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)

(21) International Application Number: PCT/US97/00652

(22) International Filing Date: 17 January 1997 (17.01.97)

(30) Priority Data:
08/587,944 17 January 1996 (17.01.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(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).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(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).

Published
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.

(54) Title: METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

(57) Abstract

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.

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	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

FIELD OF INVENTION

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 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 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 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 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.

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 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 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 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 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 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 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

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 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 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 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. "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 "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 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 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 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 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 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 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 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 "erase" 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.

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 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 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 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 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 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 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.

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 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 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 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 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 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 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.

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 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" 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 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 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 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 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 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 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 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, "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 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 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 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;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver 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 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 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.

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 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 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 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 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, 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 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 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 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. A method for using a computer to generate a random or pseudo random key for a digital watermark system wherein said random key includes:

a random or pseudo random sequence of binary 1s and 0s

information describing the application of the random sequence to a stream of digitized samples wherein said information includes:

at least one list of time delimiters describing segments of the stream;

at least one list of frequency delimiters describing frequency bands to be included in watermark computations; and

a signal encoding level;

wherein the method comprises the step of receiving human interactive input information used to describe limits on where, at what level, and at what frequencies the random binary information of the random key is to be applied to the stream of digitized samples in encoding the digital watermark;

wherein said human interactive input information comprises at least one of the following datum:

a list of time delimiters;

a list of frequency delimiters; and

a signal encoding level.

2. The method of claim 1 further comprising the step of selecting said stream of digitized samples from a list provided by a computer system.

3. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer

system, wherein said graphical representation includes a time axis and a signal frequency axis.

4. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer system, wherein said graphical representation includes a time axis and a signal amplitude axis.

5. The method of claim 3 or 4, further comprising the step of updating the graphical display to reflect receipt of new human interactive input information.

6. The method of claim 5 further comprising the step of generating a random or pseudo random sequence of 1s and 0s.

7. The method of claim 6 further comprising the step of storing input information in association with the random sequence of 1s and 0s as a single record in a database of such records.

8. The method of claim 7 wherein the record is encrypted using a pass phrase.

9. The method of claim 1 where the stream of digitized samples contains a digital audio recording.

10. The method of claim 1 where the stream of digitized samples to be watermarked contains a digital video recording.

11. The method of claim 6 wherein the process of generating the random sequence comprises the steps of:

(a) collecting a series of random bits derived from keyboard latency intervals in random typing;

(b) processing the initial series of random bits through a secure one-way hash function;

(c) using the results of one-way hash function to seed a block encryption cipher loop;

(d) cycling through the block encryption loop, and extracting the least significant bit of each result after cycle; and

(e) concatenating the block encryption output bits into the random key sequence

12. A method of encoding and decoding a digital watermark where the encoder and decoder are separate software applications or hardware devices.

13. The method of claim 12 wherein the decoder functionality is embedded in a software search engine, word-wide web-crawler file scanning engine, intelligent agent, or a virus.

14. The method of claim 12 wherein the decoder can access only a limited number of watermark channels, corresponding to public watermark keys, or any keys otherwise made available to said decoder.

15. The method of claim 12 wherein the decoder is capable of detecting the presence of a valid watermark but not of accessing the information in the watermark.

16. The method of claim 12 wherein the encoder places a separate signal, which does not interfere with the watermark, into a content stream, where said separate signal can indicate

watermark synchronization information, which helps locate watermarks in the content; and

the presence of a valid watermark in the content.

17. A method of using digital watermarks to convey information which is to be used for a content metering service, wherein said watermarks contain at least one of the following pieces of information:

title identification;

unit measure;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver indicating percent of content received.

18. A method of encoding digital watermarks which contain information pertaining to distribution restrictions and a location of an addressable directory containing related content, where said watermarks contain at least one of the following pieces of information:

geographical constraints on distribution (state, country, etc);

logical constraints on distribution;

Universal Resource Locator (URL);

telephone number;

Internet Protocol address;

Internet domain name;

email address; and

file name.

19. A method of encoding multiple digital watermarks into a single content stream wherein each watermark is encoded with a separate key.

20. The method of claim 18 wherein watermark information from each watermark is interleaved in the time domain.

21. A method of claim 18 wherein watermark information from each watermark is placed into specific frequency bands, or interleaved in the frequency domain.

22. A method of associating with a pseudo-random key, a list of component function references, which dictate what component functions are applied to the encoding and decoding of a digital watermark using the key in question.

23. A method of providing synchronization of a decoder to watermark which consists of the following steps:

a) recording a feature of sample stream, or a marker extracted from the sample stream immediately preceding the start of an encoded watermark;

b) recording the order in which a list of markers was encountered in the sample stream;

c) storing a list of such markers and the order of their appearance in a file for use by the decoder;

d) optionally, associating the stored information of step c) with a watermark key or watermark receipt or content title;

e) in the decoder, selecting a marker from the file in step c) such that the selected marker is not previous in order to any other marker previously selected in decoding the sample stream in question;

f) attempting to find a feature or marker in the portion of the sample stream currently under processing;

g) at such time as the currently selected marker is deemed unlikely to be found, discarding it and proceeding to step e);

h) at such time as marker is found, decoding the watermark, then proceeding to step e) unless the sample stream is exhausted.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/20
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. : 380/20, 54

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, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"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
"E"	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)		
"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	"&"	document member of the same patent family

Date of the actual completion of the international search 06 MAY 1997	Date of mailing of the international search report 09 JUN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer SALVATORE CANGIALOSI
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1837

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

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.

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)

(51) International Patent Classification ^{6} : **G09C 5/00, H04L 9/00**	**A1**	**(11) International Publication Number:** **WO 98/02864** **(43) International Publication Date:** 22 January 1998 (22.01.98)

(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, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US). COOPERMAN, 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).

(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
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.

(54) Title: OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

(57) Abstract

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.

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

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 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, 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, "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.

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 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.

The present invention additionally 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.

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 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 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 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 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 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 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 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 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.

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, 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.

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 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 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 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 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).

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.

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.

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 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 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 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 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 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 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 copending 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 $1x10^{-42}$ 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 perceivably 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.

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.

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 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, 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 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 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 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.

The present invention also relates to copending patent applications entitled "Staganographicc 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 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 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 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 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" 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 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.

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 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 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 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 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 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; 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 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, 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 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.

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 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 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 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 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:

$$E_{rms}=Q/(12)^{\frac{1}{2}}$$

Signal to quantization error is expressed as:

$$S/E=[S_{rms}/E_{rms}]^2=3/2(2^{2n})$$

Finally, in decibels (dB) and comparing 16-bit and 15-bit quantization:

$$S/E(dB)=10\log[3/2(2^{2n})]=10\log 3/2+2^n\log 2$$

$$(\text{or } "=20\log[(3/2)^{\frac{1}{2}}(2^n)]")$$

$$=6.02n+1.76$$

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. 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 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 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 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, 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 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 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 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 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 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 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 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 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 digitization systems, such as 2. Remainders given odd or even results (parity) that are probablistically 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 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.
- 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 CRCC design and the remainder of the error correction system.

Error correction techniques can be broken into three categories: methods for algebraic block codes, probablistic 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 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 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 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 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 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.

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 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.

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 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 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 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 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.

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 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."

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:

- Assume the composite signal contains a watermark from the sample.
- Assume the provision of the suspect composite signal $C_w(t)$ (w subscript denotes a possible watermark) and the unwatermarked original sample $S_{uw}(t)$. These are the only two recordings the analyzer is likely to have access to.

Now, it is necessary to recover a watermarked sample $S_w(t)$.

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 $S_{uw}(t)$, since watermarking makes relatively minor changes to a signal.

So, $C''_w(t)$ (an estimate of $C'_w(t)$ given $C_w(t)$ and $S_{uw}(t)$) may be obtained. 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 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 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 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 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 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 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 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 in the analysis of a single random noise signal inserted over the entire content signal as proposed by Digimarc, NEC, Thorn 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 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 currently used in copyright infringement cases pursued in the courts.

What Is Claimed Is:

1. A method for amplitude independent encoding of digital watermark information in a signal, comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide normalized samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels;

analyzing the normalized samples to determine quantization levels;

comparing the message bits to the corresponding quantization level information from the analyzing step;

when a bit conflicts with the quantization level, adjusting the quantization level of said sample window to correspond to the message bit; and

de-normalizing the analyzed normalized samples.

2. The method according to claim 1, wherein watermark signal characteristics or a watermark certificate can be compressed.

3. A method for amplitude independent decoding of digital watermark information in a signal comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels; and

analyzing the quantization level of said samples to determine a message bit value.

4. The method according to claim 3, wherein watermark signal characteristics or a watermark certificate can be compressed.

5. A method of encoding and decoding watermarks in a signal, comprising insertion and detection of abstract signal features in said signal to carry watermark information, wherein said abstract signal features are mathematical functions of the input sample window, and by extension, adjacent sample windows.

6. A method of pre-analyzing a digital signal for encoding digital watermarks using a digital filter comprising determining what changes in the digital signal will be affected by the digital filter.

7. The method according to claim 6, further comprising a step of encoding watermarks so as to either avoid frequency or time delimited areas of the signal which will be changed by the digital filter, or ensure that the watermark will survive the changes instroduced by the digital filter.

8. A method of error coding watermark message certificates using cross interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to n, wherein is a number of bits in a message block.

9. A method of pre-processing a watermark message certificate comprising determining an exact length of the watermark message as it will be encoded.

10. The method according to claim 9, further comprising a step of generating a watermark key which will provide at least one unique bit for each bit comprising the watermark message.

11. A method of generating watermark pseudo-random key bits using a non-linear generator.

12. A method of generating watermark pseudo-random key bits using a chaotic generator.

13. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a non-linear generator.

14. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a chaotic generator.

15. A method of guaranteeing watermark certificate uniqueness comprising attaching a timestamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

16. A method of generating and modulating a local noise signal to contain watermark information, wherein the noise signal is a function of at least one variable which depends on key and processing state information.

17. A method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

18. A method of encoding watermarks comprising steps of:

inverting at least one instance of the watermark bit stream; and

encoding at least one instance of the watermark using said inverted instance of the watermark bit stream.

19. A method of decoding watermarks comprising steps of:

considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks; and

decoding based on the considering step.

20. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over frequency.

21. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over time.

22. The method of claim 21, wherein the information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random, over both frequency and time.

23. A method of analyzing composite digitized signals for watermarks comprising steps of:

obtaining a composite 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 a corresponding segment of the composite signal, determined in the time aligning step;

estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal;

estimating a watermarked sample signal by subtracting the estimated pre-composite signal from the composite signal; and

scanning the estimated watermarked sample signal for watermarks.

24. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising 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 a 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).

25. The method according to claim 24, wherein watermark signal characteristics or a watermark certificate can be compressed.

26. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising steps of:

a) assigning a list of desired CODECs to a list of index values which correspond 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).

27. The method according to claim 26, wherein watermark signal characteristics or a watermark certificate can be compressed.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/11455

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G09C 5/00 H04L 9/00
US 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

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"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	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 23 OCTOBER 1997	Date of mailing of the international search report 23 DEC 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer DAVID CAIN
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1836

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

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04N 1/32

A1

(11) International Publication Number: WO 99/52271

(43) International Publication Date: 14 October 1999 (14.10.99)

(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]; 16711 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., Washington, DC 20004 (US).

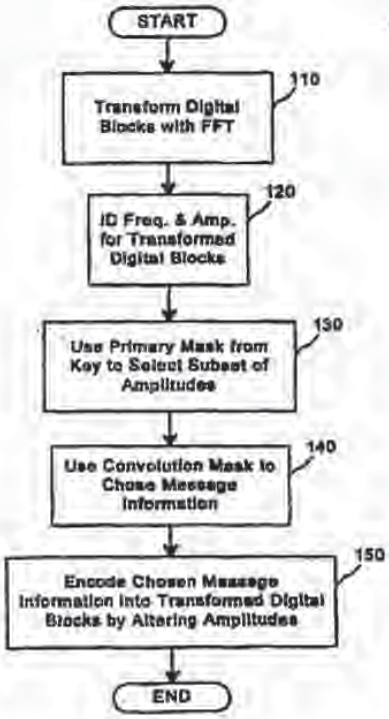
(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(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.


START
Transform Digital Blocks with FFT
110
ID Freq. & Amp. for Transformed Digital Blocks
120
Use Primary Mask from Key to Select Subset of Amplitudes
130
Use Convolution Mask to Chose Message Information
140
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
150
END

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			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

BACKGROUND

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

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

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.

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, 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 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 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 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 desirable. Note that digital watermarks are a tool in this process, but they no 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 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 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 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 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 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 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 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 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 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 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 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 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 "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 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, 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.

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 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 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 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 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 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.

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

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 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 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 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.

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.

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.

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 "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 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 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 descaling 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 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 replaced by zeroes.

Once the in formation 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 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 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 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;

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;

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.

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 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:

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:

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 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 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

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 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 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;

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

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:

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:

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

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 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.

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.

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.

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:

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; 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:

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 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;

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

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:

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;

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.

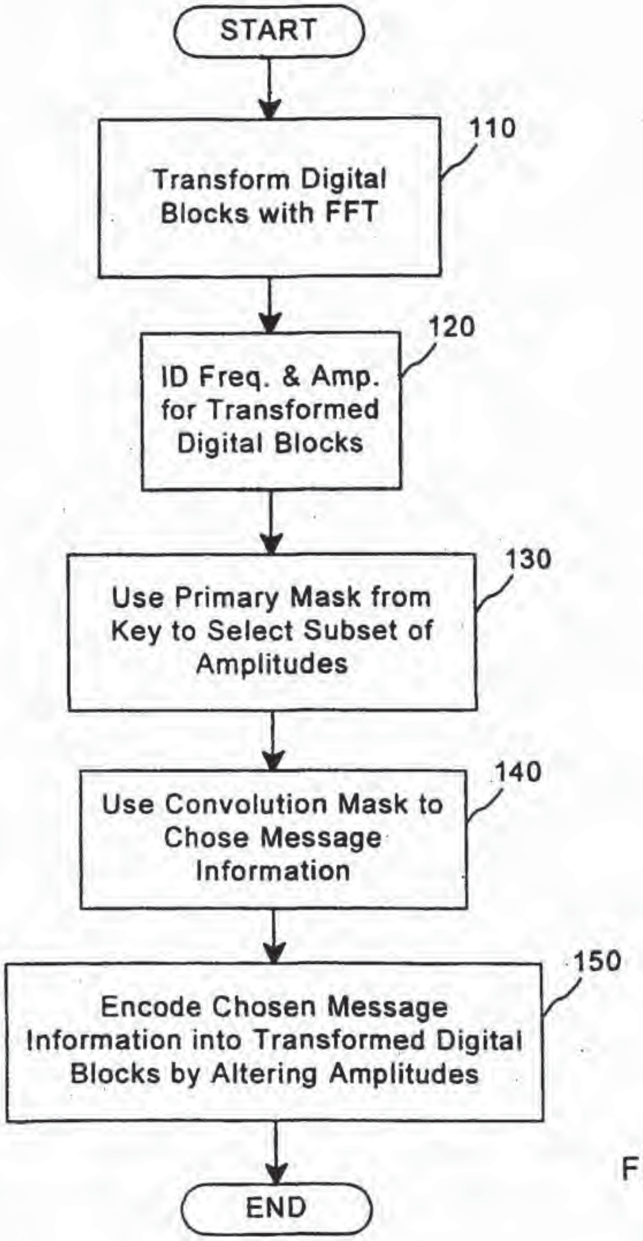

START
110
Transform Digital Blocks with FFT
120
ID Freq. & Amp. for Transformed Digital Blocks
130
Use Primary Mask from Key to Select Subset of Amplitudes
140
Use Convolution Mask to Chose Message Information
150
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
END

FIG. 1

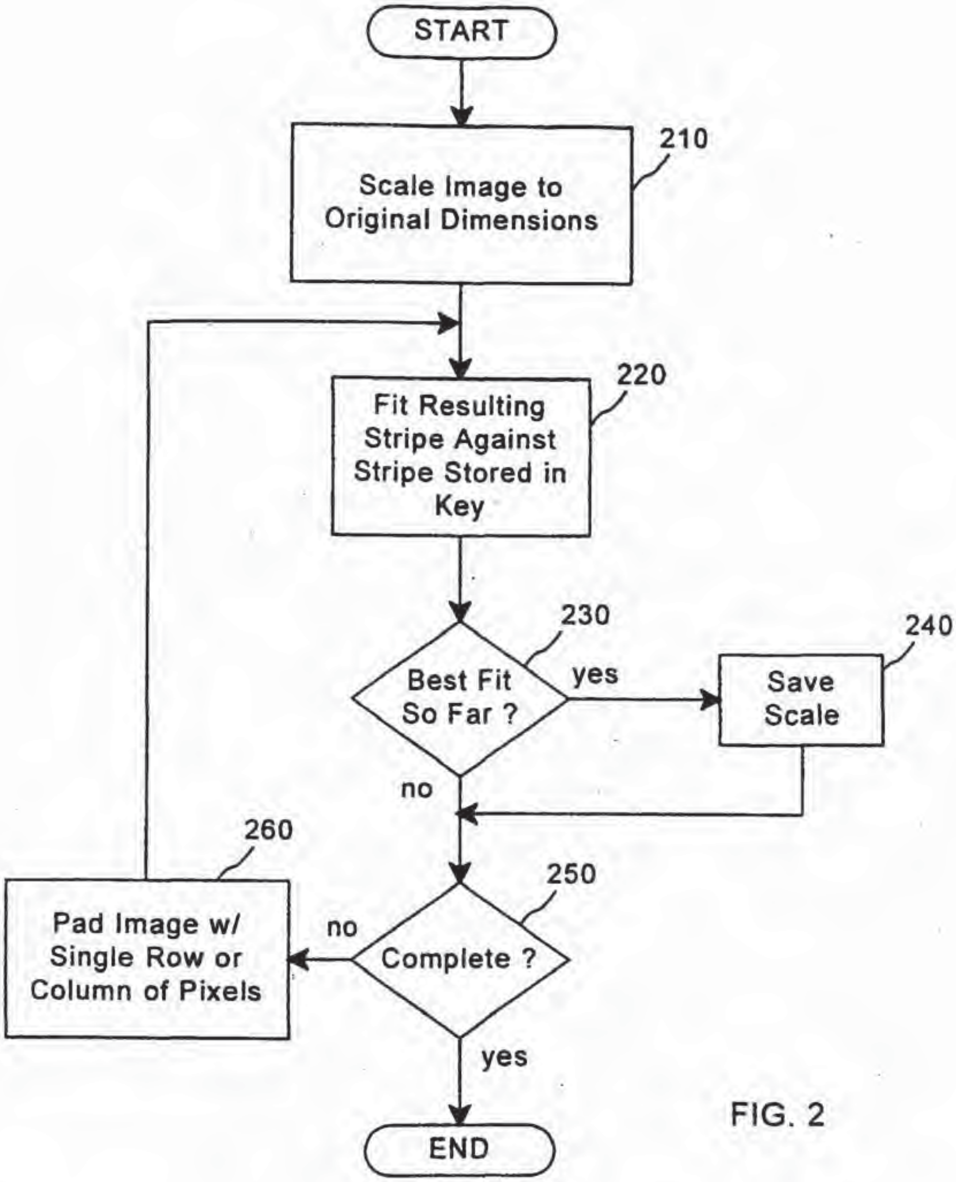

START
210
Scale Image to Original Dimensions
220
Fit Resulting Stripe Against Stripe Stored in Key
230
Best Fit So Far ?
yes
240
Save Scale
no
260
250
Pad Image w/ Single Row or Column of Pixels
no
Complete ?
yes
END

FIG. 2

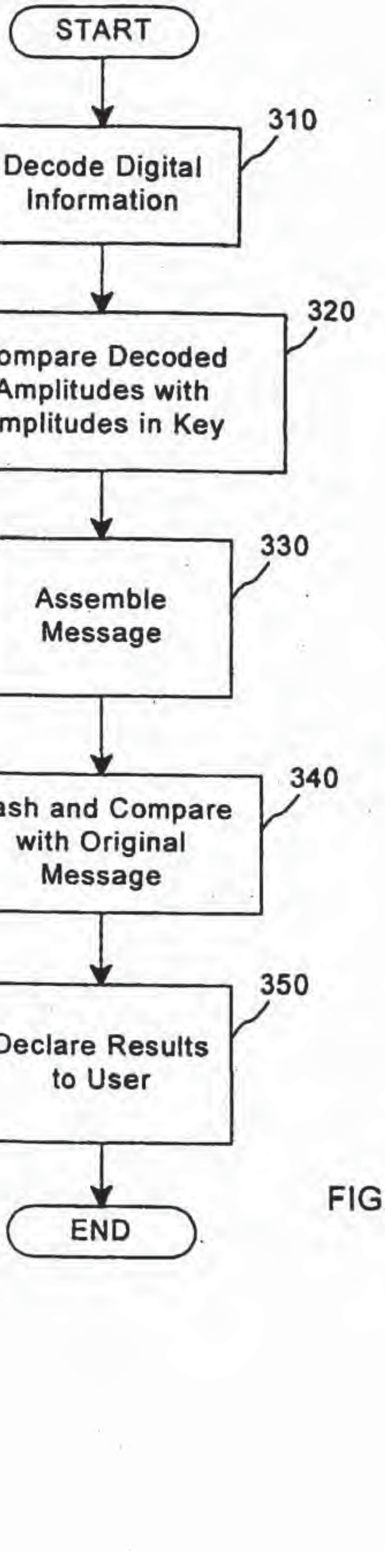

START
310
Decode Digital Information
320
Compare Decoded Amplitudes with Amplitudes in Key
330
Assemble Message
340
Hash and Compare with Original Message
350
Declare Results to User
END

FIG. 3

INTERNATIONAL SEARCH REPORT

Inte rnal Application No
PCT/US 99/07262

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32

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 6 H04N H04L

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.
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

☒ Further documents are listed in the continuation of box C.

☒ 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 doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

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

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

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

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 July 1999	Date of mailing of the international search report 21/07/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Hubeau, R

2

INTERNATIONAL SEARCH REPORT

Inte onal 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 ENGINEERSISBN: 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

2

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Inte   onal 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 WO 9642151 A US 5687236 A	21-10-1998 27-12-1996 11-11-1997

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２０６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　忠弐

【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み、

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向ハッシュ関数を

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知し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向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ＤＥ.Ｓ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る。「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、質に関する寛容度は、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ということにはならない。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見なすことになる。

【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０８／７７５，２１６号；"Human Assisted Random Key Generation and Application for Digital Watermark System"と題する米国特許出願第０８／５８７，９４４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。同様にして、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実にするために、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はなく、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

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、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、アービトロン（Arbitron）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（Giovannni）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か、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際的である。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、透かしを曖昧にして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うるデータの量を、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」（ペイロードさせる）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ペ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「ペイロード」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マ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、安全な一方向ハッシュ関数や、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っ

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１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」透かしを阿ｓくせいす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、ターゲット挿入封筒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することは必要でない。更に、すべてのビットを符号化することは、符号化方式を知りながら領域を複製することができるものにとっては、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ことがない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）と組み合わされて、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、デスクランブリング（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３２Ｘ３２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、画像を通って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／又はスケーリングがなされているかどうかがチェックされる。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／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、園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ケ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。

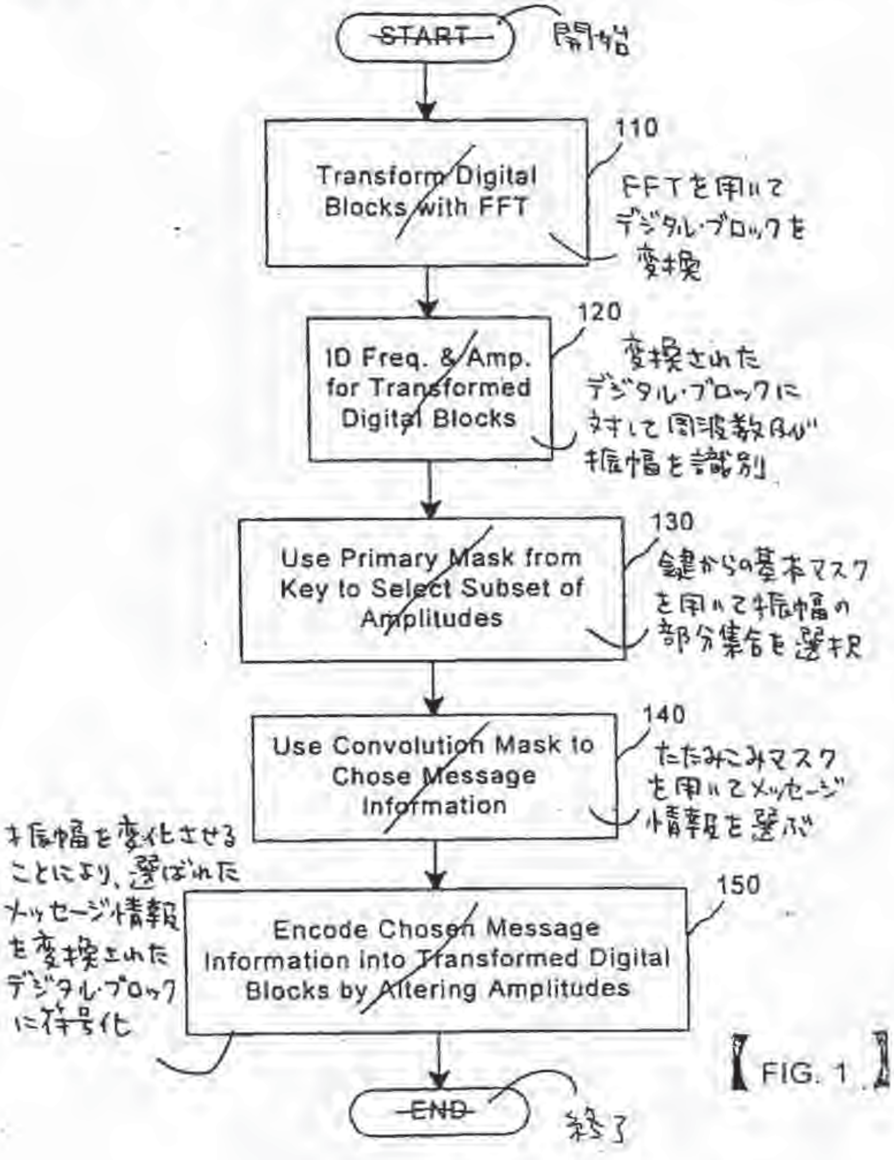
【図２】

本発明の或る実施例によるデジタル情報のデスケーリング方法のブロック流れ図である。

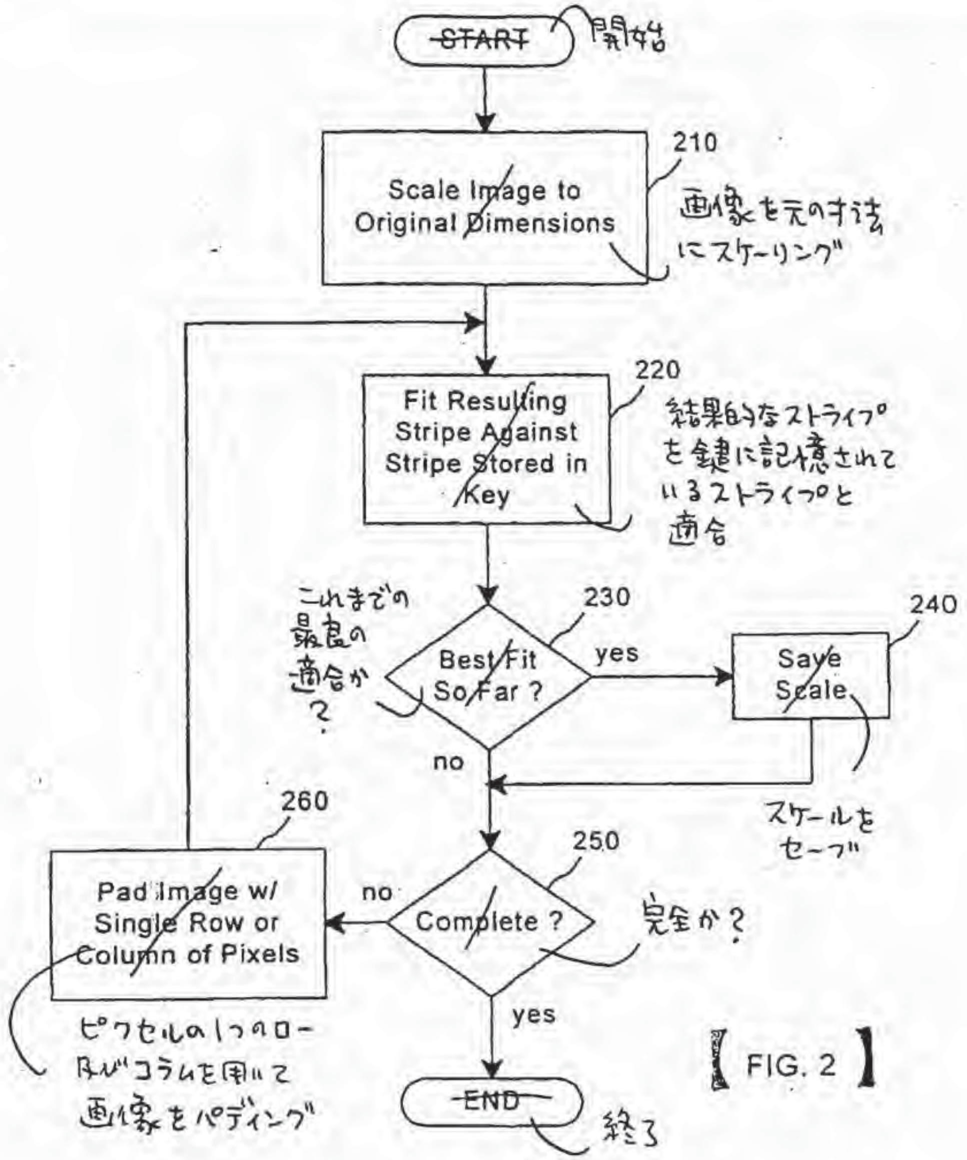
【図３】

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。

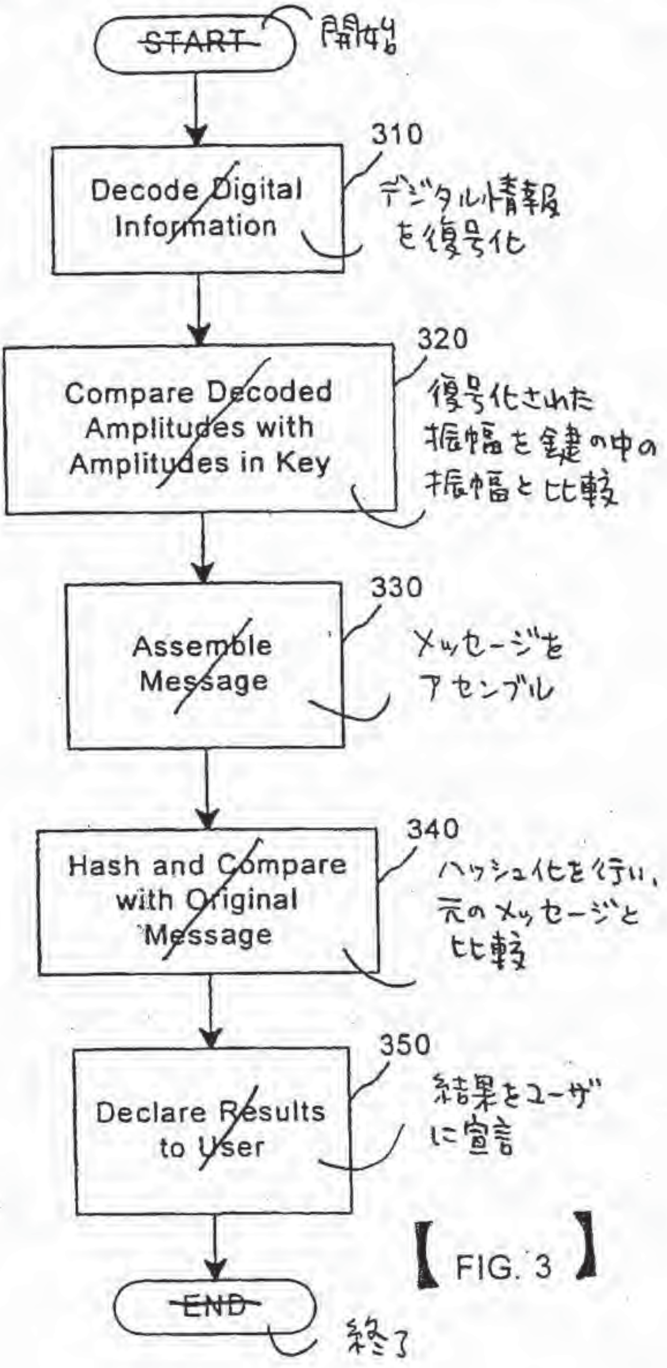
【書類名】　図面


~~START~~
開始
110
Transform Digital Blocks with FFT
FFTを用いてデジタル・ブロックを変換
120
ID Freq. & Amp. for Transformed Digital Blocks
変換されたデジタル・ブロックに対して周波数及び振幅を識別
130
Use Primary Mask from Key to Select Subset of Amplitudes
鍵からの基本マスクを用いて振幅の部分集合を選択
140
Use Convolution Mask to Chose Message Information
たたみこみマスクを用いてメッセージ情報を選ぶ
150
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
振幅を変化させることにより、選ばれたメッセージ情報を変換されたデジタル・ブロックに符号化
~~END~~
終了

【FIG. 1】


START
開始
210
Scale Image to Original Dimensions
画像を元の寸法にスケーリング
220
Fit Resulting Stripe Against Stripe Stored in Key
結果的なストライプを鍵に記憶されているストライプと適合
230
Best Fit So Far ?
これまでの最良の適合か？
yes
no
240
Save Scale
スケールをセーブ
250
Complete ?
完全か？
no
yes
260
Pad Image w/ Single Row or Column of Pixels
ピクセルの１つのロー及びコラムを用いて画像をパディング
END
終了

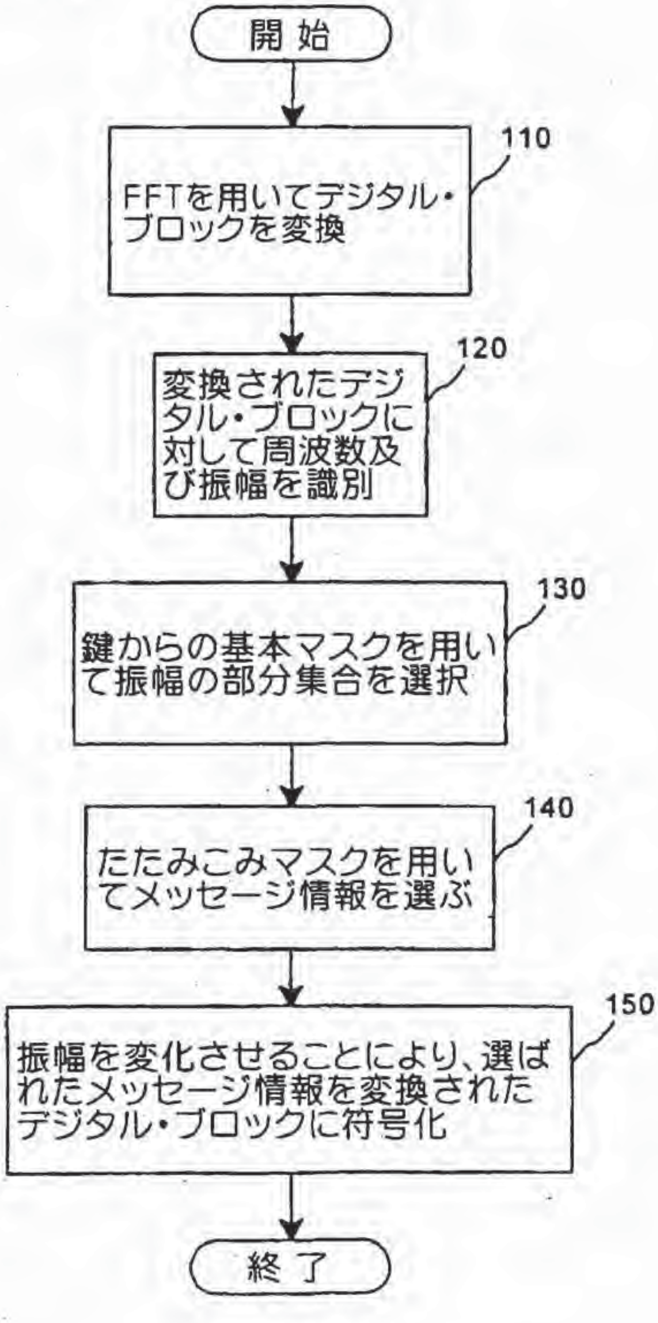
【 FIG. 2 】


~~START~~
開始
310
Decode Digital Information
デジタル情報を復号化
320
Compare Decoded Amplitudes with Amplitudes in Key
復号化された振幅を鍵の中の振幅と比較
330
Assemble Message
メッセージをアセンブル
340
Hash and Compare with Original Message
ハッシュ化を行い、元のメッセージと比較
350
Declare Results to User
結果をユーザに宣言
~~END~~
終了

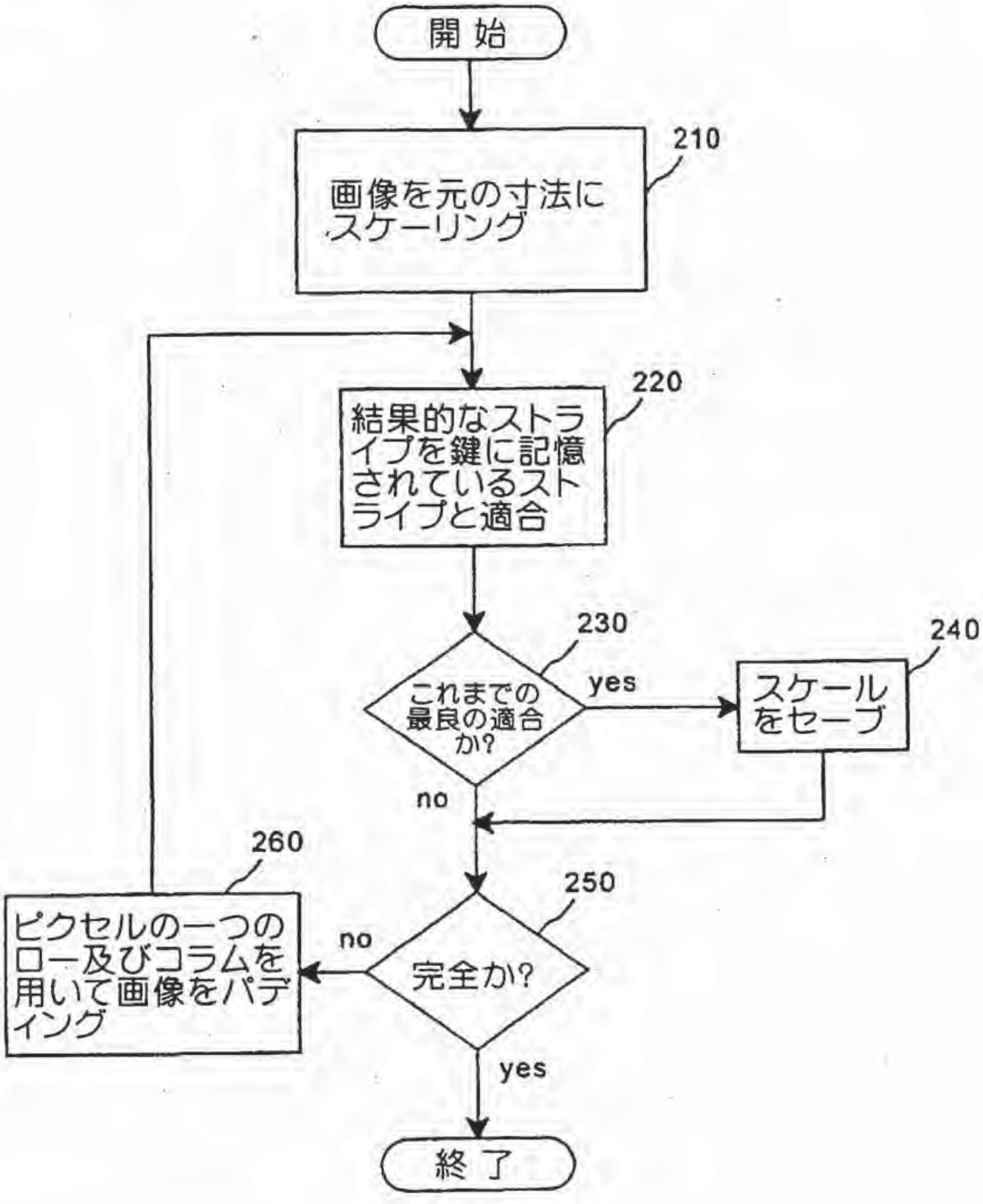
【FIG. 3】

【書類名】　図面

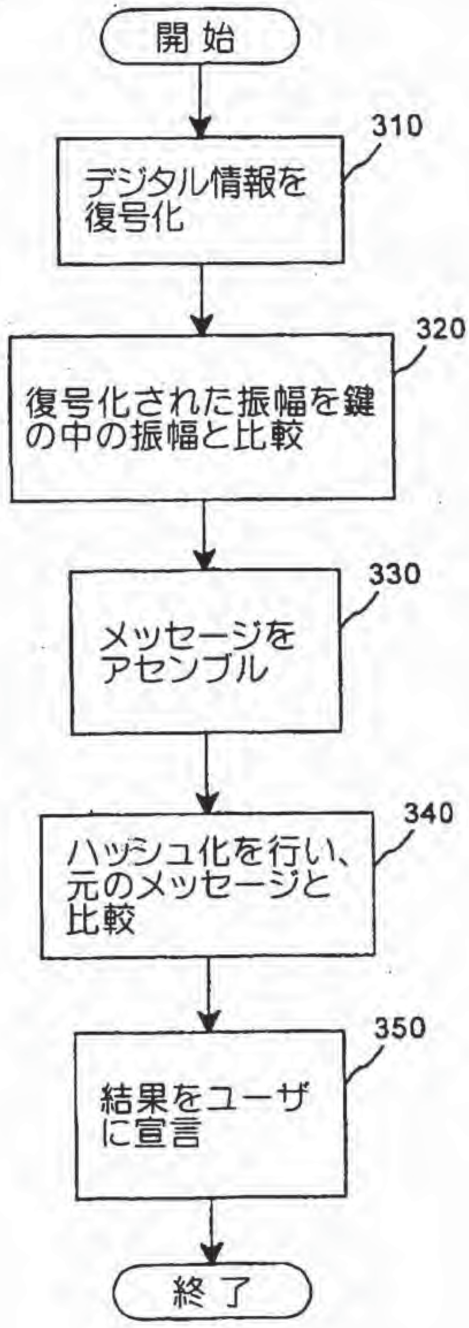
【図１】


開 始
110
FFTを用いてデジタル・ブロックを変換
120
変換されたデジタル・ブロックに対して周波数及び振幅を識別
130
鍵からの基本マスクを用いて振幅の部分集合を選択
140
たたみこみマスクを用いてメッセージ情報を選ぶ
150
振幅を変化させることにより、選ばれたメッセージ情報を変換されたデジタル・ブロックに符号化
終 了

【図２】


開始
210
画像を元の寸法にスケーリング
220
結果的なストライプを鍵に記憶されているストライプと適合
230
これまでの最良の適合か?
yes
240
スケールをセーブ
no
250
完全か?
no
260
ピクセルの一つのロー及びコラムを用いて画像をパディング
yes
終了

【図３】


開始
310
デジタル情報を復号化
320
復号化された振幅を鍵の中の振幅と比較
330
メッセージをアセンブル
340
ハッシュ化を行い、元のメッセージと比較
350
結果をユーザに宣言
終了

【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。

Your Ref.: 066358.0102JP
(Our Ref.: EL:TOT:MOH, S-1181-1/002365)

Amendment

【書類名】　手続補正書

Filed: October 13, 2000

【整理番号】　0023651

【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２０６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。

【プルーフの要否】　要

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04N 7/167

A1

(11) International Publication Number: WO 00/57643

(43) International Publication Date: 28 September 2000 (28.09.00)

(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).

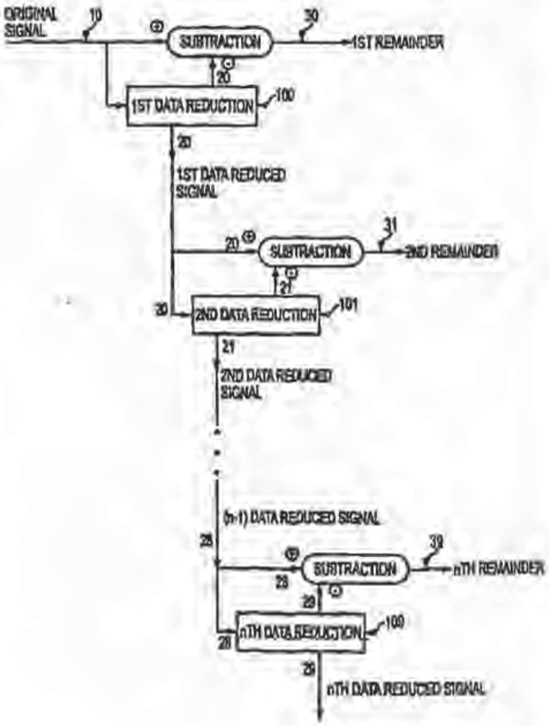
(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(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 redued 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	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

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 nth data reduction technique 109 to generate an nth data reduced signal 29. The nth data reduced signal 29 is then subtracted from the (n-1) data reduced signal 28 to produce an nth 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 nth data signal may optionally subjected to a watermarking technique, or even optionally subjected to a 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 nth 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 watermarkings.

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 "covertext" being transmitted.

Layering through data reduction offers many advantages to those who seek privacy and copyright protection. Serialization 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 produced 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 produced 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.