7715068

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 19, 2019

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

APPLICATION NUMBER: ***60/213,489***
FILING DATE: ***June 23, 2000***

Certified by

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

Please type a plus sign (+) inside this box → +

Docket Number:	066112.0138

JC714 U.S. PTO 06/23/00

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Small Entity)

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

JC625 U.S. PTO 60/213489 06/23/00

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Scott A. Michael	MOSKOWITZ BERRY	Miami, Florida USA Albuquerque, New Mexico USA

☐ *Additional inventors are being named on page 2 attached hereto*

TITLE OF THE INVENTION (280 characters max)

SECURE PERSONAL CONTENT SERVER

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ Customer Number 24735 →

24735
PATENT_TRADEMARK OFFICE

OR

☐ Firm or Individual Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒	Specification	*Number of Pages*	49	☐	Small Entity Statement
☒	Drawing(s)	*Number of Sheets*	7	☐	Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

		FILING FEE AMOUNT ($)
☐	A check or money order is enclosed to cover the filing fees	
☐	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:	$75.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE Floyd B Chapman Date June 23, 2000

TYPED or PRINTED NAME Floyd B. Chapman REGISTRATION NO. *(if appropriate)* 40,555

TELEPHONE 202/639/7700

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

19SMALL/REV04

DISH-Blue Spike-246
Exhibit 1012, Page 0002

Inventors: Scott Moskowitz & Michael Berry

A Secure Personal Content Server

Field of Invention

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

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

Cross-Reference To Related Application

This application is based on and claims the benefit of pending U.S. Patent Application Serial No. 60/147,134, filed 08/04/99, entitled, "A Secure Personal Content Server." MUST FOLLOW THIS SENTENCE WITH ONE OF THE TWO PARAGRAPHS BELOW

This application also claims the benefit of the following applications: pending U.S. Patent Application Serial No. 09/046,627, filed 3/24/98, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed 04/02/98, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No. 60/169,274, filed 12/7/99, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems"; and U.S. Patent Application Serial No._____ , filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (which is a continuation-in-part of PCT application No. PCT/US00/06522, filed 14 March 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed 24 March 1999) All of the patent applications previously identified in this paragraph are hereby incorporated by reference, in their entireties.

This application also claims the benefit of pending pending U.S. Patent Application Serial No. 08/999,766, filed 7/23/97, entitled "Steganographic Method and Device"; pending U.S. Patent Application Serial No. 08/772,222, filed 12/20/96, entitled "Z-Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 09/456,319, filed 12/08/99, entitled

DISH-Blue Spike-246
Exhibit 1012, Page 0003

"Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 08/674,726, filed 7/2/96, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management"; pending U.S. Patent Application Serial No. 09/545,589, filed 04/07/2000, entitled "Method and System for Digital Watermarking"; pending U.S. Patent Application Serial No. 09/046,627, filed 3/24/98, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed 04/02/98, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No. 09/281,279, filed 3/30/99, entitled "Optimization Methods for the Insertion, Protection, and Detection..."; U.S. Patent Application Serial No._____ , filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (which is a continuation-in-part of PCT application No. PCT/US00/06522, filed 14 March 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed 24 March 1999); and pending U.S. Application No 60/169,274, filed 12/7/99, entitled "Systems, Methods And Devices For Trusted Transactions." All of the patent applications previously identified in this paragraph are hereby incorporated by reference, in their entireties.

09545589 "09/22/2000

Summary of the Invention

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

In another approach that is related to this goal, there are instances where transactions must be allowed to happen after perceptually-based digital information can be authenticated. (Perceptually based information is information whose value is in large part, based upon its ability to be perceived by a human, and includes for example, acoustic, psychoacoustic, visual and psychovisual information.) The process of authenticating before distributing will become increasingly important for areas where the distributed material is related

DISH-Blue Spike-246
Exhibit 1012, Page 0004

to a trust-requiring transaction event. A number of examples exist. These include virtual retailers (for example, an on-line music store selling CDs and electronic versions of songs); service providers (for example, an on-line bank or broker who performs transactions on behalf of a consumer); and transaction providers (for example, wholesalers or auction houses). These parties have different authentication interests and requirements. By using the teachings of this application, these interests and requirements may be separated and then independently quantified by market participants in shorter periods of time.

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

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

DISH-Blue Spike-246
Exhibit 1012, Page 0005

arrangements over an electronic network, profitable market-based relationships can result.

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

With an increasingly anonymous marketplace, the present invention offers invaluable embodiments to accomplish "trusted" transactions in a more flexible, transparent manner while enabling market participants to negotiate terms and conditions. Negotiation may be driven by predetermined usage rules or parameters, especially as the information economy offers potentially many competitive marketplaces in which to transact, trade or exchange among businesses and consumers. As information grows exponentially, flexibility becomes an advantage to market participants, in that they need to screen, filter and verify information before making a transaction decision. Moreover, the accuracy and speed at which decisions can be made reliably enables confidence to grow with an aggregate of "trusted transactions". "Trusted transactions" beget further "trusted transactions" through experience. The present invention also provides for improvements over the prior art in the ability to utilize different independently important "modules" to enable a "trusted transaction" using competitive cryptographic and steganographic elements, as well as being able to support a wide variety of perceptually-based media and information formats. The envisioned system is not bound by a proprietary means of creating recognition for a good or service, such as that embodied in existing closed system. Instead, the flexibility of the present invention will enable a greater and more diverse information marketplace.

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

A related additional set of embodiments regards the further separation of the transaction and the consumer's identification versus the identification of the transaction only. This is accomplished through separated "trusted transactions" bound by authentication, verification and authorization in a transparent manner. With these embodiments, consumer and vendor privacy could be incorporated.

DISH-Blue Spike-246
Exhibit 1012, Page 0006

More sophisticated relationships are anticipated between parties, who can mix information about their physical goods and services with a transparent means for consumers, who may not be known to the seller, who choose not to confide in an inherently closed "trusted system" or provide additional personal information or purchasing information (in the form of a credit card or other electronic payment system), in advance of an actual purchase decision or ability to observe (audibly or visibly) the content in the clear. This dynamic is inconsistent with the prior art's emphasis on access control, not transparent access to value-added information (in the form or goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

These embodiments may include decisions about availability of a particular good or service through electronic means, such as the Internet, or means that can be modularized to conduct a transaction based on interconnection of various users (such as WebTV, a Nintendo or Sony game console with network abilities, cellular phone, PalmPilot, etc.). These embodiments may additionally be implemented in traditional auction types (including Dutch auctions). Consumers may view their anonymous marketplace transactions very differently because of a lack of physical human interactions, but the present invention can enable realistic transactions to occur by maintaining open access and offering strict authentication and verification of the information being traded. This has the effect of allowing legacy relationships, legacy information, and legacy business models to be offered in a manner which more closely reflects many observable transactions in the physical world. The tremendous benefits to sellers and consumers is obvious; existing transactions need not reduce their expectations of security. As well, the ability to isolate and quantify aspects of a transaction by module potentially allows for better price determinations of intangible asset insurance, transaction costs, advertising costs, liability, etc. which have physical world precedent.

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

A goal for providers of value-added content is to maximize profits for the sale of their content. Marketing and promotion of the informational content cannot be eliminated, considering the ever increasing amount of information vying for consumers and other market participant's attention. Nonetheless, in a market where the goods are speculatively valued, marketing budgets are inherently constrained, as you are trying to create demand for a product with little inherent value. Where such markets have participants, both buyers and sellers and their respective agents, with access to the same information in real

DISH-Blue Spike-246
Exhibit 1012, Page 0007

time, market mechanisms efficiently price the market goods or services. These markets are characterized by "price commoditization" so buyers and sellers are limited to differentiating their offerings by selection and service. If the markets are about information itself, it has proven more difficult to accurately forecast the target price where sellers can maximize their profits. Quality and quantity provide different evaluation criteria of selection and service relating to the information being traded. The present invention regards a particular set of implementations of value-added content security in markets which may include unsecure and secure versions of the same value-added data (such as songs, video, research, pictures, electronic logos, electronic trademarks, value-added information, etc.).

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

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

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

DISH-Blue Spike-246
Exhibit 1012, Page 0008

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

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

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

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

DISH-Blue Spike-246
Exhibit 1012, Page 0009

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

Definitions:

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

Secure Electronic Content Distributor (SECD): An entity, device or software application which can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. In cryptographic terms, the SECD acts as a "certification authority" or its equivalent. SECDs may have differing arrangements with consumers and providers of value-added information.

Satellite Unit (SU): A portable medium or device which can accept secure digital content from a LCS through a physical, local connection and which can either play or make playable the digital content. The SU may have other functionality as it relates to manipulating the content, such as recording. The SU has a unique ID.

LCS Domain: A secure medium or area where digital content can be stored, with an accompanying rule system for transfer of digital content in and out of the LCS Domain.

SecureChannel™: A secure channel to pass individualized content to differentiate authentic content from legacy or unauthorized, pirated content. SecureChannel may carry a value-adding component (VAC).

Standard Quality: A transfer path into the LCS Domain which maintains the digital content at a predetermined reference level or degrades the content if it is at a higher quality level. In an audio implementation, this might be defined as Red Book CD Quality (44100 Hz., 16 bits, 2 channels).

Low Quality: A transfer path into the LCS Domain which degrades the digital content to a sub-reference level. In an audio implementation, this might be defined as below CD Quality (for instance, 32000 Hz., 16 bits, 2 channels).

High Quality: A transfer path into the LCS Domain which allows digital content of any quality level to pass unaltered.

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

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

Unique ID: A Unique ID is created for a particular transaction and is unique to that transaction (roughly analogous to a human fingerprint). One way to generate a Unique ID is with a one-way hash function. Another way is by incorporating the hash result with a message into a signing algorithm will create a signature scheme. For example, the hash result may be concatenated

DISH-Blue Spike-246
Exhibit 1012, Page 0010

to the digitized, value added information which is the subject of a transaction. Additional uniqueness may be observed in a hardware device so as to differentiate that device, which may be used in a plurality of transactions, from other similar devices.

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

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

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

One way hash function: One-way hash functions are known in the art. The way in which the hash is generated is defined in such a way that does not depend on the characteristics of the input, though certainly the hash function can operates on in an input signal. The output is a hash value which is not secret, but it is computationally unfeasible to determine the pre-image that hashes to the hash value.

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

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

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the value-added or information rich data at the inherent granularity of the file format. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. **Scrambling is efficient for larger media files** and can be used to provide content in less than commercially viable or referenced quality levels. Scrambling is not

DISH-Blue Spike-246
Exhibit 1012, Page 0011

as secure as encryption for these applications, but provide more fitting manipulation of media rich content in the context of secured distribution. Scrambled data is also called "ciphertext" for the purposes of this invention. **Encryption generally acts on the data as a whole, whereas scrambling is applied often to a particular subset of the data concerned with the granularity of the data, for instance the file formatting. The result is that a smaller amount of data is "encoded" or "processed" versus strict encryption, where all of the data is "encoded" or "processed." By way of example, a cable TV signal can be scrambled by altering the signal which provides for horizontal and vertical tracking, which would alter only a subset of the data, but not all of the data—which is why the audio signal is often untouched. Encryption, however, would generally so alter the data that no recognizable signal would be perceptually appreciated. Further, the scrambled data can be compared with the unscrambled data to yield the scrambling key. The difference with encryption is that the ciphertext is not completely random, that is, the scrambled data is still perceptible albeit in a lessened quality. Unlike watermarking, which maps a change to the data set, scrambling is a transfer function which does not alter or modify the data set.**

09229494-e9e3c209

Detailed Discussion of Invention

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

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

When content leaves the LCS Domain, it is watermarked as belonging to that domain. It is allowed to leave at the quality level at which it was stored (i.e. the quality level determined by the validation path). The watermark on the exiting content is both an embedded digital watermark and an attached hash or digital signature (it may also include a secure time stamp). *Content cannot return into the domain unless both the watermark and hash can be verified as belonging to this domain.* The presence of one or the other is sufficient to allow re-entry.

This system is designed to allow a certifiable level of security for high-quality content while allowing a device to also be usable with unsecure content at a degraded quality level. The security measures are designed such that a removal of the watermark constitutes only a partial failure of the system. The

DISH-Blue Spike-246
Exhibit 1012, Page 0012

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

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

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

LCS Functions

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

The LCS may be able to receive content from a SECD, and must be able to authenticate content received via any of the plurality of implemented paths. The LCS must monitor and enforce any rules that accompany received content, such

DISH-Blue Spike-246
Exhibit 1012, Page 0013

as number of available copies. Finally, the LCS must watermark all exported material (with the exception of Path 6 - see below) and supply a hash made from the unique ID and the content characteristics (so as to be maintained perceptually within the information and increase the level of security of the watermark).

SU Functions

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

Sample Embodiments

Figure 1 is a diagram of sample LCS system, with possible paths for content to enter and leave the LCS. The diagram assumes that the LCS is a software device loaded on a general purpose computing device such as a PC. The PC has a hard drive (Rewritable media) and a CD-ROM drive (Read-Only media). The SECD is connected via the Internet. The SU is a portable player which connects to the computer using a serial interface or to other players where applicable (e.g. USB, IEEE 1394, etc...).

Generalize this more....**SCOTT SEEMS TO SUGGEST WE MAY NOT NEED THE ORIGINAL DIAGRAMS—I DON'T WANT TO LEAVE THEM OUT.**

Figure 2 is a diagram of a sample transaction module

Benefits of: bidirectionality and asymmetry in enabling a "trusted transaction"

Figure 3 is a diagram of a sample recognition module

Benefits of: bidirectionality and asymmetry in enabling a "trusted transaction"

Figure 4 is a diagram of a sample pricing module

Pricing of bandwidth patent reference...

Benefits of: bidirectionality and asymmetry in enabling a "trusted transaction"

Figure 5 is a diagram of a service and support module

Pricing of bandwidth patent reference...

265112

DISH-Blue Spike-246
Exhibit 1012, Page 0014

Benefits of: bidirectionality and asymmetry in enabling a "trusted transaction"

Path 1 depicts a secure distribution of digital content from a SECD to a LCS. The content can be secured during the transmission using one or more 'security protocols' (e.g. encryption or scrambling of the content). A single LCS may have the capability to receive content transmissions from multiple SECDs, and each SECD may use the same security protocols or different security protocols. It is also contemplated that the same SECD may periodically or randomly use different security protocols. A typical security protocol uses an asymmetric cryptographic system, an example being a public key cryptography system where private and public key pairs allow the LCS to authenticate and accept the received content. Another security protocol may involve the ability to authenticate the received content using a signature scheme. A typical transaction would have the following steps.

1.) Using an LCS, a user connects to a SECD.

2.) The user selects a group of data (e.g., a song), and purchases (or otherwise obtains the right to receive) a copy of the group of data. (The transmission of purchase information; for example, credit card information, may have entirely separate security as is known in the art of electronic commerce.)

3.) The SECD transmits the secured content to the LCS. Before transmitting any digital content, the SECD embeds at least one watermark and may also transmit (perhaps through cryptography) at least one hash output signal along with the data being transmitted. The at least one hash function output may be embedded with the at least one watermark or may be attached to the beginning or end of the data being transmitted. Alternately, the hash output may be combined in ways that are known to the art.

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

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

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

DISH-Blue Spike-246
Exhibit 1012, Page 0015

Path 2: In this path, content is imported into the LCS Domain from a rewritable medium (see Figure 2). The content is first checked to see if a LCS watermark is present. If there is no watermark, the content is degraded to Low Quality and allowed to enter the LCS domain. If a watermark is present, the hash is checked to verify that the content matches this LCS. If the hash matches the LCS, the content is allowed in at High Quality. If it does not match, the content is rejected.

Path 3: In this path, content is imported into the LCS Domain from a Read-Only medium (see Figure 3). The content is first checked to see if a LCS watermark is present. In there is no watermark, the content is degraded to Standard Quality and allowed to enter. If a watermark is present, the hash is checked to verify that the content matches this LCS. If it matches, the content is allowed in at High Quality. If it does not match, the content is rejected.

Read-Only media may also contain an media-based identifier which verifies that the content is an original, as opposed to a copy. If such an identifier exists and can be authenticated, the content is allowed in at High Quality.

Path 4: This path is the transfer from the SU to the LCS (see Figure 4). Content from an SU is marked with an SU watermark. This watermark may contain an LCS hash (see path 6 for further details). If it does, the LCS hash is checked. If it matches or if there is no LCS hash, the content is allowed to enter. If it does not match, the content is disallowed.

Path 5: This is an export path for the LCS to send content to any receiver other than a SU (see Figure 5). This might include copying to a rewritable media, creating a read-only media, or rendering the content for use (playing, viewing, etc.). Once the content is retrieved from storage the LCS adds a watermark to the content. This watermark is unique to this LCS, as determined by the LCS Unique ID. The watermark contains a hash (a signature) which is created from the combination of the content characteristics (such as signal features, etc.) and the Unique ID. The watermark may optionally contain other data, such as a timestamp, a number of allowable copies, etc. This would be described as parameters of use, usage data, etc. which could be referenced when content is exported. If the export is to a storage medium, the LCS optionally can add a second hash to the file, external to the content, which can be used for further authentication. For security purposes, the external hash should be created in a different manner from the embedded, watermark hash.

Path 6: This path is identical to Path 5 except that the receiver is a SU. This path requires a secure protocol to determine that the receiver is in fact a SU. Once the path is verified, the content can be exported without a watermark. The LCS also transmits a hash which the SU, permanently associated with the content.

DISH-Blue Spike-246
Exhibit 1012, Page 0016

Path 7: This path is for content that is recorded on a SU. All content is allowed to enter this path but it is always degraded to Low Quality.

Path 8: This path is for content that is rendered by the SU. This content is marked with a SU watermark which contains a hash from the SU Unique ID and any hash that is associated with the content from an LCS (refers to hash generated in path 6).

Sample Embodiment - SPCS Server Stage, an Audio Example

Fragile Watermark Structure

The fragile watermark can actually hold the entire SecureChannel™, encoded in the LSB of each 16 bit sample. This gives a data rate of 88200 bits per second in a stereo CD file, or a capacity of 1.89 M in a 3 minute song. This is an immense capacity relative to the expected size of the SecureChannel (100 - 200 K).

The fragile watermark needs to be bound to a specific copy of a specific song, so that it cannot be transferred to other songs. Additionally a fragile watermark may contain information which is specific to the receiver of the signal being packaged. For instance, information to optimize the performance of a song to be played on one particular machine versus other machines where differences, as can be logically constructed (file format, speed of transfer, additional information features, etc.), may be sought in buying or selling the "same" song. Perhaps a difference between say an MP3 encoded version of the song and an AAC encoded version of the song. This binding can be achieved through use of a hash in the following sequence:

1.) A block of SecureChannel is encoded into a block of samples.
2.) A hash of the SecureChannel block and a random number seeded by the owner's identity is generated and encoded into the subsequent block of samples.
3.) A hash of the first two blocks of samples and a random number seeded by the owner's identity is generated and encoded into a third block of samples.
4.) Repeat as necessary

Each SecureChannel block has the following structure:

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


DISH-Blue Spike-246
Exhibit 1012, Page 0017

}
An application can read the block identifier and determine if it recognizes the block type. If it doesn't, it can use the BlockLength to skip this block.

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

Robust Open Watermark (ROW)

This is the mark that indicates non-legacy content. There are two possible settings. 1 indicates non-legacy content that must be accompanied by an authenticatable SecureChannel for entry into the domain (e.g. electronic music distribution or EMD content). 0 indicates non-legacy media that was distributed in a pre-packaged form (e.g. CD's). 0 content may have a SecureChannel, or it may not. 0 content shall only be admitted from a read-only medium in its original file format (e.g. a 0 CD shall only be admitted if it is present on a Redbook CD medium).

Robust Forensic Watermark

This watermark is not accessible in any way to the consumer. It is secured by a symmetric key held only by the seller. A transaction ID is embedded at the time of purchase with a hash matching the symmetric key. The watermark is then embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of this watermark is not limited by real-time/low cost constraints. The recovery will only be attempted on pirated material. A recovery time of 2 hours on a 400 MHz PC is reasonable.

Sample Embodiment - Renewability

The scenario:

1) Have existing watermarked content, will also have unwatermarked legacy and unauthorized content.
2) Existing SPCS in the field
3) Hack occurs or upgrades for new algorithms are sought by content owners or their agents
4) Have a new embedding algorithm but SPCS's have yet to be upgraded
5) Want content to be recognizable by the old SPCS and the new SPCS

DISH-Blue Spike-246
Exhibit 1012, Page 0018

The system contemplates movement from an "Original watermark" to an "Upgrade watermark" and there is a transitional period. The watermark to be upgraded is a robust open watermark (ROW). A transitional period for which both original and upgrade watermarks are embedded into content—at mastering stage (SPCS is either upgraded or not upgraded), the determination is made by the content owner at the "mastering" point, prior to distribution.

Content owner knows that a hack has happened or seeks to simply upgrade the watermark ("pull the trigger" bit) and introduces upgrade watermarks in addition to the original watermarks. Movement to only upgrade watermark during transition: the content owner may want to be in both states depending on how pervasive the hack and how quickly content owner wants to upgrade.

For purposes of supporting both old and upgrade watermarks we can use predetermined "rules" for the embedding process: Statistical changes so that say if a detection window is 15 seconds for the original ROW, can upgrade every 30 seconds. Subsequent to this type of upgrade, each watermark for each 15 second window will alternatively represent an original and an upgrade watermark, respectively. Meaning timing or frequency can be used as a "modality" for where the upgrade ROW is to be introduced and allowing for co-existence with original watermarks. (i.e., old watermark has a detection window of 15 seconds, upgrade is 30 seconds, etc.). This approach anticipates multiple watermarks in a given sample stream.

Claims:

1.) A system for creating a secure local environment for digital content (LCS Domain) with the following characteristics:

a) The content is not accessible except through the approved functions of the Local Content Server (LCS).

b) The LCS has one or more paths to enable import of content, each of which has an associated set of rules governing import content quality.

c) The LCS has one or more paths to export content, where each path is secured.

d) The LCS has a unique identifier (Unique ID).

e) The LCS may interact with trusted Satellite Units (SU) which can store and/or render the content.

f) Any Satellite Units (SU) which can interact with the LCS have unique identifiers.

g) Any communication between the LCS and a SU must be on an authenticated, secure channel.

h) All export paths on SU's are secured.

2.) The system in claim 1 where the content is digital audio.

265112

3.) The system in claim 1 where the content is digital images.
4.) The system in claim 1 where the content is digital video.
5.) The system in claim 1 where the import path is from a secure provider of digital content and the transfer of the content can be authenticated such that:
a) the transfer is authorized by a trusted party,
b) the content is verified to be unchanged during the transfer,
c) the content is not usable if it is intercepted during the transfer, it is (encrypted or scrambled).
6.) The system in claim 1 where the import path is from a rewritable medium.
7.) The system in claim 6 where the content has no authenticatable watermark and the import occurs at a degraded content quality level.
8.) The system in claim 6 where the content has a authenticatable watermark which does not match the importing LCS and the import is disallowed.
9.) The system in claim 6 where the content has a authenticatable watermark which does match this LCS and the import is allowed at high content quality.
10.) The system in claim 1 where the import path is from a read-only medium.
11.) The system in claim 10 where the content has no authenticatable watermark and the import occurs at a standard content quality level.
12.) The system in claim 10 where the content has a authenticatable watermark which does not match the importing LCS and the import is disallowed.
13.) The system in claim 10 where the content has a authenticatable watermark which does match this LCS and the import is allowed at high content quality.
14.) The system in claim 10 where the content has no authenticatable watermark from an LCS but has a verifiable identifier indicating that the content is first generation and the import is allowed at high content quality.
15.) The system in claim 1 where the import is from a Satellite Unit through an authenticated, secure connection.
16.) The system in claim 15 where the SU watermark contains an identifier which matches the LCS and the import is allowed at high content quality.
17.) The system in claim 15 where the SU watermark contains an identifier which does not match the LCS and the import is disallowed.
18.) The system in claim 15 where the SU watermark contains an identifier which does not contain an LCS identifier and the import is allowed at high content quality.
19.) The system in claim 1 where the export path is to a rewritable medium. The content is marked using a watermark which contains a hash constructed from the LCS Unique ID and content characteristics.
20.) The system in claim 19 where a second hash generated by a different system is attached to the exported file outside of the content.
21.) The system in claim 1 where the export path is to a rendering device. The content is marked using a watermark which contains a hash constructed from the LCS Unique ID and content characteristics.

DISH-Blue Spike-246
Exhibit 1012, Page 0020

22.) The system in claim 1 where the export path is to a SU through an authenticated, secure connection. The LCS provides a hash to the SU, which the SU permanently associates with the content. The hash is constructed from the LCS Unique ID and content characteristics.
23.) The system in claim 22 where the SU uses the hash supplied by the LCS to generate a watermark on all exported content.
24.) The system in claim 23 where the SU adds its own hash to the watermark on all exported content. The hash is constructed from the SU Unique ID and content characteristics.
25.) The system in claim 1 where the LCS and SU do not use the same watermarking technique.

More claims: Public keys where any watermarking technique can be successfully deployed in the system.
26.) The system in claim 25 where the LCS can read watermarks written by any SU with which it can communicate.
27.) The system in claim 5 where the LCS can communicate with more than one secure provider, where each provider can use a different system of securing the transaction.
28.) The system in claim 5 where encryption is used in the transaction.
29.) The system in claim 5 where scrambling is used in the transaction.
30.) The system in claim 5 where public key cryptography is used in the transaction.

31) The method of transferring data as described in each of the Paths 1-8.

32) A method for creating a secure local environment for digital content (LCS Domain) with the following characteristics: a) The content is not accessible except through the approved functions of the Local Content Server (LCS); b) The LCS has one or more paths to enable import of content, each of which has an associated set of rules governing import content quality; c) The LCS has one or more paths to export content, where each path is secured; d) The LCS has a unique identifier (Unique ID); e) The LCS may interact with trusted Satellite Units (SU) which can store and/or render the content; f) Any Satellite Units (SU) which can interact with the LCS have unique identifiers; g) Any communication between the LCS and a SU must be on an authenticated, secure channel; and h) All export paths on SU's are secured.

DISH-Blue Spike-246
Exhibit 1012, Page 0021

33) A method for creating a secure local environment for digital content comprising transferring data as described in each of the Paths 1-8.

- A system for the transmission of data where the data is accessible through predetermined rules governed by the following conditions:

The data is available in a predefined location/environment with logical relationships to transmission paths

The data can be watermarked by at least one of a plurality of embedding protocols (dependent claims: including ROW, Fragile and Forensic watermarks)

The transmission paths are governed by predetermined rules for the import/export of the data dependent on cryptographic/steganographic verification

The location/environment has predefined rules governing the quality of the data

The data can be uniquely identified/authenticated when imported/exported/transmitted

- A system for the transmission of data where at least one of a plurality of a robust open watermark, a fragile watermark and a robust forensic watermark are embedded according to following steps:

A robust watermark is first embedded so as to enable an id/authentication check by an LCS; ("the screen" which is for quick checks and renewability)

Upon (subsequent) successful id/authentication the system then embeds a forensic watermark which is unique to the export of the data from an LCS to an SU ("unique ID" binding a transaction uniquely the LCS and SU)

A fragile watermark/SecureChannel is embedded with logical relationships to the quality/performance/enhancement of the data to be transmitted ("quality of the received data" fragile against signal manipulations – the carrot)

The system above where the robust watermark is renewable.
The system above where the robust watermark can be embedded using any one of a plurality of embedding algorithms.
The system above where the robust watermark can be upgraded by using logical relationships in time /location/modality of the original watermark and any subsequently embedded watermark
The system above where the forensic watermark is embedded upon export of data from the LCS

DISH-Blue Spike-246
Exhibit 1012, Page 0022

The system above where the forensic watermark is embedded upon successful authentication of the SU

The system above where the forensic watermark is embedded in a manner unique to the transmission of the data to an SU (time stamp, unique signature, etc.)

The system above where any SU must be accessible by a predetermined secure transmission means (encrypted line, SSL, open line but secure transmission is possible, etc.)

The system above where the SU has a unique identity

The system above where the SU's identity may be changed by the LCS in a predetermined manner

The system above where the relationship between an LCS and an SU is the basis for seeding a public key exchange

The system above where the relationship between an LCS and an SU enables steganographic ciphering of any data to be transmitted between said LCS and said SU

The system above where the fragile watermark/SecureChannel is predetermined prior to data being introduced to an LCS

The system above where the fragile watermark/SecureChannel is accessible by an SU based on predetermined access rules

The system above where the fragile watermark/SecureChannel is unique to the SU

The system above where the quality of the data is manipulated by the LCS

The system above where the quality of the data is a direct function of predetermined identification/authentication protocols

Each path as a separate claim

- A method for data transmission comprising the following steps:

  A user completes a transaction with a SECD

  An LCS sends its unique ID/public key to the SECD

  The SECD utilizes the received LCS unique ID/public key to initiate secure transmission of the data (the watermarked data can be encrypted or scrambled, "ciphertext", for transmission) to the LCS

  The LCS unwraps (converts ciphertext into plaintext) the secured data and performs a presence check/authentication/verification check dependent on at least one of a plurality of watermarks.

The method above where a plurality of SECDs uses any of a plurality of security protocols

The method above where payment is independent of the data transmission

The method above where payment is a requirement for authorized transmission

The above where a public key cryptosystem is used for enabling secure transmissions

DISH-Blue Spike-246
Exhibit 1012, Page 0023

The method above where the LCS and SECD agree to a secure key exchange

- (LCS to Rewritable medium) A method for data transmission comprising the following steps:

  Data is imported/transmitted into a LCS from a rewritable medium

  The data undergoes authentication/verification of the LCS watermark (robust open watermark - ROW)

  If the watermark is NOT present/authenticated the data is degraded to "Low Quality"

  If the watermark IS present/verified/authenticated, the imported/transmitted hash is verified/checked against the LCS and the data is enabled to enter the LCS at High Quality.

- (LCS from Read-Only medium) A method for data transmission comprising the following steps:

  Data is imported/transmitted into a LCS from a read-only medium.

  The data undergoes authentication/verification of the LCS watermark (robust open watermark - ROW)

  In the watermark is NOT present/verified/authenticated the data is degraded to "Standard Quality" and allowed to enter the LCS.

  If a watermark IS present/verified/authenticated the imported/transmitted hash is checked to verify that the content matches said LCS.

  If the imported/transmitted hash matches the LCS, the data is allowed in at High Quality.

The method above where the read-only medium has a media-based identifier to enable differentiations between original media and copied media.
The method above where the media-based identifier is verified/authenticated, the data is able to be imported/transmitted to the LCS at "High Quality".

- (From SU to LCS) A method for data transmission comprising the following steps:

  Data is watermarked by the SU with information uniquely identifying the SU

  The data can also contained a hash dependent on the unique identity of the LCS

  If the LCS hash of the data IS checked/verified/authenticated the data can be imported/transmitted into the LCS

- (LCS to non-SU's) A method for data transmission comprising the following steps:

DISH-Blue Spike-246
Exhibit 1012, Page 0024

Data is received from a device which lacks unique ID such as with a unique SU ID

The LCS embeds a watermark unique to the LCS and the characteristics of the content which includes a one way function (hash, time stamp, signature) (the embedded hash)

The LCS watermark can contain additional information related to the use parameters/manipulation/handling of the data

If the data is exported to a rewritable medium, the LCS can further add a second/unrelated external one way function (hash, time stamp, signature) in a manner not logically related to the first one way function generated (the second hash should not be easily determined with knowledge of the first) by using cryptographic ciphers (the second hash is to associated externally to the data- it is not embedded in the data)

- (LCS to SU) A method for secure data transmission comprising the following steps:

  Data is received from a device which successfully identifies itself as an SU

  If the data is exported to a rewritable medium, the LCS can further add an external one way function (hash, time stamp, signature) in a manner not logically related to the LCS watermark (the second hash should not be easily determined with knowledge of the watermark or embedded hash) by using cryptographic ciphers (the second hash is to be associated externally to the data- it is not embedded in the data)

The method above where the data is check by a public key cryptosystem.
The method above where the data/SU/path can be authenticated/verified/authorized by the LCS with predetermined transmission security protocols.

- (Data recorded on an SU) A method for data transmission comprising the following steps:

  Data is first recorded by the SU and watermarked as SU recorded data.

  The SU identifies itself.

  The SU watermark

Path 7: This path is for content that is recorded on a SU. All content is allowed to enter this path but it is always degraded to Low Quality.

Path 8: This path is for content that is rendered by the SU. This content is

1.) An apparatus for creating a secure local environment for digital content (LCS Domain) with the following characteristics:

DISH-Blue Spike-246
Exhibit 1012, Page 0025

a) The content is not accessible except through the approved functions of the Local Content Server (LCS).
b) The LCS has one or more paths to enable import of content, each of which has an associated set of rules governing import content quality.
c) The LCS has one or more paths to export content, where each path is secured.
d) The LCS has a unique identifier (Unique ID).
e) The LCS may interact with **trusted** Satellite Units (SU) which can store and/or render the content.
f) Any Satellite Units (SU) which can interact with the LCS have unique identifiers.
g) Any communication between the LCS and a SU must be on an authenticated, secure channel.
h) All export paths on SU's are secured.
2.) The method in claim 1 where the content is digital audio.
3.) The method in claim 1 where the content is digital images.
4.) The method in claim 1 where the content is digital video.
5.) The method in claim 1 where the import path is from a secure provider of digital content and the transfer of the content can be authenticated such that:
a) the transfer is authorized by a trusted party,
b) the content is verified to be unchanged during the transfer,
c) the content is not usable if it is intercepted during the transfer, it is (encrypted or scrambled).
6.) The method in claim 1 where the import path is from a rewritable medium.
7.) The method in claim 6 where the content has no authenticatable watermark and the import occurs at a degraded content quality level.
8.) The method in claim 6 where the content has a authenticatable watermark which does not match the importing LCS and the import is disallowed.
9.) The method in claim 6 where the content has a authenticatable watermark which does match this LCS and the import is allowed at high content quality.
10.) The method in claim 1 where the import path is from a read-only medium.
11.) The method in claim 10 where the content has no authenticatable watermark and the import occurs at a standard content quality level.
12.) The method in claim 10 where the content has a authenticatable watermark which does not match the importing LCS and the import is disallowed.
13.) The method in claim 10 where the content has a authenticatable watermark which does match this LCS and the import is allowed at high content quality.
14.) The method in claim 10 where the content has no authenticatable watermark from an LCS but has a verifiable identifier indicating that the content is first generation and the import is allowed at high content quality.
15.) The method in claim 1 where the import is from a Satellite Unit through an authenticated, secure connection.
16.) The method in claim 15 where the SU watermark contains an identifier which matches the LCS and the import is allowed at high content quality.

DISH-Blue Spike-246
Exhibit 1012, Page 0026

17.) The method in claim 15 where the SU watermark contains an identifier which does not match the LCS and the import is disallowed.
18.) The method in claim 15 where the SU watermark contains an identifier which does not contain an LCS identifier and the import is allowed at high content quality.
19.) The method in claim 1 where the export path is to a rewritable medium. The content is marked using a watermark which contains a hash constructed from the LCS Unique ID and content characteristics.
20.) The method in claim 19 where a second hash generated by a different method is attached to the exported file outside of the content.
21.) The method in claim 1 where the export path is to a rendering device. The content is marked using a watermark which contains a hash constructed from the LCS Unique ID and content characteristics.
22.) The method in claim 1 where the export path is to a SU through an authenticated, secure connection. The LCS provides a hash to the SU, which the SU permanently associates with the content. The hash is constructed from the LCS Unique ID and content characteristics.
23.) The method in claim 22 where the SU uses the hash supplied by the LCS to generate a watermark on all exported content.
24.) The method in claim 23 where the SU adds its own hash to the watermark on all exported content. The hash is constructed from the SU Unique ID and content characteristics.
25.) The method in claim 1 where the LCS and SU do not use the same watermarking technique.
26.) The method in claim 25 where the LCS can read watermarks written by any SU with which it can communicate.
27.) The method in claim 5 where the LCS can communicate with more than one secure provider, where each provider can use a different method of securing the transaction.
28.) The method in claim 5 where encryption is used in the transaction.
29.) The method in claim 5 where scrambling is used in the transaction.
30.) The method in claim 5 where public key cryptography is used in the transaction.

RENEWABILITY CLAIMS:

•A method for data protection where a data signal carries at least one bit of watermark data that enables determination of additional, subsequent embedding of separate independent data.

•A method for data protection where predetermined locations can be used to differentiate between an original watermark data and any subsequent watermark data.

DISH-Blue Spike-246
Exhibit 1012, Page 0027

•A method for data protection where watermarked data is checked/authenticated/verified prior to embedding subsequent independent data.

100. A method in claim 1 (see claim 1 above: the apparatus claim) where a robust watermark is embedded in new content to distinguish it from legacy content, where the robust watermark carries a single bit payload which distinguishes content distributed in individualized packages from content distributed in non-individualized packages. ("individualized" pertaining additionally to uniqueness of the content given a transaction event)

101. A method in claim 100 where the robust watermark is added to all content which enters the environment without a robust watermark. The added watermark is set to the individualized media setting/condition/predetermined status.

102a. A method in claim 100 where the robust watermark system can be periodically replaced with a new system with the same payload.

102b. A method in claim 100 where the robust watermark algorithm can be periodically replaced with a new algorithm with the same payload.

103. A method in claim 102 where, during a transitional period between robust watermarking systems, released content can be marked with both the old and new watermarks.

104. A method in claim 103 where the watermarks are overlaid directly upon one another.

105. A method in claim 103 where the watermarks are interleaved in time.

106. A method in claim 103 where the watermarks are interleaved in space.

107. A method in claim 103 where the watermarks are interleaved in frequency.

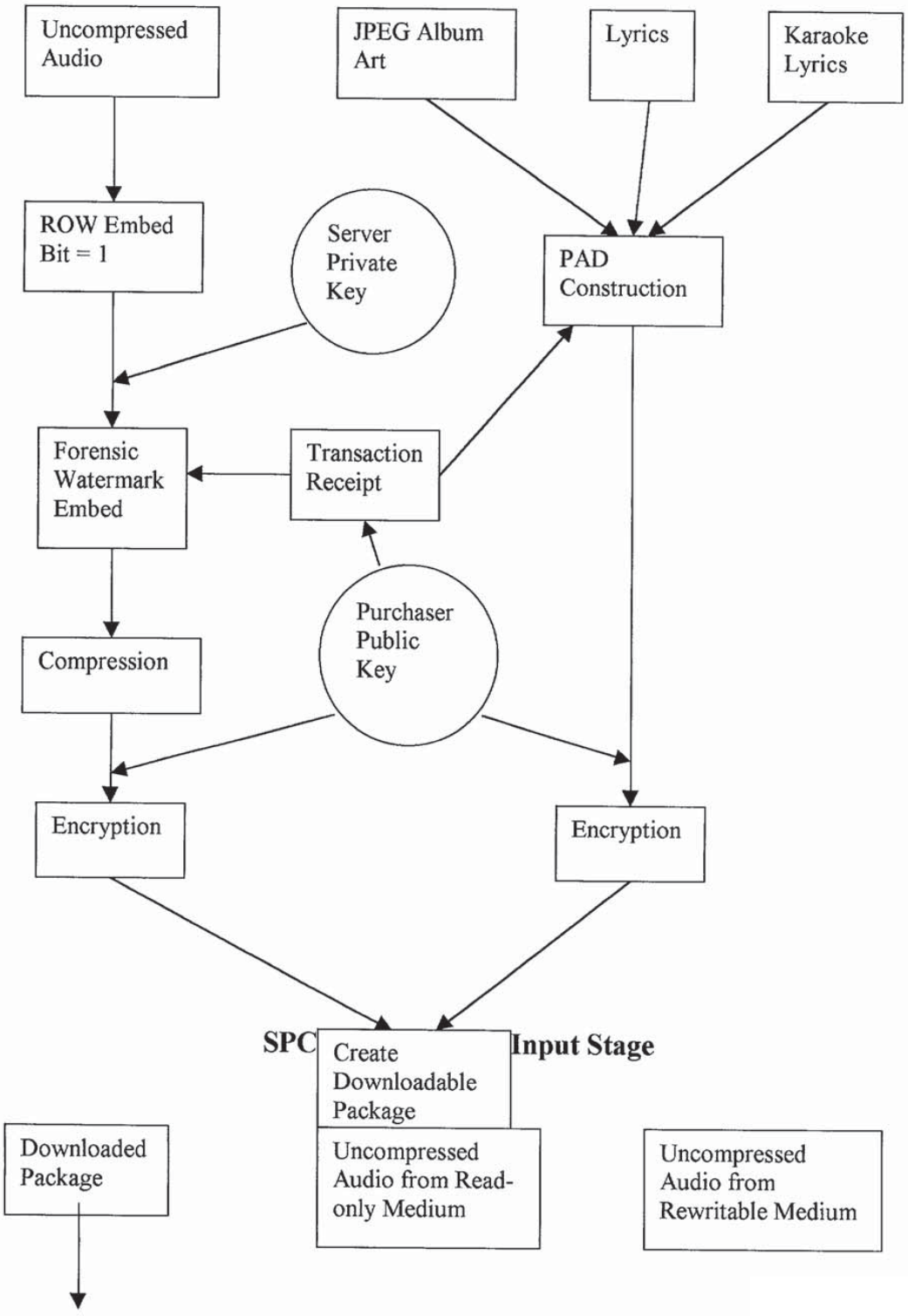
DISH-Blue Spike-246
Exhibit 1012, Page 0028

A method where the LCM watermark is secured using the following steps:
-A block of PAD is encoded into a block of samples.
-A hash of the the PAD block and a random number seeded by the owner's identity is generated and encoded into the subsequent block of samples.
-A hash of the first two blocks of samples and a random number seeded by the owner's identity is generated and encoded into a third block of samples.

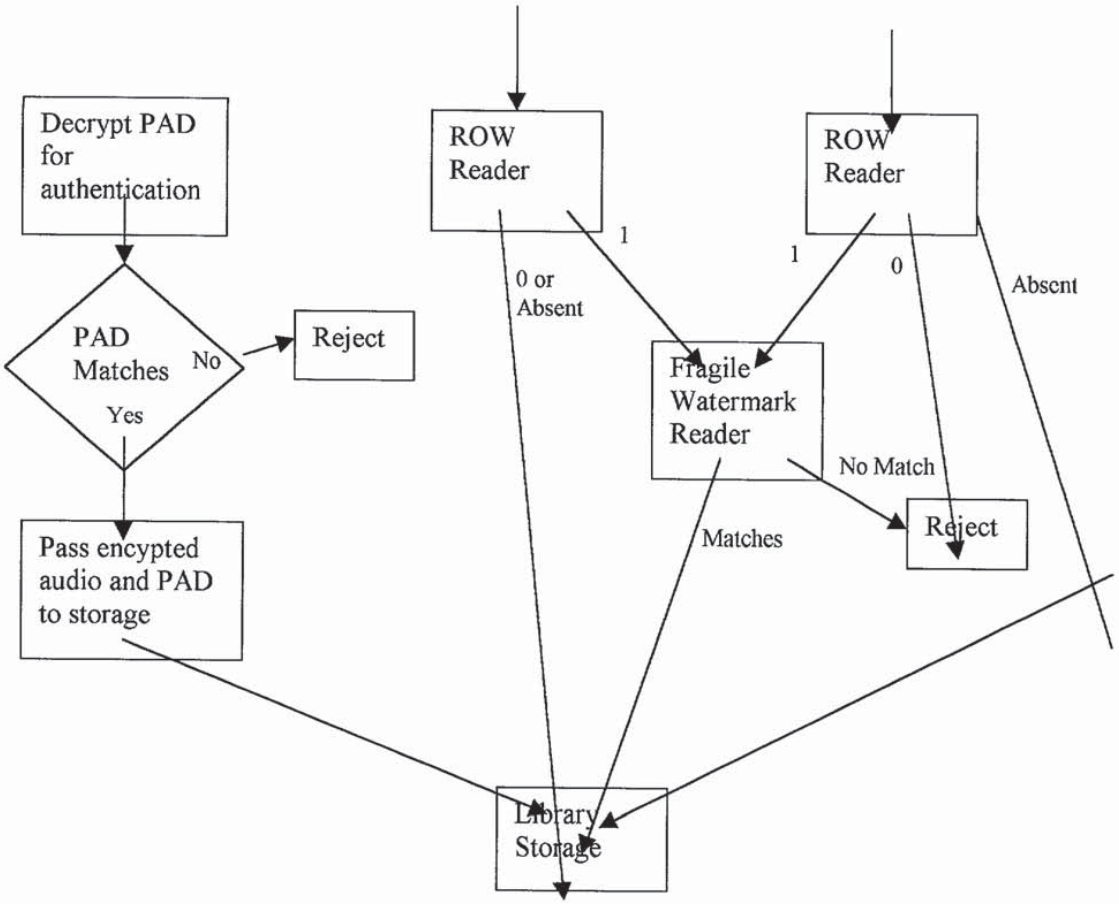
x) A method where the SU Watermark has two possible states.
x1) A method of claim x where one of the watermark states corresponds to content which is only allowed entry with a verifiable LCM watermark.
x2) A method of claim x where one of the watermark states corresponds to content which is only allowed entry either if the transfer is from a read-only medium or if the content has a verifiable LCM watermark.
--

DISH-Blue Spike-246
Exhibit 1012, Page 0029

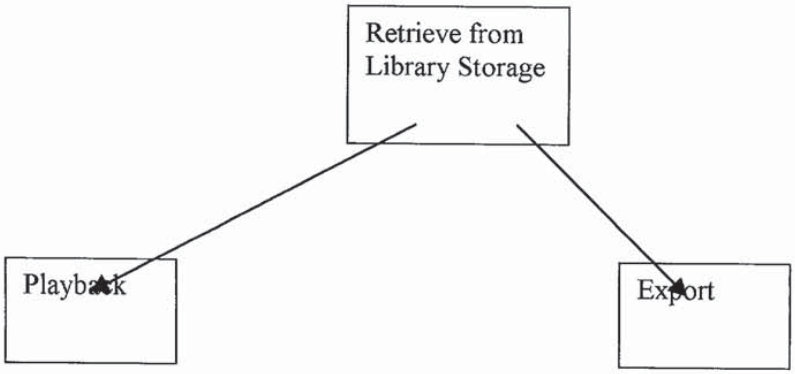
"Secure Personal Content Server" Provisional Patent Application No. 60/147,134
SAMPLE EMBODIMENT- SPCS Audio Server Stage

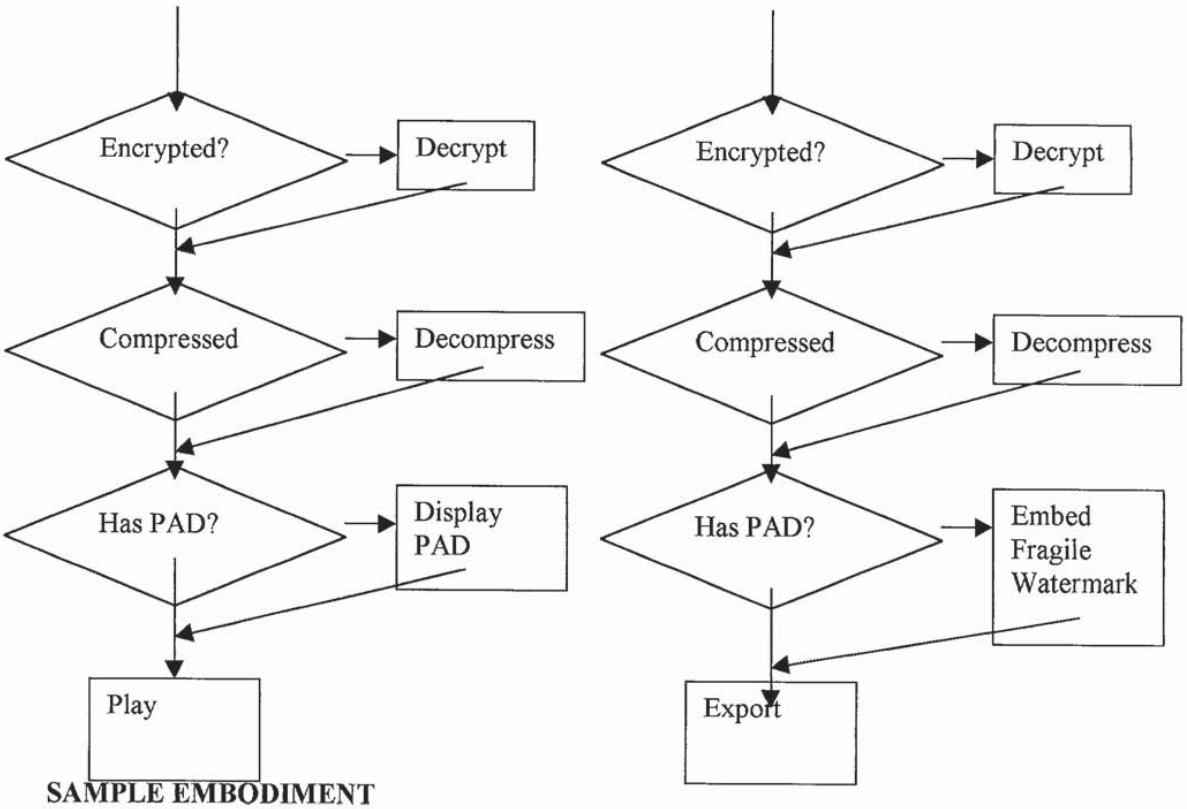


DISH-Blue Spike-246
Exhibit 1012, Page 0030



SPCS Audio Player Output Stage





SAMPLE EMBODIMENT
Fragile Watermark Structure

The fragile watermark can actually hold the entire PAD, encoded in the LSB of each 16 bit sample. This gives a data rate of 88200 bits per second in a stereo CD file, or a capacity of 1.89 M in a 3 minute song. This is an immense capacity relative to the expected size of the PAD (100 - 200 K).

The fragile watermark needs to be bound to a specific copy of a specific song, so that it cannot be transferred to other songs. This binding can be achieved through use of a hash in the following sequence:

1.) A block of PAD is encoded into a block of samples.
2.) A hash of the the PAD block and a random number seeded by the owner's identity is generated and encoded into the subsequent block of samples.
3.) A hash of the first two blocks of samples and a random number seeded by the owner's identity is generated and encoded into a third block of samples.
4.) repeat as necessary

Each PAD block has the following structure:

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

An application can read the block identifier and determine if it recognizes the block type. If it doesn't, it can use the BlockLength to skip this block.

Certain Block types will be required to be present if the PAD is going to be accepted. These might include and identity block and a PAD Hash block. The Block Data may or may not be encrypted, depending on whether the data is transfer-restricted (value-adding) or simply informative. For instance, user-added PAD data would not need to be encrypted. The BlockIdentifier would indicate whether the block data was encrypted or not.

Robust Open Watermark

This is the mark that indicates non-legacy content. There are two possible settings. 1 indicates non-legacy content that must be accompanied by an authenticatable PAD for entry into the domain (e.g. electronic music distribution or EMD content). 0 indicates non-legacy media that was distributed in a pre-packaged form (e.g. CD's). 0 content may have a PAD, or it may not. 0 content shall only be admitted from a read-only medium in its original file format (e.g. a 0 CD shall only be admitted if it is present on a Redbook CD medium).

Robust Forensic Watermark

This watermark is not accessible in any way to the consumer. It is secured by a symmetric key held only by the seller. A transaction ID is embedded at the time of purchase with a hash matching the symmetric key. The watermark is then embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of this watermark is not limited by real-time/low cost constraints. The recovery will only be attempted on pirated material. A recovery time of 2 hours on a 400 MHz PC is reasonable.

Additional Claims for "Secure Personal Content Server" : "Renewability"
Provisional Patent Application No. 60/147,134

These claims primarily relate to "renewability" for the SPCS provisional patent application.

The scenario:

1) Have existing watermarked content, will also have nonwatermarked content of course.

2) Existing SPCS in the field

3) Hack occurs or Upgrades for new algorithms are sought by content owners or their agents

4) Have new embedding algorithm but SPCS's have yet to be upgraded

5) Want content to be recognizable by the old SPCS and the new SPCS

We move from an "Original watermark" to an "Upgrade watermark" and there is a transitional period.

Transitional period for which both original and upgrade watermarks are embedded into content—at mastering stage (SPCS is either upgraded or not upgraded), the determination is made by the content owner at the "mastering" point, prior to distribution.

Content owner knows that a hack has happened or seeks to simply upgrade ("pull the trigger" bit) and introduces both original and upgrade watermarks. Movement to only upgrade watermark during transition: the content owner may want to be in both states depending on how pervasive the hack and how quickly content owner wants to upgrade.

For purposes of supporting both old and upgrade watermarks we can use predetermined "rules" for the embedding process: Statistical changes so that say if a detection window is 15 seconds can upgrade every 30 seconds. Meaning timing or frequency can be used as a "modality" for where the upgrade watermark is to be introduced and allowing for co-existence with original watermark. (i.e., old watermark has a detection window of 15 seconds, upgrade is 30 seconds, etc.)

Claims:

DISH-Blue Spike-246
Exhibit 1012, Page 0034

•A method for data protection where a data signal carries at least one bit of watermark data that enables determination of additional, subsequent embedding of separate independent data.

•A method for data protection where predetermined locations can be used to differentiate between an original watermark data and any subsequent watermark data.

•A method for data protection where watermarked data is checked/authenticated/verified prior to embedding subsequent independent data.

100. A method in claim 1 where a robust watermark is embedded in new content to distinguish it from legacy content, where the robust watermark caries a single bit payload which distinguishes content distributed in individualized packages from content distributed in non-individualized packages. ("individualized" pertaining additionally to uniqueness of the content given a transaction event)

101. A method in claim 100 where the robust watermark is added to all content which enters the environment without a robust watermark. The added watermark is set to the individualized media setting/condition/predetermined status.

102a. A method in claim 100 where the robust watermark system can be periodically replaced with a new system with the same payload.

102b. A method in claim 100 where the robust watermark algorithm can be periodically replaced with a new algorithm with the same payload.

103. A method in claim 102 where, during a transitional period between robust watermarking systems, released content can be marked with both the old and new watermarks.

104. A method in claim 103 where the watermarks are overlaid directly upon one another.

105. A method in claim 103 where the watermarks are interleaved in time.

106. A method in claim 103 where the watermarks are interleaved in space.

107. A method in claim 103 where the watermarks are interleaved in frequency.

DISH-Blue Spike-246
Exhibit 1012, Page 0035

SDMI Phase II Descriptive Summary

Using Blue Spike's Trusted Transaction Security Architecture

The Blue Spike Secure Digital Watermarking System for Music

Overview:

The Blue Spike SDMI Phase II proposal is for a Robust Open Watermark (ROW) which is tied to out-of-band usage and rights information and a fragile watermark for compression detection. The ROW has a simple 1 bit payload. The ROW detector can be implemented in a small footprint on hardware or software devices. The ROW is renewable.

Functional Overview:

The Blue Spike ROW splits music into three general classes: music distributed in a secured format, music distributed in an unsecured format, and legacy music. Each of these is represented by a state of the ROW.

ROW = Secure Protected:

This state is set for any content which is distributed in a secured manner. This would include EMD and future secured physical carriers such as DVD-Audio or SACD. When a detector registers "Secure Protected," it is required to validate out-of-band information. This could be an encrypted header, or a secured channel for streaming (such as a secured port on a DVD-Audio player). If the out-of-band data cannot be authenticated, the content is not allowed through the screen.

ROW = Unsecured Carrier:

This state would primarily be used for Redbook CD Audio. It would be coupled with a compression detecting fragile watermark. If both the ROW and the fragile watermark were present, the content would be admitted. If only the ROW were present, the content would be rejected.

ROW = Absent

This state would exist for all legacy content. All legacy content would be admitted into the system. On higher capability devices, legacy content would then be remarked "Secure Protected."

What about Copy Control?

All copy control situations envisaged by the SDMI Phase I CCI bits can be accomplished using the Blue Spike ROW in conjunction with a secured channel for streaming.

-Redbook CD-Audio does not have CCI capability under Phase I. Our system would add a limitation for compressed copies.

- Future physical formats. A secured physical format would be distributed with the ROW set to "Secure Protected." Copies could only be made on a secured channel, similar to the "One More Copy" setting. The secured channel would also have the capability of communicating more detailed usage information in a low overhead manner through out-of-band data.

- EMD. EMD already would come in a SDMI Protected format. Once it is removed from that package, no copies will be allowed.

DISH-Blue Spike-246
Exhibit 1012, Page 0037

Renewability

An "Open Watermark" is one which relies on a secret which is shared by an entire class of devices, as differentiated from a "Secure Watermark" which is readable only by a single member of a class of devices. An Open Watermark is required for an SDMI screen, since the screen must be able to read the watermark from content which is not individualized before sale. However, ANY Open Watermark will eventually be hacked, first by removal and then by falsification. Thus a renewable system is an absolute necessity.

The Blue Spike ROW is renewable because of the simple nature of its payload. Since the payload only concerns the initial admit/reject decision, already admitted content has no relevant persistent open watermark data. Renewablility is achieved through the following scenario:

1.) The ROW is hacked, but the hack is hard to distribute or only works on certain content. This hack does not justify a renew decision. - or -
2.) A pervasive hack is created, easily distributed, posing a serious threat to the SDMI system.
3.) The renew decision is made by SDMI, balancing the cost of content lost against the cost of system upgrades.
4.) Blue Spike issues the new ROW algorithm, which is resistant to the hack and is updated to the current state of the art. The new ROW is guaranteed to take no more system resources than the old ROW, insuring that all devices can be upgraded. The new ROW detector completely replaces the old ROW detector.
5.) Content is issued with the new ROW and the old ROW. Furthermore, SDMI Protected Content also carries the message that the upgrade is required for new content to be admitted.
6.) The consumer upgrades his/her device (software upgradeRIGHT). In larger devices which had marking capability for legacy content, the upgrade also contains a new marker which upgrades, in the background, all old ROW content, which has become legacy.

Through this system, the Blue Spike ROW can be upgraded whenever there is a hack pervasive enough to justify the upgrade expense. Furthermore, this upgrade does not require a Phase III, or IV, and can be implemented within a short period of time after the hack reached critical mass. The upgrade does require a secure delivery system for the screen upgrade, which can be determined by the device manufacturer in accordance with SDMI specifications.

Testing the Blue Spike ROW

The Blue Spike ROW should be tested for robustness and audibility using the guidelines set out by SDMI. The robustness tests should determine whether the alleged mark (either Secure Protected or Unsecured Carrier is present after manipulation. Furthermore, for content marked Unsecured Carrier, the compression detection bit should be tested under the SDMI guidelines for compression detection.

The Blue Spike ROW should be subjected to reasonable malicious testing for removal. There is no need to test for falsification, since there is no conceivable gain to falsification over removal. As stated before, ANY open watermark will be subject to removal under some circumstances, such as overencoding by the same process. However, the renewablility of the Blue Spike ROW means that the malicious tests should only conclude that there is not an easy, general removal hack for the ROW.

Comparative Advantages

While the Licensed Technology currently purports the ability to maintain a fixed secret, the embedding algorithm for Phase 1, Blue Spike's proposal is based on the belief that flexibility and renewability are advantageous to any copyright security system. No fixed location or fixed secret can be expected to provide long term effectiveness as a screen. To the extent that maintenance of a shared secret across all portable devices (including the associated legal costs associated with interpretations of confidentiality) which are SDMI-compliant is not a reasonable expectation, Blue Spike's proposal also represents the ability to effectively compare the cost of renewing the screen versus the cost of an observed hack to an existing screen. As well, consistent support of legacy content enables a smoother transition from legacy content to an SDMI-compliant domain for authentic content.

Cost of an upgrade? Computational ease?

BLUE SPIKE

Didya Use Protection™

The Blue Spike Secure Digital Watermarking System for Music

Introduction

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

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

But the industry does have control over its copyrights, and armed with an effective security architecture, will be able to make these decisions for itself and protect its rights. Through consultations over several years with representatives of all facets of the music industry, coupled with a deep understanding of the security and digital watermarking technologies it has pioneered with its partners, Blue Spike Inc. has developed such an architecture for the protection of copyrights in the new millennium. That architecture is summarized here.

Market Requirements

Changing Consumer Behavior

Once a pattern of behavior has been established, it can be very difficult to change. Some examples of patterns consumers are currently in include:

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

We believe a successful solution will work within these realities rather than attempt to change them. Fortunately, we have designed a system that can ensure full protection of copyright owner's rights within these circumstances.

Nature of a Solution

To move a population into conformance with a new pattern, both carrot and stick must be applied judiciously. Blue Spike's architecture has potent implementations of each. Here is a list of the hallmarks of a successful solution:

Universality: We believe a successful architecture will have one universally applicable security system for physical carriers and electronically distributed files. Recordings must now be viewed as information made out of bits rather than tangible objects made out of atoms. How that information is stored will become increasingly irrelevant. The industry must seek to secure the information, not the media, or risk continuous obsolescence of its efforts.

Compatibility: Security-mandatory distribution is possible and desirable for new formats such as DVD-Audio or SACD, but obviously not for Red Book CDs. However, Red Book CDs must have some security included or they will present a gaping hole in the security scheme. Secure digital watermarking is the only feasible solution to this problem.

Inaudibility: In order for a watermark to be robust it must make significant changes to the audio stream. Blue Spike has succeeded in developing embedding technology that uses psychoacoustic filters to ensure the watermark is inaudible to the most discriminating ear.

Security: The implementation must be practically impervious to attack by even the most seasoned hacker. Since cryptosystems are only considered secure if subjected to open public malicious testing, Blue Spike advocates such testing before any implementation is chosen. Furthermore, the design must not be subject to one successful attack bringing the entire system down, as happened with CSS.

Transparency: While we seek to strongly impede and prevent their ability to distribute unauthorized recordings, we believe the security implementation should be utterly transparent to consumers until they attempt to overstep its boundaries.

Added Value: Finally, on the carrot side, we believe consumers will not pay more money for less functionality than they currently enjoy. They aren't likely to replace their existing audio hardware, which has no security implementation, with secure equivalents if they can help it. Therefore we provide them added value via our SecureChannel, which only the original purchaser may decode. SecureChannel can

carry any form of data, from HTML-based liner notes to merchandising coupons to custom sonic enhancement parameters.

Blue Spike is the only company that can provide an implementation that meets these requirements, by virtue of its extensive patent portfolio. Fortunately, Blue Spike now has a running implementation ready for immediate deployment.

DISH-Blue Spike-246
Exhibit 1012, Page 0043

Implementation

Blue Spike's Secure Digital Watermarking Architecture is built around five concepts:

The Robust Open Watermark (ROW)

The ROW is embedded in the original master recordings as they are prepared to enter distribution. There are only three possible states of the ROW:

Secure Protected: This indicates that the music is personalized to a single customer when it is distributed, for example through EMD or a kiosk system that creates physical media on demand.

Pre-Packaged Media: This indicates that the music came on a physical carrier that was not individualized to a particular consumer.

Absent: All currently extant music (legacy media) is obviously unmarked.

The ROW enables a simple set of rules:

- Only allow Secure Protected music to be used if its identity can be authenticated.
- Only allow Pre-Packaged Media to be used if the original medium can be found.
- Allow free usage of legacy media.

The ROW travels with the audio wherever it goes, through a large number of possible transformations. It is the basic gatekeeper to the system.

The Forensic Watermark

The forensic watermark is a secret mark placed into the audio at the last possible moment before distribution. It identifies the transaction. The forensic watermark is only readable by the holder of the key used to create it. No one else can read or alter the forensic watermark without this key.

The Download Package (DLP)

The DLP is an individualized cryptographic container which protects the music while it is inside the Blue Spike system. In an EMD situation, the DLP is prepared by the music server and then sent via a network to the customer. The DLP uses public key cryptography, ciphering, and, if desired, compression.

SecureChannel

SecureChannel is an auxiliary channel through which all of the members of the production and distribution chain can communicate directly with individual consumers. SecureChannel is never exposed and can only be obtained by legitimate methods. Its contents are vendor-definable and only limited by imagination. Some possibilities include:

Multimedia documents: album art, lyrics (including karaoke), webpages.

Playback enhancements: custom mixing coefficients for surround sound and environmental processing.

Sales material: coupons, promotions, other artists and projects, tie-ins.

DISH-Blue Spike-246
Exhibit 1012, Page 0044

Additional technologies: Digital Rights Management systems.

We provide SecureChannel. You provide the content. The content SecureChannel carries will be the carrot consumers use to justify the purchase of new, secure hardware and software that provides them the added value whilst denying them redistribution ability.

DISH-Blue Spike-246
Exhibit 1012, Page 0045

The Domain

At the heart of our system is the idea of a domain. A domain is a device or group of devices which share a single identity. A domain may be a single person, or a family. But the domain is always linked to a single purchasing account.

Inside a domain, you have free (fair) use of your music. You can make copies for different devices, you can upgrade your system, and you can add new devices. What you can't do is transfer music between domains. Each device can only be a member of one domain at a time. You can take a song to play in a friend's car, but only while your device or media is present. She can't save the song into her system.

The idea of a domain is crucial for consumer acceptance. Consumers will not accept a system which strongly curtails their usage rights when they are doing nothing wrong. However, consumers will also understand that there are unacceptable uses of their music (such as indiscriminate copying and redistribution) and will not mind that these activities are denied.

From a security standpoint, we only need to police the boundaries of the domain, while facilitating easy use inside the domain. So we check every piece of music as it enters the domain, but do not place heavy requirements upon the devices in the domain during everyday usage. Our system scales depending on the capabilities of the device. A simple playback device (like a portable player) has very little security overhead. Recording devices have more, as do Internet-capable devices. Overall, our system can be implemented with only a small incremental cost in each device, and without requiring new levels of processing power or storage.

DISH-Blue Spike-246

The System in Practice

A Typical Scenario

The band has finished recording, and the masters are back from the mastering engineer. The record company decides to pursue both Physical Carrier and Electronic Music Distribution strategies with their hot new product, while maintaining the best possible protection from piracy. They wisely choose Blue Spike's implementation, and obtain a unique private key for encryption.

The company gathers data for delivery via SecureChannel: album art and liner notes, catalogues and coupons for merchandise and live performances, lyrics with karaoke timing, and proprietary sonic optimization parameters that are exclusively available within secure playback systems.

The distribution engineer launches Blue Spike's encoder software and creates assemblies of the audio files and SecureChannel components along with descriptive information about each track.

The versions that will be distributed via physical carriers such as Compact Discs are given a corresponding Robust Open Watermark. At the glass mastering facility, each batch of discs is given a unique Forensic Watermark, which will assist in tracking them through sales channels.

The consumer of the CD will be able to play it on any standard CD player, new or old. However, if the user decides to import the audio from their hard drive they will be prompted to insert the original CD to verify they have a physical copy. This will be true of security-compliant MP3 players as well, since the watermark will survive MP3 compression. Furthermore, only security-compliant CD players will be able to view the SecureChannel data off the CD.

Files for Electronic Music Distribution are posted on a transaction server incorporating Blue Spike's security technology. Consumers log into this server and register their public keys generating a unique account with the record company.

For each track the consumer purchases, a forensic watermark uniquely identifying the transaction and the consumer is inaudibly embedded in the audio stream and will be virtually impossible for third parties to detect and remove. Thus each consumer is identifiable as the rightful owner of the track.

The Robust Open Watermark for EMD directs the player to look in the SecureChannel, where the user's information is also stored, to ensure that this track is being played with the purchaser's domain, rather than having been brought in from someone else's domain.

The consumer decides to export the track to another device within their domain. For systems where direct links aren't implemented, the consumer can use a standard .WAV file format for interchange. This .WAV file will inaudibly carry the watermarks and the encrypted SecureChannel data even though its audio will be playable in any standard .WAV player. No security compliant device outside of the domain will be able to play the audio or read the SecureChannel data, however.

Import of audio into the secure domain is possible, but will require the presence of the physical carrier to hinder piracy of legacy recordings.

0001-0000-0000-0000-0000-0000

Technical Specifications

Robust Open Watermark (ROW)

- Only encoded once, at the mastering studio.
- 1 bit payload
- Readable by all devices
- Average detection window 15-45 seconds.
- Encodes at real-time on PII 400.
- Decodes at 5x real-time on a PII 400.
- Detector necessary on any device that accepts and stores raw audio.
- Survives compression (MP3 64 or 80 Kbps), filtering, time-base modification (+/- 6%), pitch shifting (+/- 20%), dynamic compression, truncation, phase inversion, down-sampling (to 6 kHz), noise addition (at least -18 dB white noise).

Forensic Watermark

- Encoded at the time of purchase/distribution.
- 64 bit payload
- Embedded with a symmetric key which creates an embedding mask. The watermark is placed in only 25% of the available locations, known only to the keyholder.
- Payload contains an additional 96 bits of a hash (SHA-1) created from the message and the key, so that messages cannot be falsified without possession of the key.
- Average detection window 15 - 60 seconds.
- Preprocess encoding at mastering studio 50% real-time on PII 400.
- Encoding rate at purchase point limited only by disk access speed.
- Decoding may take up to 30 minutes. Decoding is only performed by the key holder and only on pirated material.
- No consumer detector required or possible.
- Similar robustness specs to ROW.

Fragile Watermark

- Encoded into any audio exported to a file from a consumer device.
- Payloads up to 1/16 of the uncompressed audio file size.
- Uniquely identifies the originating device, allowing for reimportation to other devices in the domain.
- Encode and decode speed limited only by disk access.
- Contains a hash made from the carrier audio, preventing the watermark from being copied to other audio.
- Disappears or becomes invalid under any audio transformation.

Encryption

- Unique public/private key pair for each purchased song.
- Encryption using the Blowfish symmetric cipher.
- Key storage of ~500 bytes per song.

SecureChannel

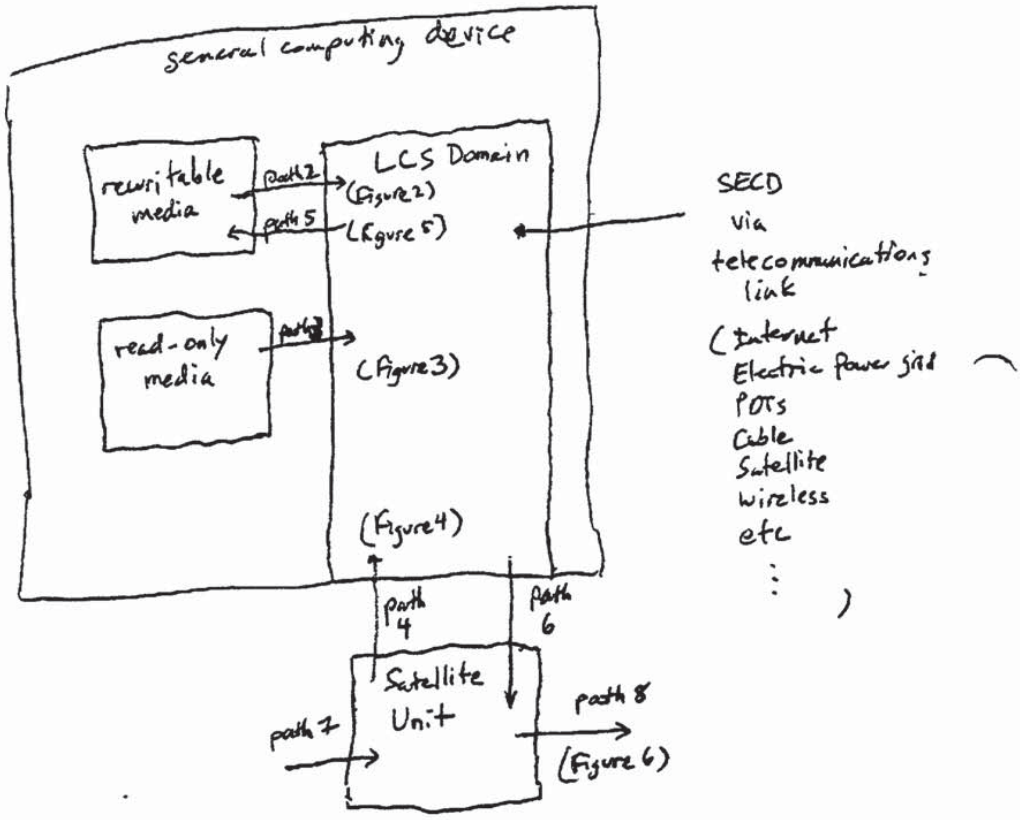
- Chunk-based format.
- Each chunk encrypted separately.
- Each device only receives and decodes the chunks that it understands.

DISH-Blue Spike-246
Exhibit 1012, Page 0049

Blue Spike Inc.
www.bluespike.com

Figure 1

Local Content Server
(general computing device)



confidential

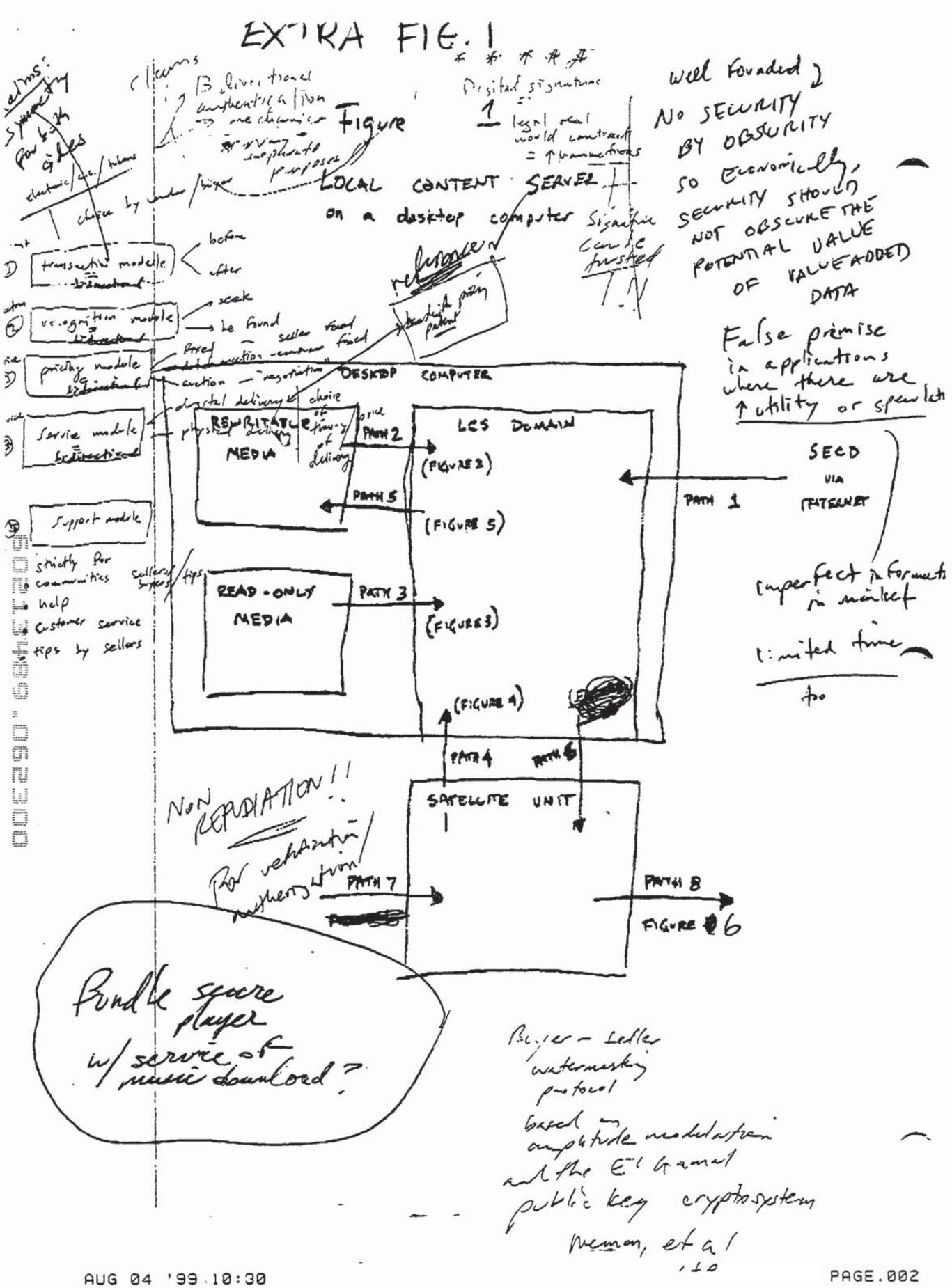
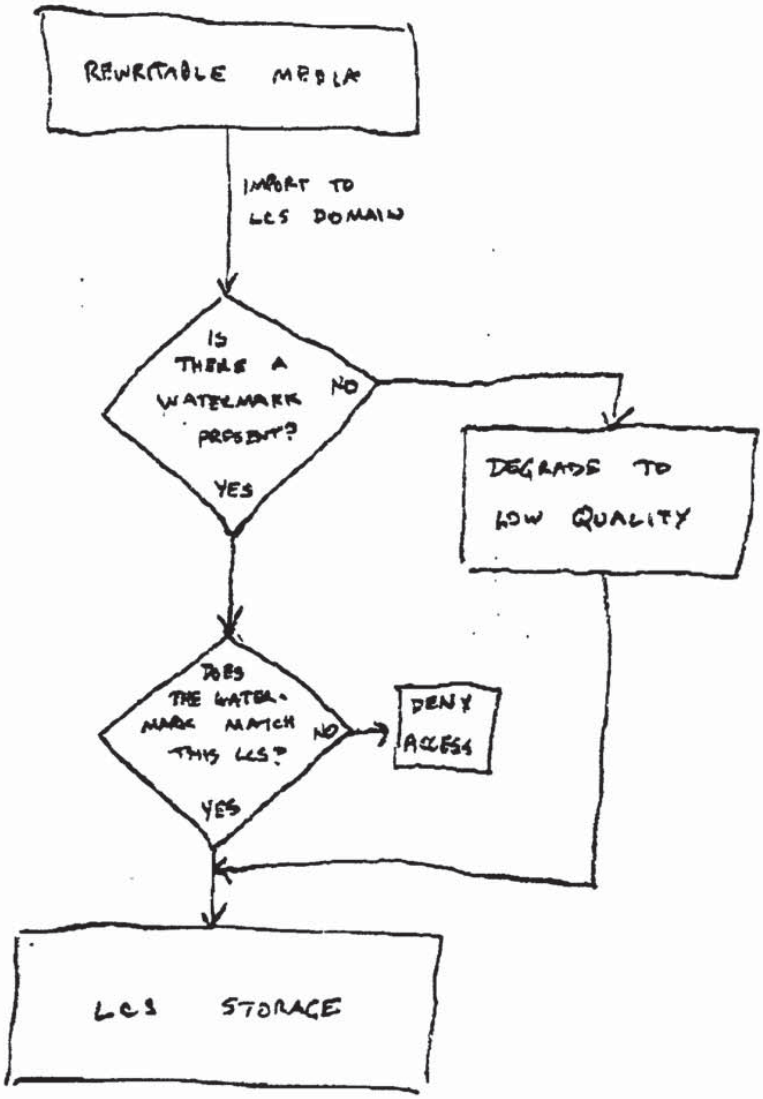

EXTRA FIG. 1
Figure
LOCAL CONTENT SERVER
on a desktop computer
Digital signature
1 legal real world contract
= ↑ transactions
Well founded
NO SECURITY BY OBSCURITY
SO ECONOMICALLY, SECURITY SHOULD NOT OBSCURE THE POTENTIAL VALUE OF VALUE ADDED DATA
False premise in applications where there are ↑ utility or speculation
transaction module
before
after
recognition module
seek
be found
pricing module
fixed
seller fixed
auction
negotiation
digital delivery
choice of
physical delivery
service module
support module
strictly for communities
help
customer service
tips by sellers
sellers/buyers/tips
DESKTOP COMPUTER
REWRITABLE MEDIA
PATH 2
PATH 5
LCS DOMAIN
(FIGURE 2)
(FIGURE 5)
PATH 1
SECD VIA INTERNET
imperfect information in market
limited time
too
READ-ONLY MEDIA
PATH 3
(FIGURE 3)
(FIGURE 4)
PATH 4
PATH 6
SATELLITE UNIT
NON REPUDIATION!!
For verification/authorization
PATH 7
PATH 8
FIGURE 6
Bundle secure player w/ service of music download?
Buyer - seller watermarking protocol
based on amplitude modulation and the El Gamal public key cryptosystem
Memon, et al
AUG 04 '99 10:30
PAGE.002

Figure 2.

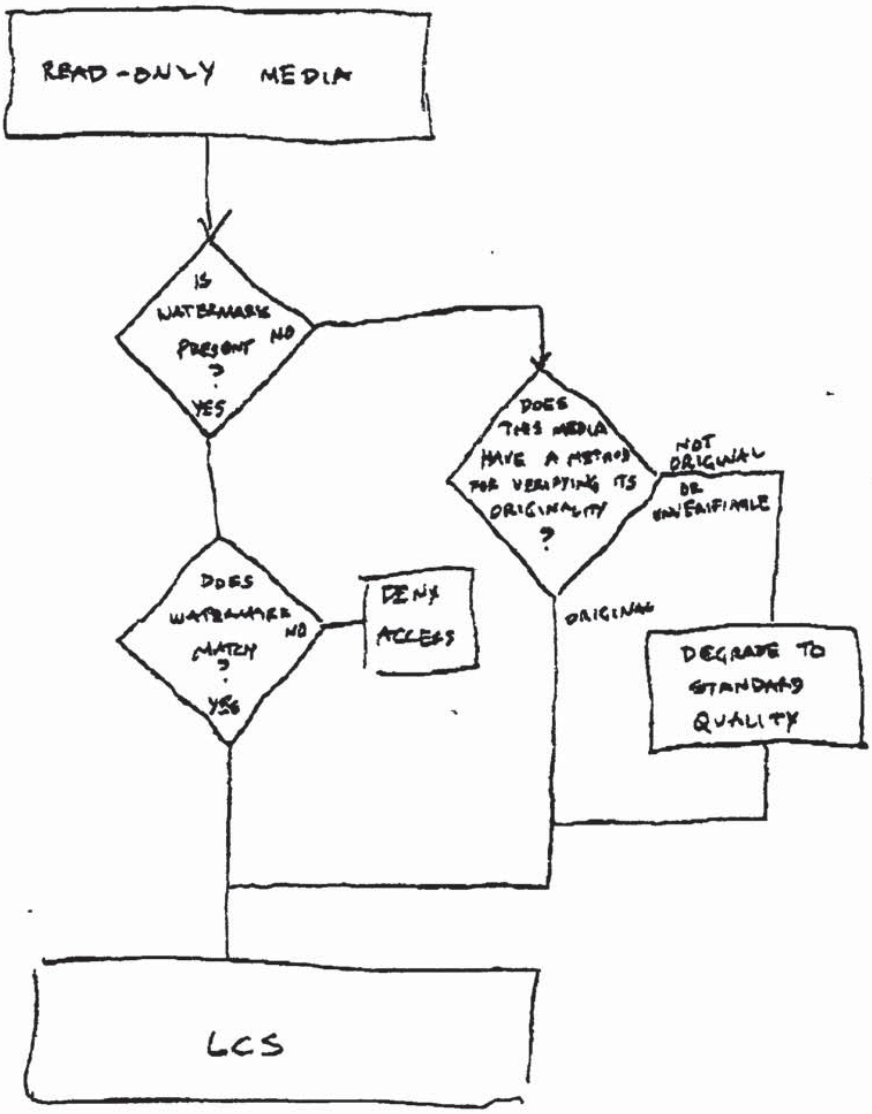
CONTENT ENTERING LCS DOMAIN FROM REWRITABLE MEDIA



DISH-Blue Spike-246
Exhibit 1012, Page 0053

FIGURE 3

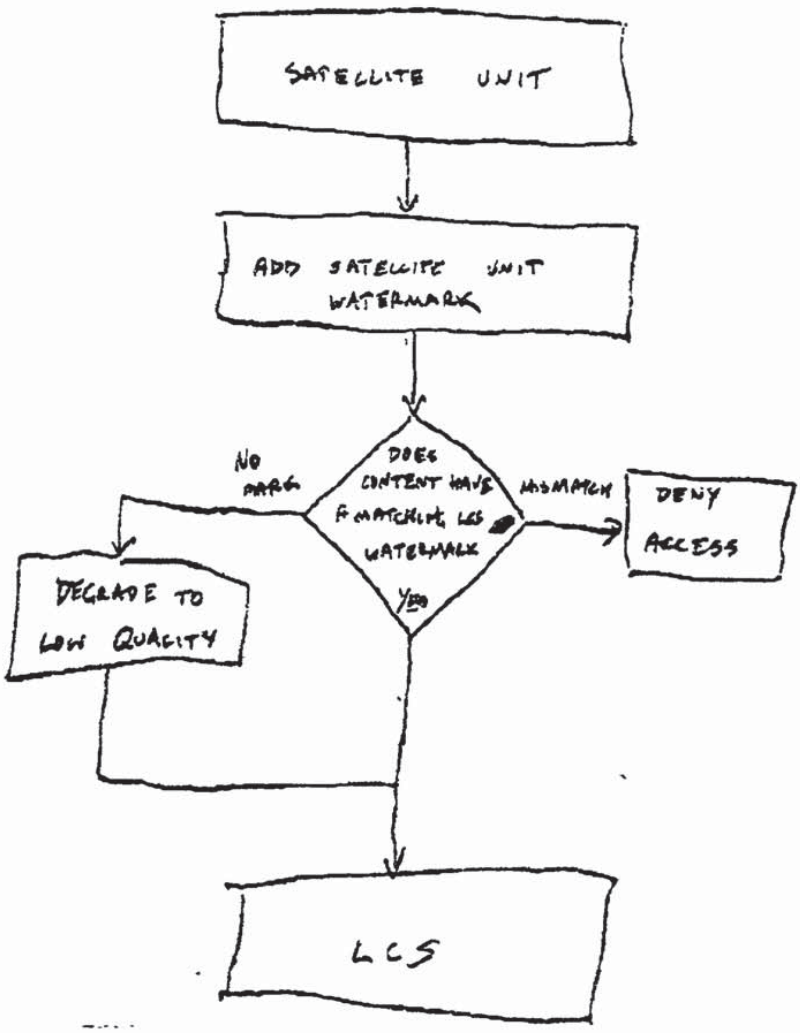
CONTENT ENTERING LCS DOMAIN FROM READ-ONLY MEDIA



DISH-Blue Spike-246
Exhibit 1012, Page 0054

FIGURE 4

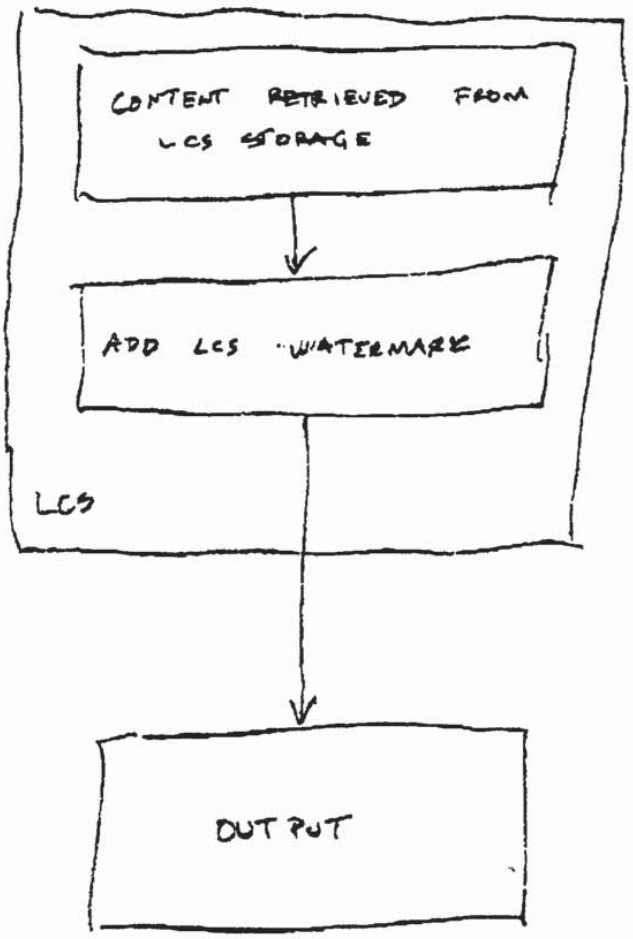
CONTENT ENTERING ECS DOMAIN FROM SATELLITE UNIT



DISH-Blue Spike-246
Exhibit 1012, Page 0055

FIGURE 5

CONTENT LEAVING LCS DOMAIN

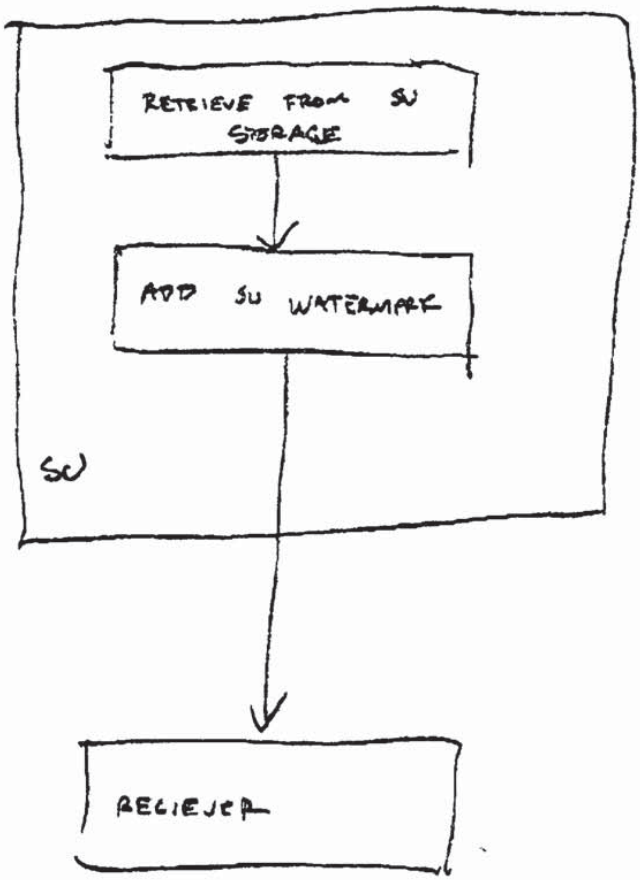


DISH-Blue Spike-246
Exhibit 1012, Page 0056

FIGURE 7

CONTENT LEAVING SU

TO RECIEVER OTHER THAN CCS



DISH-Blue Spike-246
Exhibit 1012, Page 0057