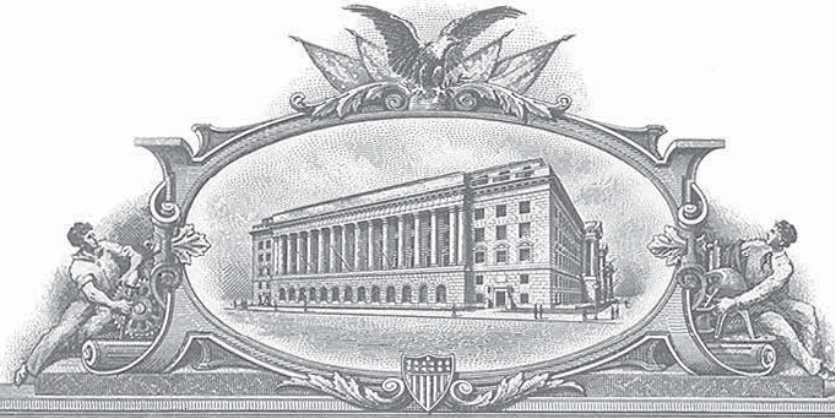


7715068



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

1c714 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).

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		
<input type="checkbox"/> 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:				
<input checked="" type="checkbox"/> Customer Number	24735	 24735 PATENT TRADEMARK OFFICE		
OR				
<input type="checkbox"/> Firm or Individual Name				
Address				
Address				
City	State	ZIP		
Country	Telephone	Fax		
ENCLOSED APPLICATION PARTS (check all that apply)				
<input checked="" type="checkbox"/> Specification	Number of Pages	49	<input type="checkbox"/> Small Entity Statement	
<input checked="" type="checkbox"/> Drawing(s)	Number of Sheets	7	<input type="checkbox"/> Other (specify)	
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)				
<input type="checkbox"/> A check or money order is enclosed to cover the filing fees				FILING FEE AMOUNT (\$)
<input type="checkbox"/> 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.				
<input checked="" type="checkbox"/> No.				
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are:				

3625 U.S. PTO
60/213489
06/23/00

60243489 062300

Respectfully submitted,

SIGNATURE Floyd B. Chapman

Date June 23, 2000

TYPED or PRINTED NAME Floyd B. Chapman

REGISTRATION NO. 40,555
(if appropriate)

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

June 23, 2000

066112.0138

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

265112

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 their role as consumers.

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

The present invention also seeks to provide improvements to the art in enabling a realistic model for building trust between parties (or their agents) not in a “system”, per se. Because prior art systems lack any inherent ability to allow for information to flow freely to enable buyers and sellers to react to changing market conditions. The present invention can co-exist with these “trusted systems” to the extent that all market participants in a given industry have relatively similar information with which to price value-added data. The improvement over such systems, however, addresses a core features in most data-added value markets: predictions, forecasts, and speculation over the value of information is largely 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

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

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

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

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

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

Definitions:

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

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

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

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

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

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

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

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

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

One way hash function: One-way hash functions are known in the art. 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 operate on 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

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.

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

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.

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.

}

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 an 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

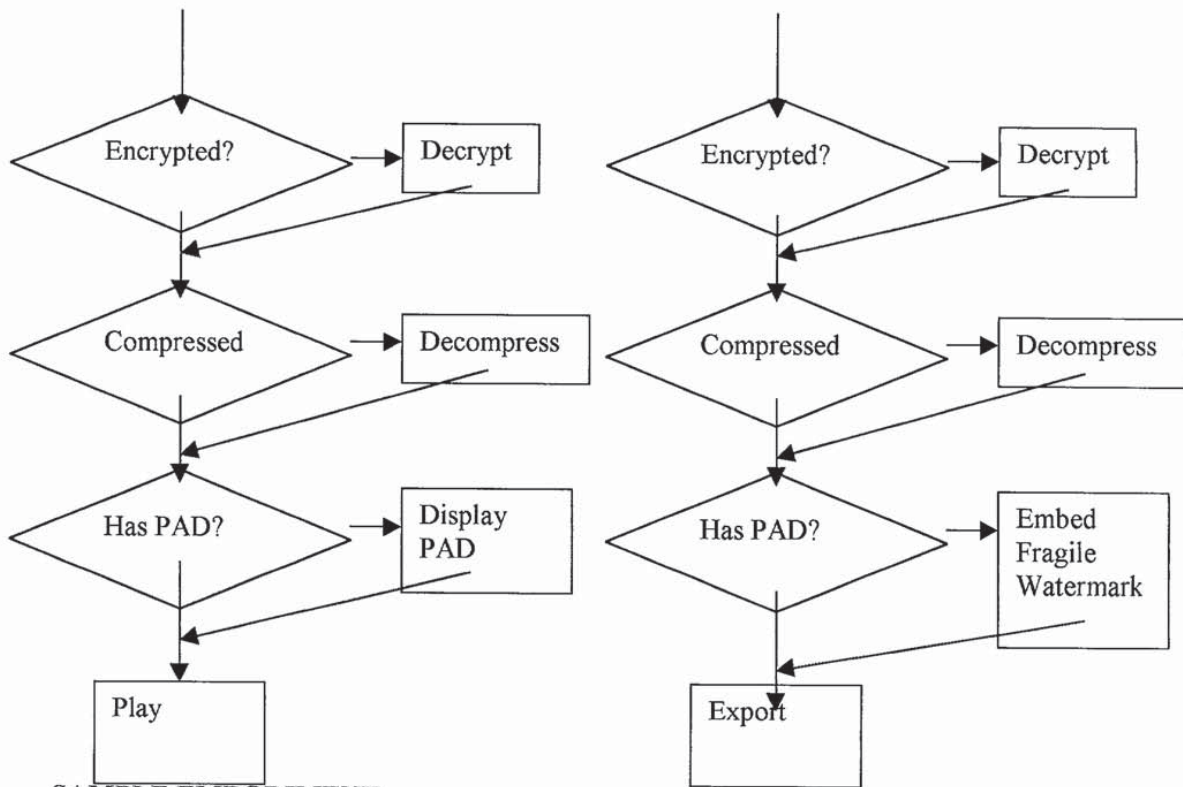
- 22.) The system in claim 1 where the export path is to a SU through an authenticated, secure connection. The LCS provides a hash to the SU, which the SU permanently associates with the content. The hash is constructed from the LCS Unique ID and content characteristics.
- 23.) The system in claim 22 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.



**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:

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.

000290" 04HET209

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.

SECURECHANNEL

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.

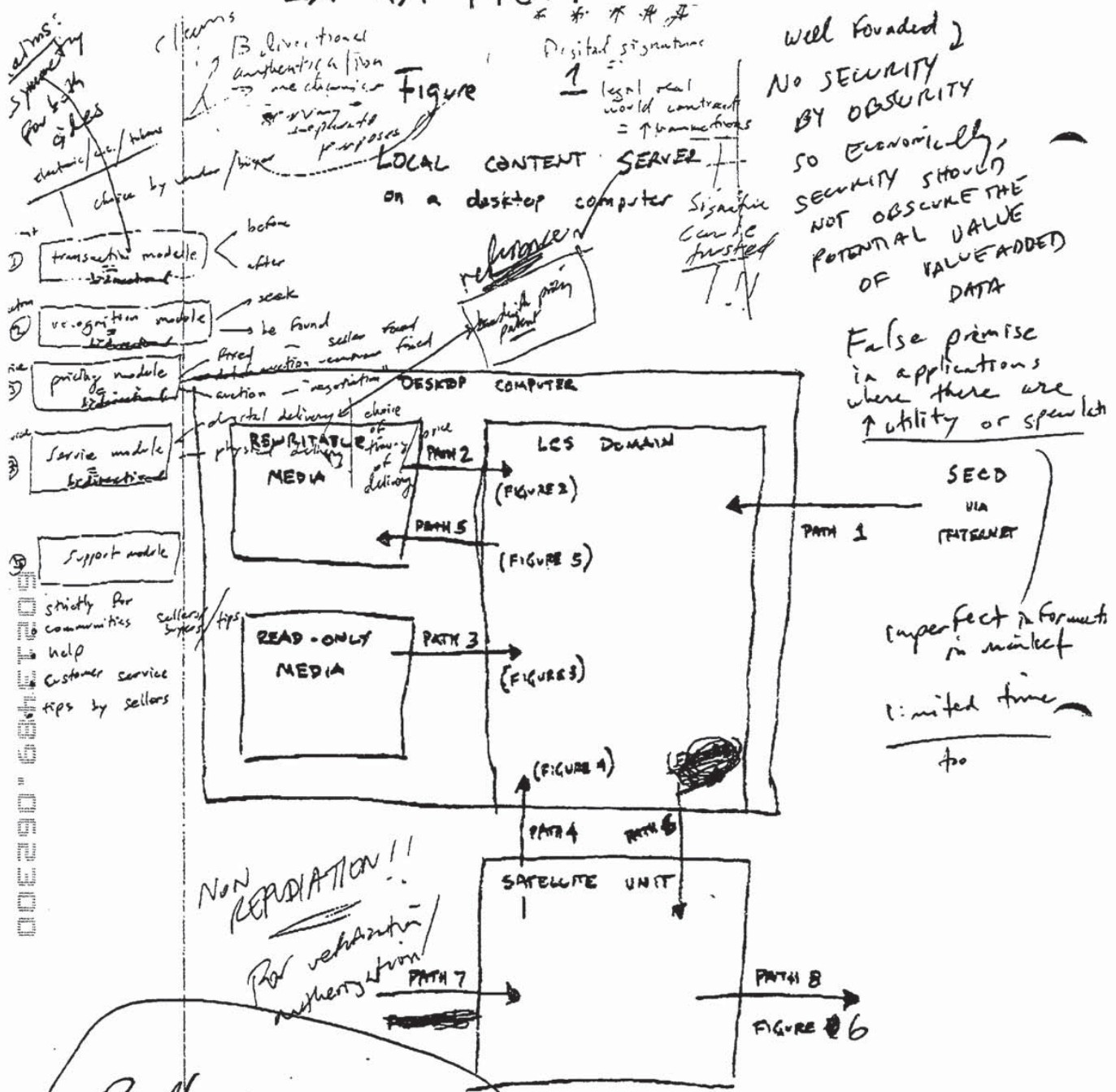
Inside a domain, you have free (fair) use of your music. You can make copies for different devices, you can upgrade your system, and you can add new devices. What you can't do is transfer music between domains. Each device can only be a member of one domain at a time. You can take a song to play in a 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.

00213489-062300

EXTRA FIG. 1

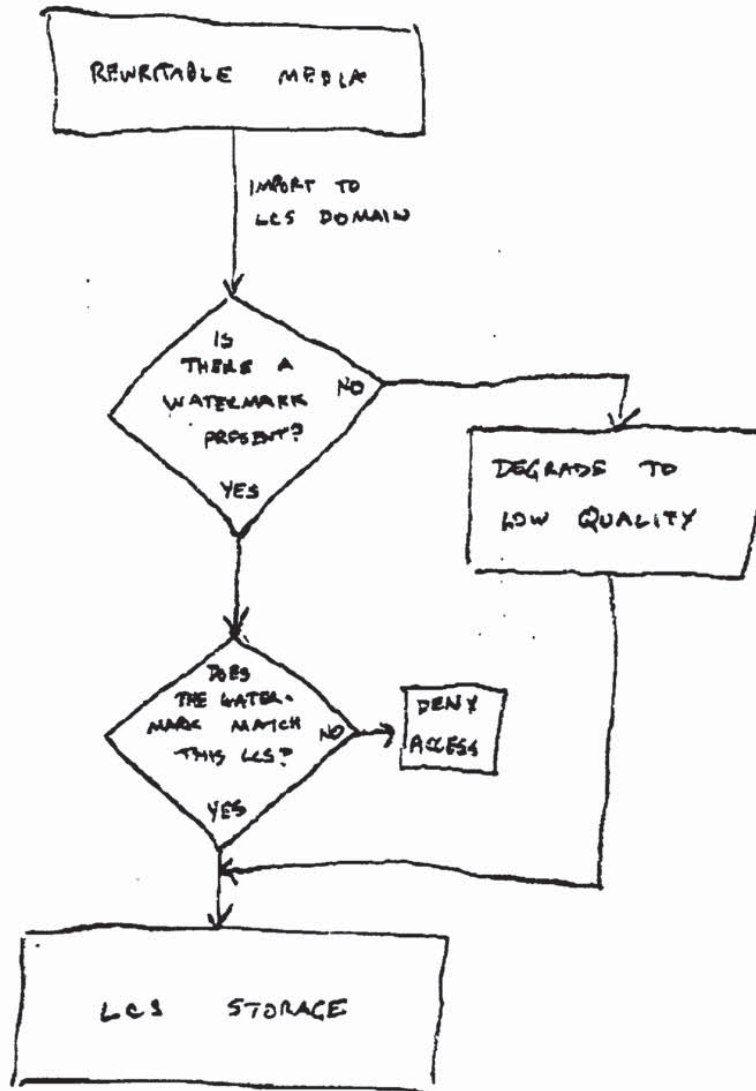


Bundle spare player w/ service of music download?

Buyer - Seller watermarking protocol based on amplitude modulation and the E² channel public key cryptosystem
 Memon, et al

Figure 2

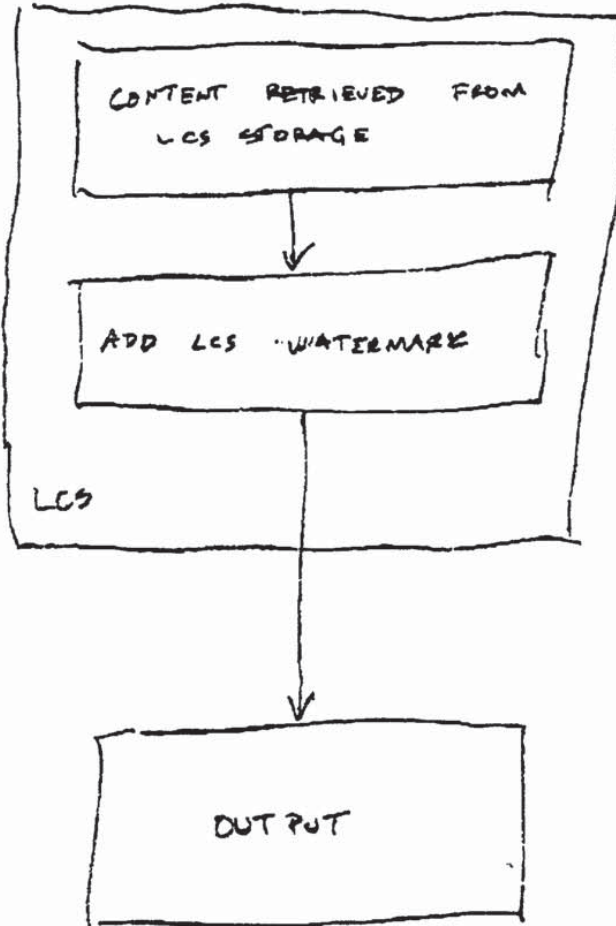
CONTENT ENTERING LCS DOMAIN FROM REWRITABLE MEDIA



000290" 6842209

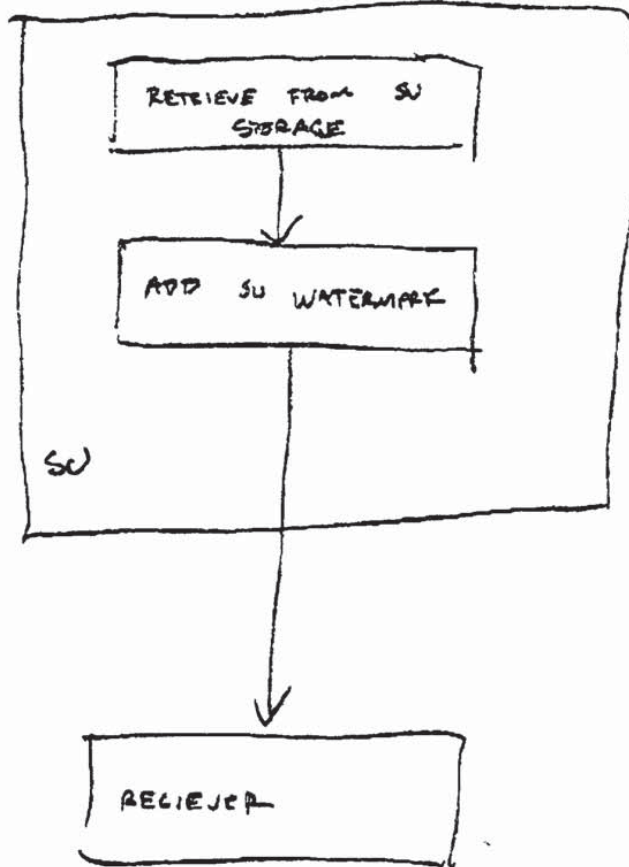
FIGURE 5

CONTENT LEAVING LCS DOMAIN



002290 68HETED9

FIGURE 7
CONTENT LEAVING SU
TO RECEIVER OTHER THAN LCS



000290*68HEF209