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: ***60/147,134***
FILING DATE: ***August 04, 1999***

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:	066112.0133

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

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

TITLE OF THE INVENTION (280 characters max)

A SECURE PERSONAL CONTENT SERVER

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

☒ Firm *or* Individual Name	Floyd B. Chapman, Esq.				
Address	Baker & Botts, L.L.P.				
Address	1299 Pennsylvania Avenue, N.W.				
City	Washington	State	DC	ZIP	20004-2400
Country	USA	Telephone	202/639-7700	Fax	202/639-7890

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification	*Number of Pages*	18	☐ 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		$75.00
☐ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:	[ ]	

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 **August 4, 1999**

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

P19SMALL/REV04

August 4, 1999 066112.0133

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.

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: an advantage and a disadvantage to commercial publishers who face the real threat of unauthorized duplication of their value-added data content. Where cost reduction is an important business consideration, securing payment and authentication of an individual copy of digital information, such as media content, presents unique opportunities to information service and media content providers with the appropriate tools. 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 these parties, or 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 [acoustic (hearing)/psychoacoustic (perceived hearing) or visual (viewing)/psychovisual (perceived viewing)] digital information can be authenticated. This type of verification will become increasingly important for areas where the distributed material relates more to a provided, 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); transaction providers (for example, wholesalers or auction houses). These parties rely on different authentication issues which can be separated and independently quantified or qualified by market participants in shorter periods of time under what is described by the present invention.

Any party who must establish authentication of information that is perceptually-observed, by nature of media content-richness, by users or market

DISH-Blue Spike-246
Exhibit 1013, Page 0003

participants. This information is typically digitized, and may be perceptually based in nature, can easily be copied and redistributed, negatively impacting buyers and sellers or other market participants, in confusing authenticity, non-repudiation, limit of liability and other important "transaction events". In a networked environment, transactions and interactions occur over a transmission line between a buyer and seller, or networked groups of users (Internet communities, closed electronic trading environments, etc.). While network effects may lead to increasing economic utility of the underlying value-added information: in the absolute instantaneous piracy can render the economic value of the good and services being offered to zero, or less than optimal profit positions.

Related situations extend to instances ranging 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 existing prior art by describing optimal combinations of cryptographic and steganographic protocols for "trusted" verification, confidence and non-repudiation of perceptually-based, digitized representations of the actual seller, vendor or another associated institution 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 that are not physically present for the actual transaction, 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. The ability to match information 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—and serves to assist in narrowing and focusing profitable trade between parties. Another 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 and exposure, value-added information is such an asset. By encouraging separate and distinct "trust" arrangements over an electronic network, profitable, market-based relationships can result.

Utilizing the present invention in one of its many embodiments, efficient, openly accessible markets for trade-based information can be made possible. Existing transaction security, including on-line credit card purchasing, electronic cash or its equivalents, wallets, electronic tokens, etc. which primarily use cryptographic techniques to secure a transmission channel but are not directly associated or dependent on the value-added information being transacted or purchased fails to meet this valuable need. The present invention proposes a departure from the prior art by separating transactions from authentication of digitized data. These data may include videos, songs, images, electronic stamps, electronic trademarks, electronic logos used to ensure membership in some

DISH-Blue Spike-246
Exhibit 1013, Page 0004

institutional body whose purpose is to assist in a dispute, limit liability and provide indirect guidance to consumers and market participants, alike.

Buyers' should still beware: but 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 should not only be seller driven through 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 in 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 envisioned in existing closed system. Instead, the flexibility of the present invention's architecture is sure to enable a greater and more diverse information marketplace.

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

A related additional set of embodiments regards the further separation of the transaction and the consumer's identification versus the identification of the transaction only. This is accomplished through separated "trusted transactions" bound by authentication, verification and authorization in a transparent manner. With these embodiments, consumer and vendor privacy could be incorporated. More sophisticated relationships are anticipated between parties, who can mix information about their physical goods and services with a transparent means for consumers, who may not be known to the seller, who choose not to confide in an inherently closed "trusted system" or provide additional personal information or purchasing information (in the form of a credit card or other electronic payment system), in advance of an actual purchase decision or ability to observe (audibly or visibly) the content in the clear. This dynamic is inconsistent with existing systems' 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 (recognition, search engine

DISH-Blue Spike-246
Exhibit 1013, Page 0005

function or find, so-called push, functions), such as the Internet, or means that can be modularized to conduct a transaction based on the present invention (such as WebTV, a Nintendo or Sony game console which can be networked, cellular phone, PalmPilot, etc.) that may have the capability of interconnections with a network of users (including sellers and consumers). Additionally, modularity of price and service desired by the consumer and available by the seller (fixed price, Dutch auction where the consumer fixes a price, auction where a market of buyers and sellers can "decide" a price). 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 value-added information. 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 but the ability to isolate and quantify aspects of an over transaction by module potentially allows for better price determinations of intangible asset insurance, transaction costs, advertising costs, liability, etc. which have physical world precedent. In some embodiments, standardization or government support are surely anticipated, as the physical world will undoubtedly continue to make legal determinations in transactions under dispute.

An important area of the prior art is discussed under the heading of "trusted systems" which architecturally enable users, almost always the publisher or rights owner, to set rules which bind digitized information copies to an inflexible and "containerized" architecture. System security is typically based on persistence of access control over the content in a variety of implementations, with access and subsequent usage being tightly tied into the distribution system. The prior art has many disclosures which fail to mimic the real world and, in effect, eliminate impulse buying, sampling, re-creation of existing works, making a transaction more transparent to consumers, providing for support of both controlled and uncontrolled value-added information within the same system, and other important aspects of information distribution that cannot be predicted in advance of more open consumer access or recognition of the information in question. 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 this content still requires costly advertising that will not be eliminated with an ever-increasing amount of information vying for consumers and other market participants attention. Pricing, when inflexible, and expense limitations in creating recognition of a particular piece of value-added content are inherent to the nature of a market for speculatively valued goods. Where such markets have participants, both buyers and sellers and their respective agents, with access to the same information in real time, market mechanisms efficiently price the market goods or services.

DISH-Blue Spike-246
Exhibit 1013, Page 0006

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 market price where sellers maximize their profits. Quality and quantity provide different evaluation criteria of selection and service relating to the value-added information to be 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.).

One fundamental weakness with systems known to those skilled in the art is the lack of mechanisms to ensure that buyers and sellers can reach pricing equilibrium. This deficit is related to the "speculative", "fashion", "vanity" aspect 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 or choose never to see an actual location with which the transaction is being sought. A physical location may simply not exist. There are number of such virtual operations in business today who 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, as a matter of maintaining "security". 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 in 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 are 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. As well, the separation of the transaction from the exchange of the value-added information, giving 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

DISH-Blue Spike-246
Exhibit 1013, Page 0007

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 ("recognition, recognition, 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 further creativity, competitive marketplace for 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 age vendors—continuing to develop customer relations, trust and profitable sales of their products and services. While the information economy, if largely an anonymous marketplace, is making it much harder to identify consumers "and" sellers alike: a fundamental problem for an information economy. The present invention provides remedies to these weaknesses versus other related systems described in the prior art.

One approach U.S. Pat. No. 5, 892, 900 to Ginter et al., relies on "universal" adoption of a "virtual distribution environment" (VDE) leaving all control over distribution to the publisher, without any flexibility provided to the consumer. The limited flexibility that exists is predetermined by the seller. While in theory this approach appears to offer important advantages in markets where price and product information may be readily available and known to market participants (such as commodities), often the sale and exchange of "value-added information", itself, is speculative. Absent open access to said data by consumers or other market participants (aggregators, distributors, wholesalers, financial interests, etc.) leaves a condition of indeterminable valuation, or even underexploitation of the intangible information asset.

While Ginter et al. discusses "persistence" of the separation between rights applications and the foundation of the VDE, what results is a strict set of control which unnecessarily limits potentially useful and economically beneficial access by those potential purchasers who do not choose to rigidly make decision solely on price. The pricing structure has no relationship with the underlying value-added data, only the predetermined rules governing the use of the content is anticipated. Additionally, the architecture replaces one set of controlled distribution with another in the form of a proprietary VDE distribution channel or channels; preservation of a "virtual black box" limits the free flow of content,

DISH-Blue Spike-246
Exhibit 1013, Page 0008

and information about that content, that actually exists to the commercial benefit of media content owners.

The present invention concerns itself with higher economic efficiencies by preserving an open architecture that is focused primarily on authentication, verification and authorization of value-added information: access restriction is not a primary goal. Thus, failure of authentication or verification do not constitute a security failure within the context of the present invention as it would with Ginter el al. Moreover, legacy media which may exist as physical media such as CDs, LaserDiscs, MiniDiscs, photographs, PhotoCD, VHS, Digital Video, etc., pre-recorded or otherwise, or other unsecure tangible recorded media is not excluded by fiat. Consumers are given flexibility in their choice of recording media, content characteristics such as quality, time of delivery, etc.: publishers are still assured payment and also benefit from better information flow to and from the marketplace. This is not possible with Ginter et al. because information is used and accessed in only "authorized ways".

Another series of related systems, are US Pat. No. 5,715,403, US Patent No. 5,634,012, US Pat. No. 5,629,980 all to Stefik, propose associations between "usage rights" and a digital work. While these system offer arguably more flexibility in enabling different rule sets for different proposed digital distribution channels, all digital works have permanently attached rights. And all transactions must be coupled to a repository. It is not clear that affixing rights to content necessarily aides sellers or owners of content, especially if the consumers or other participants in the market find use in the information not known by the seller at the time rights were affixed. Unlike, physical media sold and exchanged, limited only by the "format" (CD, MiniDisc, cassette, LP, for examples in music) or "player" (respectively, CD player, MiniDisc player, cassette player, LP player, for examples in music, more generally a reader which connects to a transducer) chosen by consumers, the digital works must always pass through a repository. While this favors owners of digitized media, the proposed technologies cannot handle any legacy media or media which will undoubtedly remain unsecure even with an increasing number of digitized works being made available to consumers. Not all publishers choose to restrict their data, but the format must be readily acceptable for consumers to make purchase decisions. Additionally such transactions create situations where the information in the digital work has the appearance of being obscured by the rights and usage rules attached and coupled to a repository. The present invention alleviates the main concern of publishers, that they get paid for their value-added data while seeking to maximize their profits, because the security is obscured through steganography (digital watermarking in particular), and only authentication protocols are necessary to effect a transaction. This leaves consumers less suspect of the system or seller and enables the development of relationships based on trust between parties, not between a consumer and a closed system.

Copied - Serial No. 09/644,779

DISH-Blue Spike-246
Exhibit 1013, Page 0009

Simply, the nature of information, that it wants to be free, is not equivalent to the desire of creators of intellectual property (such as a copyrights, design, value-added datum) to maximize the commercial value of his work by economic incentives. But legal concepts such as "fair use", "first sale doctrine", and "copyright" are necessarily gray areas that should remain open so as to increase the potential growth in an information marketplace that is both robust and competitive; e.g., both buyers and sellers are satisfied. The present invention de-couples the value-added information media from the underlying distribution mechanism by emphasizing authentication, verification and authorization independent of the transaction mechanisms which are persistently included in the prior art. Consumers benefit with the present invention, because the processes envisioned more closely resemble real world exchange of content and other value-added data. The prior art is limiting in that consumers are not trusted, trust is "held" or "escrowed" in an inflexible system. Instead of relationships with consumers, these systems mandate relationships with protocols.

US Pat. No. 5,638,443 and US Pat. No. 5,530,235 both to Stefik et al. seek to alleviate problems in determining the contents of value-added data and enabling a system of repository-stored "composite digital works". The deficiencies of these two applications lie in the restriction of access by consumers to media or other value-added data, and prevent legacy media or unsecure, non-content revealing storage media to be inaccessible without any increased benefit to any given publisher. For recognizable digital works, these complementary systems may offer some limited benefits in access control, but they do not allow for interactions with unsecured or existing legacy media files, as they exist in the real world, or as contemplated under the present invention. Further, the system may give the appearance to consumers that they cannot be trusted. The present invention seeks to "keep honest people honest".

Another approach which is arguably less stringent than the "trusted systems" and "secure containers" in the art is that disclosed in US Pat No. 5,673,316 to Auerbach et al. Auerbach et al. disclose a means for restricting access to digital information by breaking information parts and associating encryption keys for these parts. The parts form a cryptographic envelope with related part encryption keys (PEKs) which predetermine access, control and distribution of the digital data, based on pre-determined terms and conditions. In essence, Auerbach is using the "open nature" of public key cryptography and its "scalable" infrastructure but based on pre-processing of data to enable secured access. The implicit assumption is that sellers benefit from "superdistribution", meaning so long as a rights owner is paid no other factor in a transaction for media is valuable to the seller. The present invention seeks to bring buyers and sellers closer together for beneficial economic relationships, not distance them with predetermined rules for purchase and use. Because the PEKs must be permanently associated with the digital information, again, as with the above mentioned prior art, legacy media in pre-recorded format (CD, Laser Disc,

DISH-Blue Spike-246
Exhibit 1013, Page 0010

PhotoCD, Nintendo, etc.) cannot be effectively leveraged, nor can unsecure media in the future coexist in a consistent manner to the benefit of both the publisher and consumer. It would not be possible to successfully authenticate the content unless all content passed through Auerbach et al.'s contemplated embodiments. While publishers may certainly choose to limit access to their value-added data, the present invention offers a unique means to leverage the overall commercial value of such works by incorporating open authentication, verification and authorization protocols and allowing co-existence of legacy media. Moreover, the present invention does not change the file's format as does Auerback et al. The present invention accomplishes this with cryptographic (for confidence, authentication and data integrity) and steganographic (for tamperproofing, authentication and content-based embedding security) protocols seeking to isolate a transaction from exchange of value-added data at various content characteristic-based quality levels.

Some further related prior art includes US Pat. No. 5,412,718 to Narasimhalu et al. disclose a means for utilizing storage medium "nonuniformities" which are processed as a signature for any particular storage medium and its subsequently generated cryptographic signature. Although this represents a form of copy protection security, more robust techniques in the art, including those by the present inventor, are better able at securing, authenticating and maintaining content quality—namely digital watermarks. The present invention is not storage medium-based, but portable and scalable in authentication and distribution of value-added media. Bright el al. disclose, in US Pat. No. 4,262,329, means for maintaining all cryptographic processes in a secure "vault". This example of prior art is more restrictive than many "trusted systems" disclosures, and thus suffers from the same weaknesses described above. US Pat. No. 5,287,407 to Holmes suggests a means for software copy protection. To the extent that tools are now available to rid any non-cryptographically embedded data in a file without adverse repercussions is a weakness that is overcome with digital watermarking techniques for both content (digital sampled content) and functional software (zero error tolerance). The present invention relies on content quality degradation as well as verification of authentic value-added information as important facets in increasing the benefits of both buyers and sellers of value-added data. US Pat. No. 5,191,573 and US Patent No. 5,675,734 both to Hair, describe a means for distributing audio or video signals. The present invention offers the improvement on this art, and related systems, in separating the transaction function from the delivery functions. The present invention also has mechanisms for ensuring payment, authentication of the content signal, and the ability to handle secure and unsecure information in a consistent, secure manner.

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

DISH-Blue Spike-246
Exhibit 1013, Page 0011

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 which can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. Known in cryptography 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 into and out of itself.

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: Created with a one-way hash function (similar to a human fingerprint) or instead, incorporating the hash with a message into a signing algorithm will create a signature scheme.

Value-added:

DISH-Blue Spike-246
Exhibit 1013, Page 0012

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: Called "integrity", in cryptography, an intruder should not be able to substitute false messages for legitimate ones; the receiver of the message (embedded or otherwise within the value-added information) should be assured that the message (or by effects, the origin of the carrier within which the message is stored) that the message was not modified or altered in transit.

One way hash function: One-way hash functions are defined by the fact that the output does not depend on the input in any way.

Authorization:

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.

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.

DISH-Blue Spike-246
Exhibit 1013, Page 0013

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 wiped content 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 and commercial interests in the content than to consumers). Ideally, as previously disclosed, security should not obscure the content, nor prevent market participants from accessing information, and longer term, developing trust or creating 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).

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

DISH-Blue Spike-246
Exhibit 1013, Page 0014

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 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. If the content came from a LCS, the SU must also add the hash received from the LCS to the watermark. 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....

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"

DISH-Blue Spike-246
Exhibit 1013, Page 0015

Figure 5 is a diagram of a service and support module
Pricing of bandwidth patent reference...
Benefits of: bidirectionality and asymmetry in enabling a "trusted transaction"

Path 1: This path is a secure distribution of digital content. 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 might have the capability to receive from multiple SECD's, where each might use a different security protocol. The security protocol uses a asymmetric cryptographic system, an example being a public key cryptography system where there are private and public key pairs, to allow the LCS to authenticate and accept the received content. (signature schemes may also work) The transaction would have the following steps.

1.) The user would make a connection to the SECD, make a selection, and complete a sale. (note: sales security can be entirely separate, explain)

2.) The LCS would send its public key to the SECD.

3.) The SECD would use the LCS public key to initialize the transmission security.

4.) The SECD would transmit the secured content to the LCS.

5.) The LCS would receive the content, authenticate that it was unchanged during transmission by a watermark and hash check, and unpack it from its security wrapper (which could include a secured transmission line, such as SSL). If the content can be authenticated, the content would be accepted into the LCS domain. Otherwise, it would 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

DISH-Blue Spike-246
Exhibit 1013, Page 0016

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.

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).

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.

DISH-Blue Spike-246
Exhibit 1013, Page 0017

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.
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.

DISH-Blue Spike-246
Exhibit 1013, Page 0018

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.
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

DISH-Blue Spike-246
Exhibit 1013, Page 0019

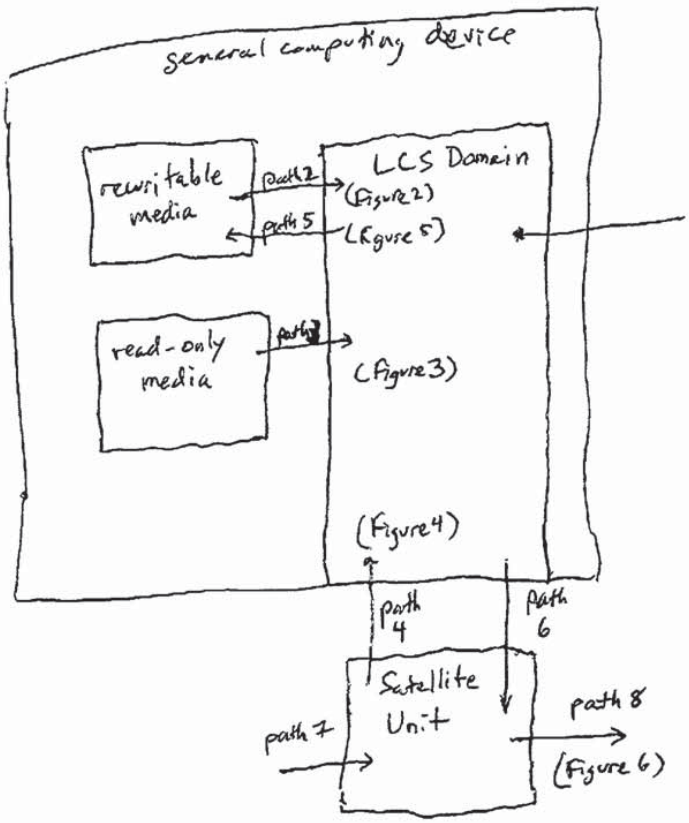
between the LCS and a SU must be on an authenticated, secure channel; and h) All export paths on SU's are secured.

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

Confidential - Attorneys' Eyes Only

Figure 1

Local Content Server
(general computing device)



SECD
via
telecommunications
link
(Internet
Electric Power grid
POTs
Cable
Satellite
wireless
etc
⋮)

DISH-Blue Spike-246
Exhibit 1013, Page 0021

EXTRA FIG. 1

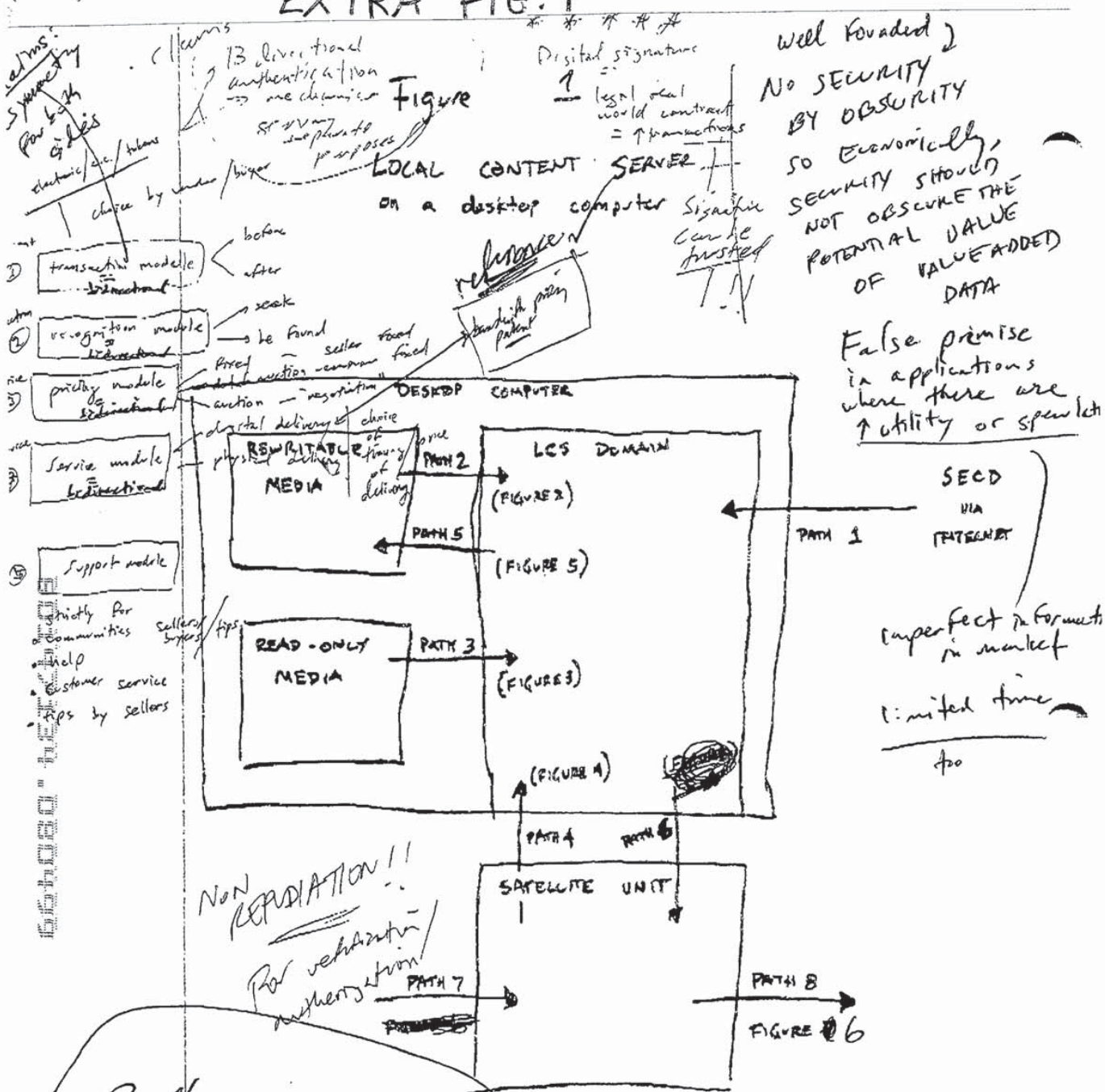


Figure
LOCAL CONTENT SERVER
on a desktop computer
Digital signature
legal real world contract = ↑ transactions
Signature can be trusted
Well founded
NO SECURITY BY OBSCURITY
SO ECONOMICALLY, SECURITY SHOULD NOT OBSCURE THE POTENTIAL VALUE OF VALUE ADDED DATA
False premise in applications where there are ↑ utility or speculation
transaction module
before
after
recognition module
seek
be found
pricing module
fixed
seller fixed
auction
negotiation
digital delivery
choice of timing/price of delivery
physical delivery
service module
support module
strictly for communities
help
customer service
tips by sellers
sellers/buyers/tips
DESKTOP COMPUTER
REWRITABLE MEDIA
PATH 2
(FIGURE 2)
PATH 5
(FIGURE 5)
LCS DOMAIN
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
PATH 7
PATH 8
FIGURE 6
NON REPUDIATION!!
For verification/authorization
Bundle secure player w/ service of music download?
Buyer – seller watermarking protocol based on amplitude modulation and the E-Gamal public key cryptosystem
Memon, et al

Figure 2.

CONTENT ENTERING LCS DOMAIN FROM REWRITABLE MEDIA

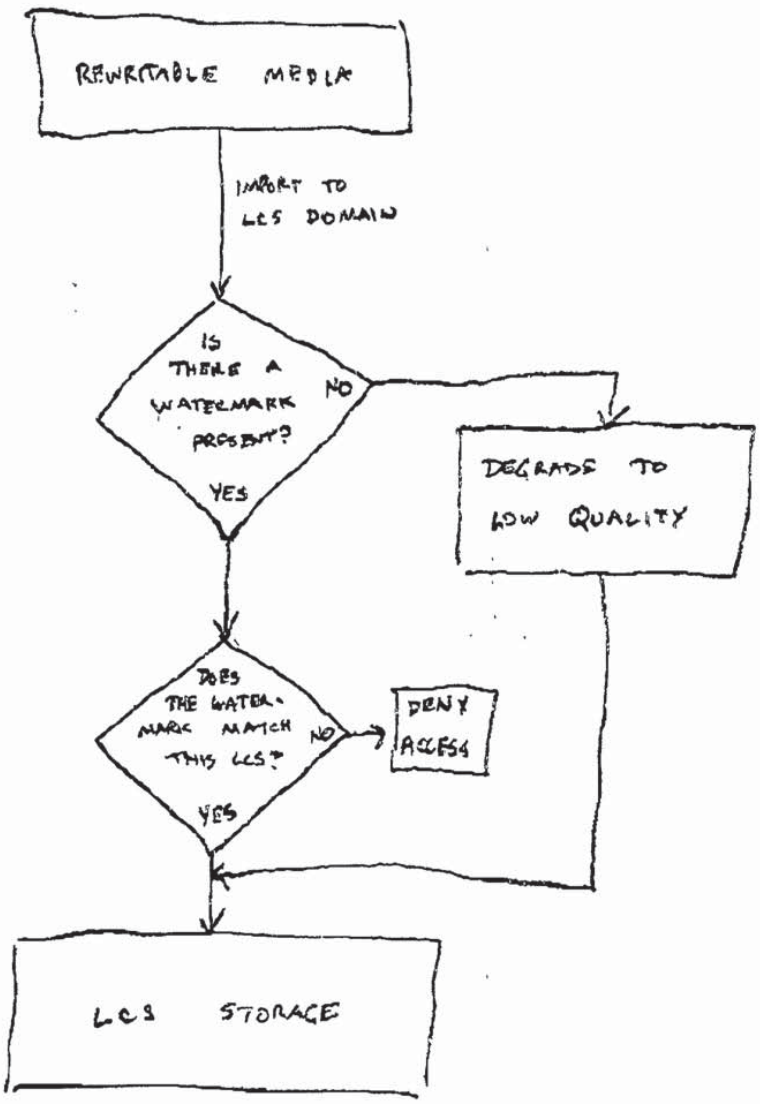


FIGURE 3

CONTENT ENTERING LCS DOMAIN
FROM READ-ONLY MEDIA

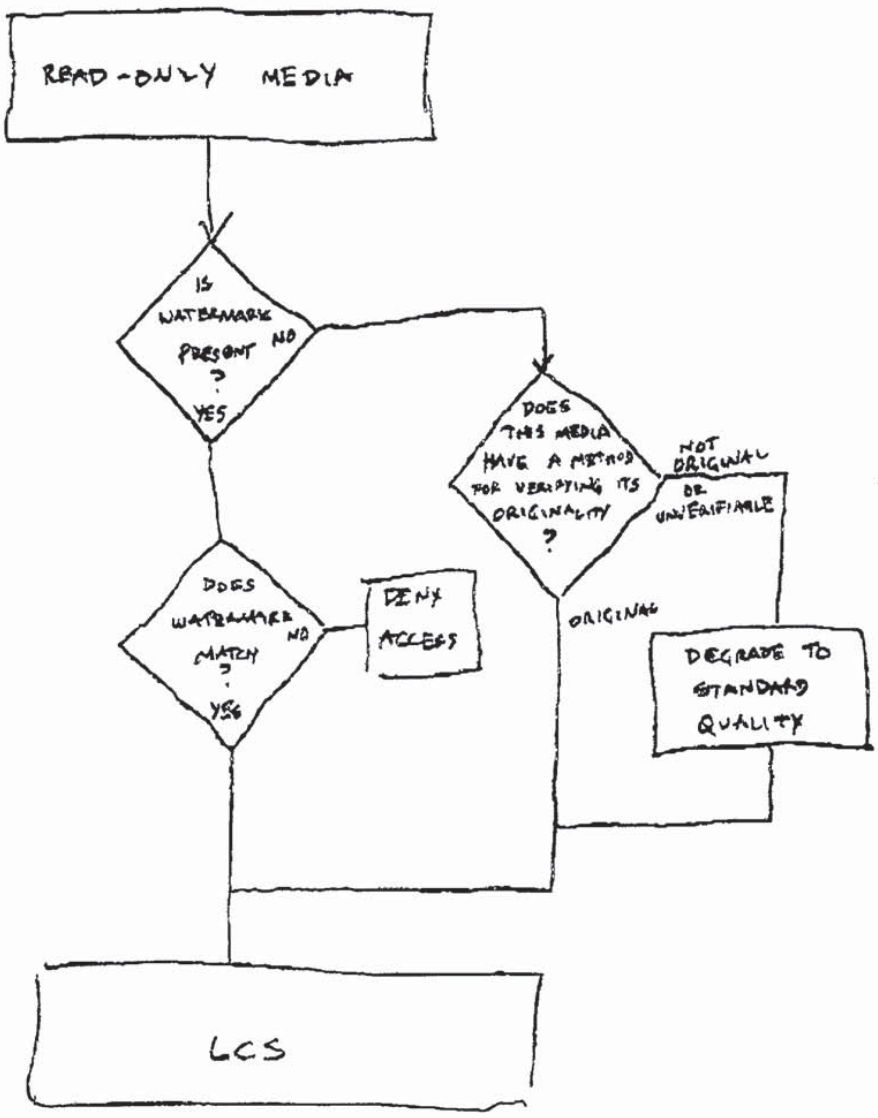
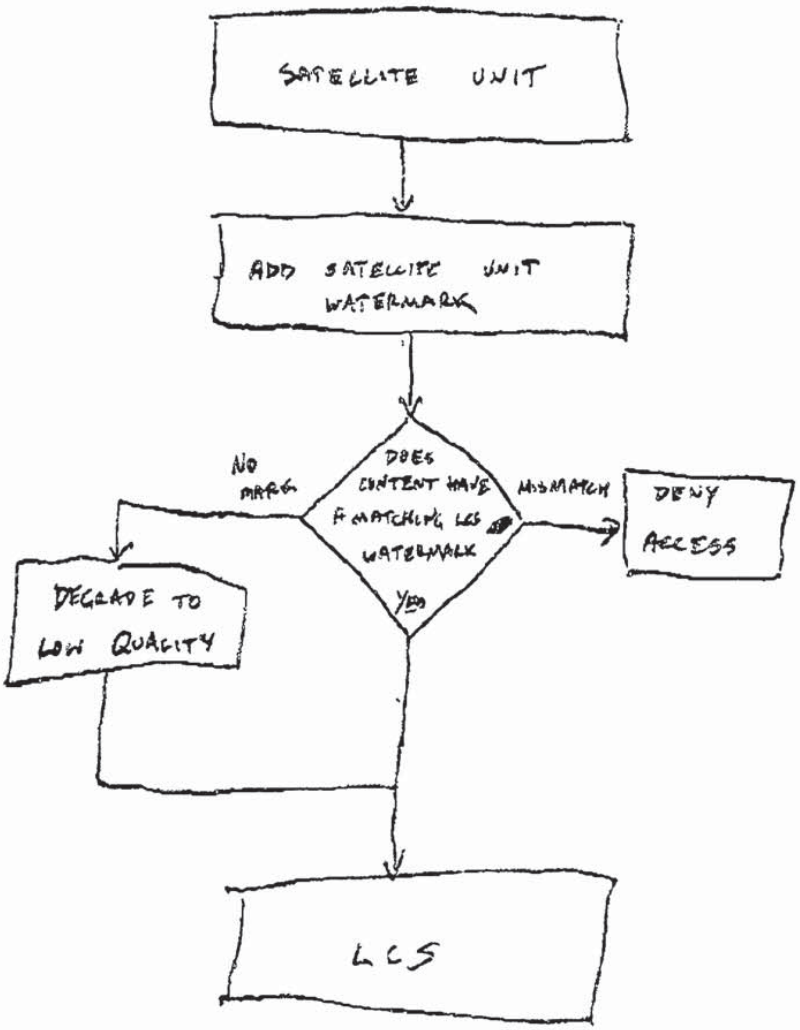


FIGURE 4

CONTENT ENTERING ECS DOMAIN FROM SATELLITE UNIT



DISH-Blue Spike-246
Exhibit 1013, Page 0025

FIGURE 5

CONTENT LEAVING LCS DOMAIN

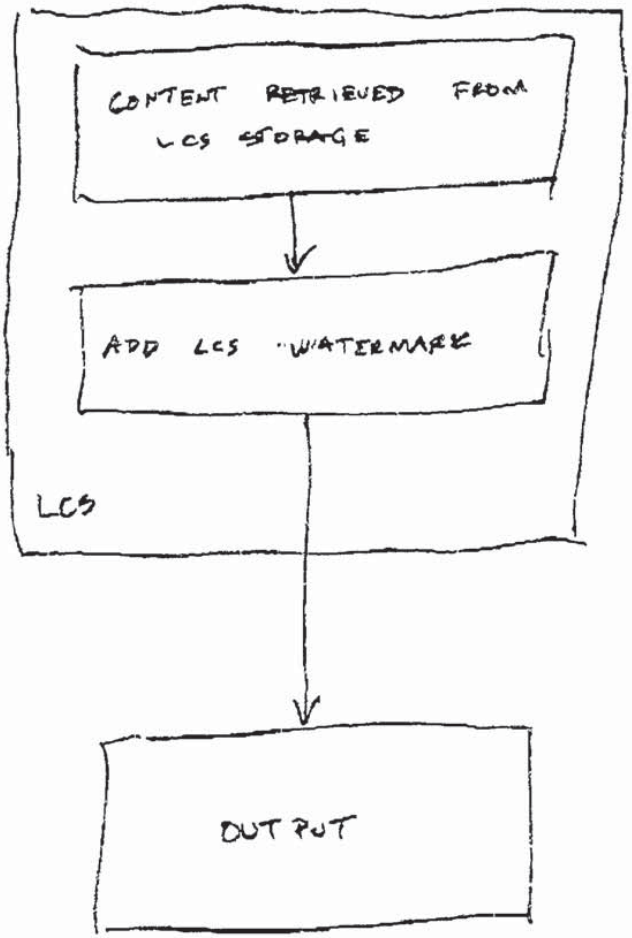
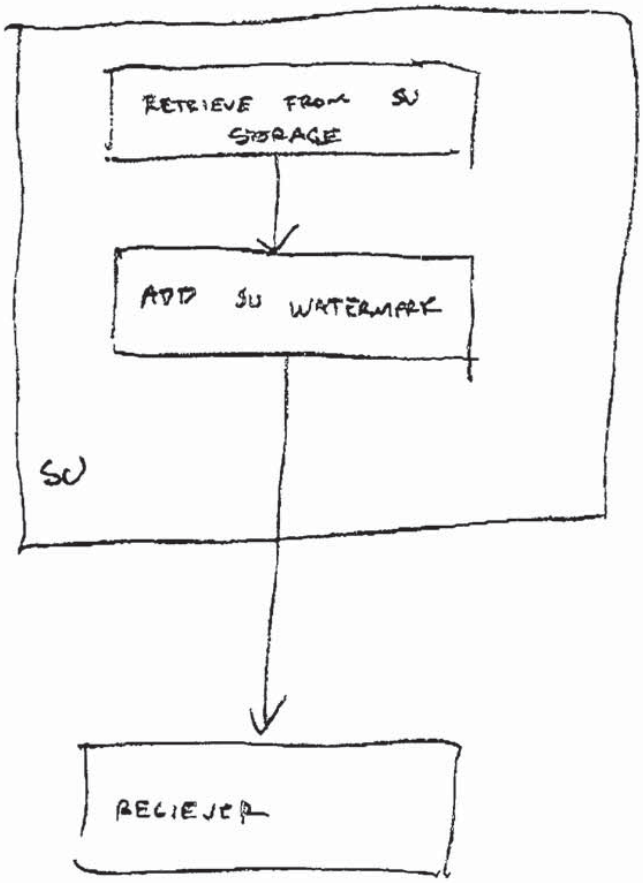


FIGURE 7

CONTENT LEANING SU

TO RECIEVER OTHER THAN LCS



DISH-Blue Spike-246
Exhibit 1013, Page 0027