(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2001 (22.02.2001)

PCT

(10) International Publication Number
WO 01/13310 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/22823

(22) International Filing Date: 18 August 2000 (18.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/149,826	19 August 1999 (19.08.1999)	US
60/162,591	29 October 1999 (29.10.1999)	US
09/641,357	17 August 2000 (17.08.2000)	US

(71) Applicant and
(72) Inventor: **JASRASARIA, Suresh, K.** [US/US]; 115 Blanchard Road, Boxboro, MA 01719 (US).

(74) Agents: **COHEN, Jerry** et al.; Perkins, Smith & Cohen, LLP, One Beacon Street, 30th Floor, Boston, MA 02108 (US).

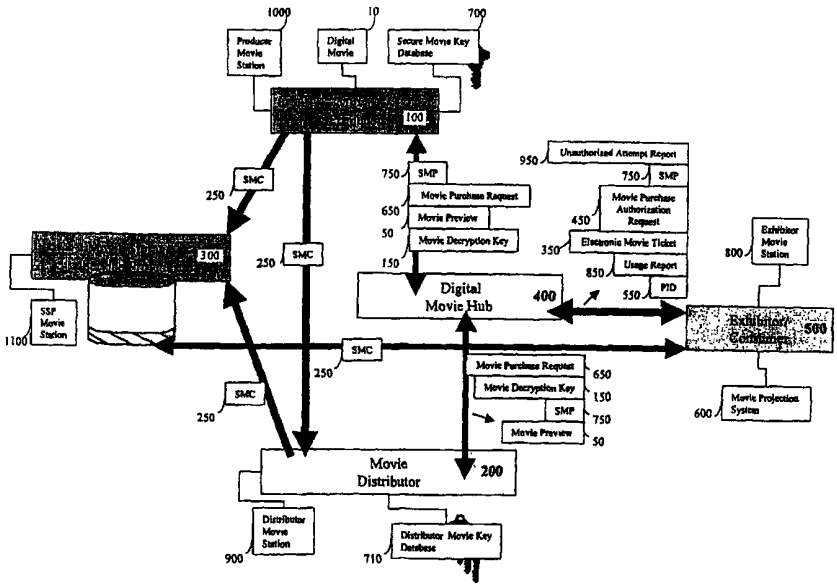
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR SECURE DISTRIBUTION AND ON-LINE ELECTRONIC USAGE MANAGEMENT



(57) **Abstract:** Disclosed is a system and methods for secure distribution of digital content (see the figure). The content is digitized and encrypted forming a secure content container (250). The decryption key (710) and means to authorize the presentation or playing of the material are provided to form a secure player system (750). The content will be limited by a series of negotiated restraints including number of presentations, time of presentation and geographic and/or type of audience limitations. A specific player or projector (600) is physically enabled by the secure player system and ensures that the limitations are met. The system sends a message to the provider upon unauthorized access to the content. The system may deactivate and/or destroy a local copy of the material upon misuse.

WO 01/13310 A1

METHOD AND SYSTEM FOR SECURE DISTRIBUTION AND ON-LINE ELECTRONIC USAGE MANAGEMENT

BACKGROUND OF THE INVENTION

This invention relates generally to systems and methods for secure distribution over the Internet or other such communications networks and for on-line electronic usage management of digital content.

As the world around us increasingly becomes digital and connected, businesses and consumers are getting more comfortable and savvy about leveraging the technology and using the Internet to download digital content. Many businesses and consumers are downloading the digital content just for electronic use - without printing or without converting it into any other physical form. For example businesses and consumers can download digital books, newspapers and magazines, digital images, digital audio, and digital cinema. They can use this downloaded digital content for such on-line use like reading digital books, newspapers and magazines, displaying digital images on digital screens for advertisements and in-mall promotions, listening or broadcasting the digital audio, exhibiting the digital cinema for entertainment and viewing the digital cinema content from daily shootings for editing and commenting. When such digital content is copyrighted, the content creators and providers need to ensure that distribution of such content is controlled and their property rights are protected.

It is an object of this invention to reliably control the distribution of digital content.

It is still another object of the present invention to control electronic on-line usage of digital content.

It is another object of the present invention to allow electronic on-line use of digital content by authorized businesses or consumers solely for the amount of time or the number of times authorized by the digital content provider.

It is also an object of the present invention to secure and protect digital content from intrusion during distribution.

SUMMARY OF THE INVENTION

The objects set forth above as well as further and other objects and advantages of the present invention are achieved by the embodiments of the invention described herein below.

The present invention provides architecture for systems and methods for secure distribution and authorized usage of digital content. The proposed architecture results in a system with built-in scalability.

The entire digital content distribution scheme, including the transport of the digital content and the transport of usage management information, mentioned in a preferred embodiment of this invention works over a communications network, such as the Internet, using a broadcast medium or a point-to-point transmission medium. Moreover, in the same preferred embodiment, depending on the size, suitability and cost factors, the secure transport of usage management information can take place over a communications network, such as the Internet, and the digital content can be securely delivered using a combination of a communications network, such as the Internet, and a distribution network, such as FedEx, of a physical medium, such as flash memory cards, erasable magnetic or optical disks or holographic

disks which can store, for example, more than 100 gigabytes on one disk platter.

Although authorization and transfer of digital content takes place between a digital content provider and a business or a consumer, the systems and methods described in this invention do not prohibit the use of intermediaries like business-to-business (B2B) or business-to-consumer (B2C) electronic commerce Internet hubs and portals. In fact, using such intermediaries is a preferred embodiment for implementing the proposed systems and methods of this invention.

In a preferred embodiment of this invention, the businesses and consumers have uniquely numbered specific Internet appliances like uniquely numbered digital readers for displaying digital books, digital magazines and digital newspapers, uniquely numbered digital stereo systems for playing digital audio and uniquely numbered digital video projection systems for screening digital cinema. These Internet appliances also have electronic storage and playback capability to store and play the digital content that will be consumed on-line.

The systems of this invention use encryption for security of the digital content during distribution as well as during consumption by the appliance used by the business or consumer. The usage meter is not included in the content. The usage meter is included in a digital content player (DCP), a software program that can be executed only by authorized personnel and authorized appliances.

Upon successful on-line usage or consumption of the digital content as per the agreed upon limitations of presentations or playing of the content, the DCP may allow the business or consumer to further extend the content usage or destroy (or disable) the DCP and/or the content itself. The DCP also sends a report to the digital content providers. This allows the content providers an opportunity for repeating the authorization (sale),

balancing their books for usage authorized (product sold), as well as collecting usage information (feedback) for future marketing and new product creation.

Furthermore, unauthorized access to the digital content or the digital content player (DCP) may cause self-destruction as described above and an unauthorized attempt report is sent to the content providers. This allows the content providers to put alerts in their system to automatically restrict future access or sale of content to unsecured or unclean intermediaries, businesses and consumers.

A preferred embodiment of the invention includes methods for encrypting a digital movie, distributing the encrypted digital movie, authorizing a user for projection of the encrypted movie, enabling a movie projector to decrypt the movie, verifying the user and the enabled movie projector, and exhibiting said movie on said enabled movie projector.

A system for distributing and playing digital movies includes an encrypted digital movie, one or more decryption key(s) for the movie, a movie player program, means for providing the encrypted movie and the movie player program to a user for exhibiting the movie on a projector, means for enabling the movie player program, means for authorizing the user and the projector, means for verifying the authorized user and the authorized projector, and means for decrypting and exhibiting said movie on said authorized projector. A distributed secure digital movie distribution system includes:

- A movie producer data processing system with software applications that generate a secure digital movie, a distributed and replicated secure database of movie encryption and decryption keys and algorithms, and secure digital movie players.
- A digital movie distributor data processing system with software applications for marketing and selling digital

movies to consumers and exhibitors, transporting secure digital movies and their players to the consumers and exhibitors, monitoring and scheduling exhibition, metering digital movie usage and doing credit and collection from exhibitors.

- A movie exhibitor data processing system with software applications to buy or license digital movie for exhibition, conduct box office collection from consumers, exhibit digital movie and provide feedback to movie producers and distributors.
- A movie storage service provider data processing system with software applications for storage and asset management of digital movies and on-demand transport of digital movies to exhibitors/consumers.

For a better understanding of the present invention, together with other and further objects thereof, reference is made to the accompanying drawings and detailed description and its scope will be pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic block diagram of the inventive system;
FIG. 2 is a flow chart for generating a secure movie container;
FIG. 3 is a flow chart for generating a secure movie player;
FIG. 4 is a flow chart for executing a secure movie player;
FIG. 5 is a schematic block diagram of a secure movie projection system; and
FIG. 6 is the format of entries in a secure movie key database.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

This invention can be applied in multiple types of digital content producer-consumption scenarios. Depending on the content and the usage pattern the following are examples of preferred

embodiments of the present invention, although these examples are not to be construed as limiting the invention.

A. Secure distribution and usage management system for digital cinema and digital music. The digital content player (DCP), a software program, in this case meters the usage on the basis of number of times played during a specified elapsed time.

B. Secure distribution and usage management system for digital newspaper, digital magazine, digital books, digital advertisements and digital cinema trailers, and digital cinema dailies (the end of the day footage sent to various consultants for editing and feedback). The DCP, a software program, in this case meters the usage on the basis of elapsed time.

For a clear understanding of this invention, reference is now made to FIG. 1 of the drawings. Regarding item A above, FIG. 1 shows a secure digital movie distribution and usage management system. Using a Producer Movie Station 1000, a movie producer 100 (independent filmmaker or a major motion picture studio) registers its digital movies 10 with a digital movie hub 400 (hereinafter referred to as the hub). During registration the movie producer 100 provides the hub 400 with a movie preview 50 and a decryption key 150 that must be used to decrypt the encrypted digital movie 10 by the exhibitor/consumer 500 who purchase the movie for exhibiting. The movie producers 100 may decide to store the encrypted digital movies 10 at their own magnetic and/or optical disk farm (not shown), or in a more likely scenario, send the encrypted digital movie 10 as a secure movie container (SMC) 250 to a movie storage service provider 300 who rents out large farms of magnetic and/or optical disks to movie producers 100.

The exhibitor 500, who has a secure movie projection system 600 buys an electronic movie ticket 350 (hereinafter referred to as the ticket) from the hub 400 for exhibiting a movie. The ticket

350 grants the exhibitor 500 the rights to exhibit the movie N times within a time period T from the time of the ticket 350 purchase.

To obtain a ticket 350 the exhibitor 500 interacts with the hub 400 through an exhibitor movie station 800. The exhibitor 500 sends a movie purchase authorization request (MPAR) 450 to the hub 400. The hub 400 communicates with the exhibitor movie station 800 to obtain the unique projector identification descriptor (PID) 550 of the movie projection system 600 at the exhibitor premises. The hub 400 then returns a ticket 350 that is used by the exhibitor movie station 800 to exhibit the movie.

The movie exhibitors 500 can obtain the movie tickets 350 in various ways: they can pay for the movie ticket 350 upfront by entering their credit card number or they can obtain the movie ticket 350 by entering their account number, if they are preferred users of the hub 400. Using the digital content player (DCP) the system can also accommodate a box office revenue sharing type of payment method before issuing a movie ticket 350. As the lion's share of the box office revenue is collected before the show begins, the pre-negotiated box office revenue split must be electronically transferred to the movie producer 100 just before the show begins, then and then only the system will release the authorization to the DCP to exhibit the movie.

Once the hub 400 issues a movie ticket 350 (either after obtaining an authorization from the credit card provider or after making an entry in its general ledger for a preferred user), it sends a movie purchase request (MPR) 650 to the movie producer 100. Upon receiving the MPR 650, the movie producer generates a secure movie player (SMP) 750 that is a software player uniquely and specifically programmed based on the information contained in MPR 650 received from the hub 400. The movie producer 100 then sends the SMP 750 to the hub 400 who in turn sends it to the exhibitor movie station 800 that has a secure connection to the

movie projection system 600. The SMP 750 can only play the designated movie on the secure movie projection system 600 for N times before the time T expires.

The SMP 750 contains the location (for example the name of the web site) and the instructions allowing the exhibitor to obtain the SMC 250. In the event that sufficient movie tickets 350 are issued for a movie, the movie producer 100 may decide to broadcast the movie at a specified time. Those exhibitors/consumers 500 who have obtained the movie tickets 350 and whose premises are equipped with broadcast reception hardware can receive the SMC 250 containing the movie. A SMP 750 can enable this to happen automatically under software control. Moreover, if the movie has already been released on a physical media like a secure digital cinema disk (DCD), the SMP 750 can also obtain the SMC 250 from the secure DCD.

Upon successful exhibition of the movie, the SMP 750 may allow the exhibitor/consumer 500 to further extend the expiration time period T and/or the number of exhibitions N for playing the movie. If no extension is desired, the SMP 750 disables itself and/or the SMC 250 and sends a usage report 850 to the hub 400.

Any unauthorized attempt to access SMC 250, which is sensed by the software in the SMP 750, ends in self-destruction of the SMP 750 and/or the SMC 250 and an unauthorized attempt report 950 is sent to the hub 400. This allows the hub 400 to put alerts in its system to automatically restrict future access or sale of digital movies 10 to unsecured or unclean exhibitors 500.

The hub 400 aggregates all the usage reports 850 and unauthorized attempt reports 950 and makes them available to appropriate entities under password control. Movie producers 100, movie exhibitors/consumers 500 and movie storage service providers (SSP) 300 can use these reports for their future operations including marketing and new product creation.

Still referring to FIG. 1, in the above example, an intermediary like a movie distributor 200, who acquires the rights to distribute the movie in digital format, can also play its traditional role of marketing and distributing the movie. A distributor movie station 900 when used in conjunction with the hub 400 and the storage service provider 300 can make the role of a distributor 200 much more efficient and streamlined by providing such services as:

- Collaboration with exhibitors/consumers for licensing a movie for exhibition;
- Secure duplication and transportation of a digital movie 10 to exhibitors/consumers;
- Credit and collection from exhibitors/consumers;
- Creating multiple versions of a movie based on language, rating and length of time;
- Sending electronic marketing and promotion materials of a movie to exhibitors/consumers;
- Disseminating trailers of movies to targeted exhibitors/consumers; and
- Collecting movie feedback from exhibitors/consumers.

The systems and methods of secure distribution of a digital movie 10 described in the preferred embodiment of this invention will, on one hand, accelerate the acceptance of a good movie, however, on the other hand a bad movie will die quickly. This system and method will also have a similar effect on the role of a movie distributor 200. On one hand it will expand the reach of a movie distributor 200 beyond the traditional distribution to theatres into all other channels of distribution including consumers on the day a movie is released. However, on the other hand a movie producer 100 can disinter-mediate a movie distributor 200 by self marketing and distributing the movie in conjunction with the services offered by the hub 400 and the movie storage service provider 300.

As shown in FIG. 1, the distributor movie key database 710 can now be used to restrict the distribution rights of movie distributor 200 to a specific geography or to a specific channel of distribution. While interacting with the rest of the entities in the system, the distributor 200 has a role similar to that of a movie producer 100. Like a movie producer 100, a movie distributor 200 may also register its movies with the hub 400. Movie distributors 200 may decide to store the digital movies 10 at their own magnetic and/or optical disk farm (not shown), or in a more likely scenario, obtain the services of a movie storage service provider 300. The only difference between the producer 100 and the distributor 200 in this context is that the producer 100 holds the secure movie key database 700 whereas the distributor 200 only has keys from the distributor movie key database 710 that expire after a certain time period or are restricted to a specific geography or a specific exhibition channel. This allows the movie producer 100 to have enhanced security and a complete long-term control of the digital movie 10. Movie producers 100 can thus concentrate on creating new movies and not worry about the marketing and distribution headaches.

The above systems and methods provide an end-to-end description of a complete on-line movie transaction. As a result of this transaction the exhibitor 500 gets to exhibit the movie N number of times in a specified period T, the movie producer 100 gets the usage reports 850 or a predetermined payment for each exhibition of the movie, the SSP 300 and the hub 400 get paid by the producers 100 or the distributors 200 for their services. The above system also allows for roles to be played by movie distributors 200 and movie storage service providers 300.

Currently there are many digital movie 10 formats as well as compression and encryption mechanisms that are known in the industry. Each implementation is unique. Thus, a number of different standards exist for creating secure movie containers

SMC 250 and secure movie players SMP 750 of digital movies 10. This requires hardware manufacturers to build secure movie projection system 600 appliances such that these appliances can play digital movies 10 from multiple SMC 250 and SMP 750 standards, much like today's 35 mm movie projection hardware that can project a 35 mm movie print of any movie.

Provided below is a more detailed description of the major components of the methods and systems of the preferred embodiment of this invention.

Digital Movie 10

A digital movie 10 is a movie that is made by using a digital movie camera and storing the captured images on a digital media like a magnetic tape or a hard disk. A digital movie 10 may also refer to a movie that is captured on a film and later digitized using currently available digitization equipment and storing the resulting data on a digital media like a magnetic tape or a hard disk. A digital movie 10 is often simply referred to as a movie in this document.

Movie Producer 100

A movie producer 100 could be a major motion picture studio or an independent filmmaker. In the context of this invention, a movie producer 100 uses the producer movie station 1000 to perform the following tasks:

- A movie producer 100 keeps an up to date secure movie key database 700 of all digital movies 10 it has released including their titles, their encryption keys, their compression methods and the location of their SMCs 250. The movie producer encrypts this database and stores it in a highly secure manner. This database is distributed and replicated for maximum security and availability. The number of encryption keys used for each movie can vary depending on the strategy employed, for example a movie producer 100 may

decide to use an encryption key for every two-minute segment of a movie.

- A movie producer 100 registers each of its movies with the hub 400 by sending the hub a movie preview 50 and a movie decryption key 150.

- Upon receipt of a movie purchase request 650 for a digital movie 10 from the hub 400 the movie producer 100 uses the decryption key 150, and the various information contained in the movie purchase request 650 to generate a SMP 750 for the movie. The movie producer 100 then sends the SMP 750 to the hub 400 who in turn delivers the SMP 750 to the exhibitor 500 who purchased the movie. The SMP 750 is username-password protected.

- Once a movie has been exhibited, the movie producer 100 can view the usage report 850 at the hub 400 and settle the payment for N screenings of the movie with the hub 400. As described before various payment methods, including box office revenue split can be implemented by using the SMP 750.

- The producer movie station 1000 in conjunction with the hub 400 is also used to collaborate with distributors 200 to negotiate a distribution agreement.

Movie Distributor 200

A movie distributor 200 is an entity that has bought the rights to distribute a digital movie 10 from its producer 100 to the exhibitor 500. In the context of this invention, a movie producer 100 may sell the rights to distribute the SMC 250 of a specific digital movie 10 to a movie distributor 200. These rights can be for a specific period of time or for a specific geography or for a specific exhibition channel. The distribution rights for digital movies 10 can be very specific and are easy to administer

because the SMP's 750 that are can be programmed to monitor the distribution rights of a movie distributor 200.

Movie Storage Service Provider 300

A movie storage service provider 300 is an entity that maintains a large farm of magnetic or optical disks and rents the storage space to movie producers 100 and movie distributors 200. Such storage must be high performance, highly secure and always available - 24 hours a day, 7 days a week. A movie storage service provider 300 may have to store multiple copies of a movie in geographically separate strategic locations in separate time zones around the world. A movie storage service provider 300 should also deploy disaster tolerance techniques to satisfy the varying degrees of performance, security and availability requirements of storing SMC's 250.

In the context of this invention, a movie storage service provider 300 should also have high-speed Internet connections to the movie storage such that exhibitors 500 can obtain a movie at a desired network speed. Under program control they should also be able to provide SMC's 250 of a movie via wireless transmission of SMC's 250 at pre-specified times or by fulfilling a request that a SMC 250 be sent on a physical media.

Whenever an SMC 250 is sent outside the storage service provider 300 the SMC 250 is automatically assigned a new serial number and a watermark. The sent SMC 250 also contains the sender information (authorized name and signature) and the receiver information (authorized receiver).

A movie storage service provider 300 uses storage service provider movie station 1100 to perform movie asset management and delivery to intended exhibitors.

Movie Hub 400

A digital movie hub 400 provides information, such as previews, viewer comments and ratings from various critics, about digital movies 10 from multiple movie producers 100. It also has B2B (business-to-business) and B2C (business-to-consumer) electronic commerce capability as described below.

The objective of the hub 400 is to store any and all information about digital movies 10 from its participating movie producers 100 and movie distributors 200. The hub 400 makes these movies available to anyone at anytime from anywhere over the Internet. Moreover, exhibitors/consumers 500 who have digital movie projection facility are able to purchase and obtain the digital movies 10 for exhibition by one of at least three means, for example, over a satellite link, over a fiber optic connection or by a delivery service on a physical media.

The hub 400 is at the heart of the entire digital movie distribution system.

As more movies (including the movies made for television) and other entertainment, marketing and training audio-visual content become digital in nature, the hub 400 can serve as a B2B and a B2C electronic commerce site for digital entertainment and training programs including digital movies 10. The hub 400 may also introduce innovative and new services for marketing digital movies 10 to end-users like *Try and Buy* or *Pay as You Go* pricing schemes. For example, the SMP 750 can be programmed such that the first 50% of the digital movie 10 can be viewed at no charge and the exhibitor/consumer 500 is charged only if he or she decides to exhibit the rest of the movie.

The goal of the hub 400 is to drive the digital content delivery cost to zero. The process must be self-managed and automated. In a live implementation of the hub 400 there are multiple movie

producers 100 with multiple SMC's 250. The exhibitors 500 can obtain membership at the hub 400 and navigate through the hub 400 content after proper authentication. Depending upon availability, price and quality an exhibitor 500 can collaborate with the movie producer 100 or the movie distributor 200 to license the digital movies 10 for exhibition.

Once the digital movie 10 has been scheduled and paid for, the hub 400 can also provide remote digital screen management service to all exhibitors 500 to actually exhibit the movies on the secure movie projection system 600 located at the exhibitor premises. The hub 400 can also update a specific web site reflecting the schedule of shows for the digital movie 10 at each location. The hub 400 can provide this functionality to any exhibitor 500 anywhere in the world.

The hub 400 can also provide a central facility for remote ticketing for all digital movies 10 for all exhibitors 500 anywhere in the world.

Description of the Hub User Interface

A brief description of the hub 400 user interface is given below. It comprises of the following buttons:

- DIGITAL MOVIE DATABASE
- VIEWING OPTIONS
- RECENT RELEASES and COMING ATTRATIONS
- CELEBRITIES
- NEWS
- REVIEWS
- DIGITAL MOVIE AUCTION
- BUY DIGITAL MOVIES NOW
- MOVIE PRODUCERS
- MOVIE DISTRIBUTORS

- EXHIBITORS
- MOVIE STORAGE SERVICE PROVIDERS

The DIGITAL MOVIE DATABASE button provides information about the catalogued properties of each entry in the movie Database. For example, each entry may contain information about:

- Language
- Country of Origin
- Actors
- Awards
- Director
- Producer

This list of properties should be extendible to accommodate new information about the digital movie 10 from the movie producer 100.

The VIEWING OPTIONS button has information about:

- Which digital theaters is the digital movie 10 playing?
- Where and how to license (buy or rent) the movie? If the digital movie 10 is being distributed on a physical medium, which store (on-line or otherwise) is selling or renting the SMC 250 of the digital movie 10?
- How to obtain the SMP 750 of the digital movie 10?

The RECENT RELEASES and COMING ATTRACTIONS button provides information about respective digital movies 10.

The CELEBRITIES button lists the life and work of digital movie celebrities and solicits comments from their fans to build a community and new marketing avenues of an upcoming attraction.

The NEWS section has the news information about the digital movies 10 and digital movie celebrities.

The REVIEWS button provides information about reviews of digital movies 10 that are provided by viewers and critics. Each review has the following properties and is extendible:

- Reviewer name, affiliation and contact information
- Personal Comments (from people who have watched the movie)

The DIGITAL MOVIE AUCTION button provides information about the movie titles that are available for auction. Filmmakers and distributors who want to participate in auction may put information about their digital movie titles in this section.

The BUY DIGITAL MOVIES NOW button provides electronic commerce functions for purchasing digital movie 10 titles for pre-registered digital projection systems. It also implements new and innovative services like *try and buy* and *pay as you go* pricing options.

The MOVIE PRODUCERS button provides access to producer movie station 1000 applications.

The MOVIE DISTRIBUTORS button provides access to distributor movie station 900 applications.

The EXHIBITORS button provides access to exhibitor movie station 800 applications.

The MOVIE STORAGE SERVICE PROVIDERS button provides access to SSP movie station 1100 applications.

Exhibitor/Consumer 500

Still referring to FIG. 1, an exhibitor/consumer 500 is a theatre owner. It could also be a consumer. In either case availability of a secure movie projection system 600 is a pre-requisite. An exhibitor/consumer 500 is often simply referred to as an exhibitor 500 in this document. In the context of this invention,

an exhibitor 500 uses the exhibitor movie station 800 to perform the following interaction with the hub 400:

- The exhibitor 500 interacts with the hub 400 using the EXHIBITORS button on the hub 400 web site.
- The exhibitor 500 previews the available movies on the hub 400.
- The exhibitor 500 collaborates with a movie producer 100 or a movie distributor 200 to license (buy or rent) the rights of a movie to exhibit.
- The exhibitor 500 conducts an electronic commerce transaction with the hub 400 by sending a movie purchase authorization request MPAR 450 to the hub 400.
- The hub 400 obtains the unique projector identification descriptor 550 from the exhibitor movie station 800 and issues an electronic movie ticket 350 to the exhibitor 500.
- The exhibitor movie station 800 prepares itself to receive the secure movie player SMP 750 software.
- The exhibitor movie station 800 unlocks the SMP 750 with the electronic movie ticket 350.
- The SMP 750 verifies the exhibitor 500 by confirming the username and the password of the exhibitor 500. It also verifies the movie projection system 600 by using the electronic movie ticket 350 and obtains or instructs the exhibitor 500 how to obtain the SMC 250 for the movie.
- The SMP 750 unlocks the SMC 250 and securely exhibits the movie on the movie projection system 600.
- After the movie is exhibited the exhibitor 500 sends a usage report 850 to the hub 400.

Movie Projection System 600

A movie projection system 600 is a hardware device with a unique projector identification descriptor 550. FIG. 5 shows a block diagram of a movie projection system 600. It contains the following components:

- A CPU and memory subsystem 605 that can execute a SMP 750 software program. Upon unauthorized access the SMP 750 can disable itself and the SMC 250 and notify the hub 400 through exhibitor movie station 800.
- A storage drive 610 that can accept a digital cinema disk (DCD) media containing a SMC 250 or that can store a SMC 250 obtained by a SSP communications interface 620.
- An exhibitor communications interface 615 to communicate with exhibitor movie station 800 for control information like receiving SMP 750 and sending usage report 850.
- A SSP communications interface 620 to communicate with the storage service provider over a fiber optic or satellite communications network to obtain SMC 250 and store it in the storage drive 610. The SSP communications interface 620 is expected to be relatively high-speed.
- A remote control interface 625 to control SMP 750 via a remote control device 630.
- A audio-video subsystem 635 to decompress SMC 250 and execute any audio and video special effects.
- A clock and calendar subsystem 640 to control timers.
- A secure audio and video subsystem 645 that sends PID 550 and other control information to the CPU and memory subsystem 605 for verification by the SMP 750 and receives encrypted audio and video streams from the CPU and memory subsystem 605.

Secure Movie Key Database 700

Security of a digital movie 10 is ensured through a key-based encryption of the digital data. Digital watermarking is used to detect any leaks in security. The digital movie distribution system described in this invention is not dependent on any particular digital encryption and watermarking methods - open or proprietary. However, the various levels of implementation and execution of the digital encryption and watermarking methods are considered part of this invention. For clarity of presentation, watermarking is considered to be part of encryption system used

with this invention. Encryption of digital content is implemented at multiple levels as described below.

1. Using an encryption key for every two-minute segment of a raw digital movie 10 data constitutes the most basic (Level 1) encryption scheme. This will create a database of corresponding Level I decryption keys that must be duplicated and kept in a physically and electronically secure place.

2. In today's implementation of digital communications infrastructure (based on copper, fiber or satellite) a subscriber has a very wide range of bandwidths available to choose from depending upon the communications lines and hardware the subscriber is willing to deploy and the usage fee the subscriber is willing to pay. Depending upon the bandwidth available to a subscriber or his/her willingness to pay for the bandwidth, the SMP 750 can be programmed to stream sufficient content from the movie storage service provider 300 and obtain the rest of the content from a locally attached digital cinema disk (DCD). This will allow an additional layer (Level II) of security for two reasons:
   - Content of every frame is split into two portions such that each portion by itself is not meaningfully complete without the other for the intended purpose.
   - Each portion of the frame content can be encrypted in such a way that one portion holds the key for the other portion and cannot be decrypted without first assembling the two portions.

   Also note that dividing the content of each frame into more than two portions can extend the above method.

   This will create a database of corresponding Level II decryption algorithm that must be duplicated and kept in a physically and electronically secure place.

3. If the digital cinema disk (DCD) is an optical disk or the movie projection system 600 is an optical projector, the previously encrypted digital movie 10 can be further encrypted optically by using a prism (filter) of a specific quality at the source such that the same quality prism (filter) will be required at the destination for decrypting the digital content. The movie producer 100 can then use this prism (filter) as the physical key for securing the digital movie 10. This will allow yet another layer (Layer III) of security for the digital movie.

   This will create a database of corresponding Level III decryption algorithm that must be duplicated and kept in a physically and electronically secure place.

FIG. 6 shows the format of an entry K in the secure movie key database 700. Each entry consists of the following components:

- A decryption key 150 that is sent to the hub 400 during registration of a digital movie 10 with the hub 400.
- Information about the format, the compression method used and location of SMC 250 for the digital movie 10.
- Keys for Level I decryption.
- Keys and procedure for Level II decryption.
- Keys and procedure for Level III decryption.

Distributor Movie Key Database 710

The distributor movie key database 710 has movie keys that can be used to restrict the distribution rights of a movie distributor 200 to a specific geography or to a specific channel of distribution. These keys either expire at a certain time in the future or will work only on certain movie projection system 600.

Exhibitor Movie Station 800

Exhibitor movie station 800 is a collection of exhibitor applications on the hub 400. These applications can be executed on an exhibitor premises on a personal computer class hardware

system that can run a browser and connect to the hub 400. The exhibitor movie station 800 can access the digital projection system 600 and the local storage system where the SMC 250 and SMP 750 are stored. It allows the exhibitor 500 to collaborate with the movie producer 100 or the movie distributor 200 in securing the licensing rights to a movie and its marketing materials. It also allows the exhibitor 500 to send usage report 850 and provide control information to the projection system 600 for obtaining the SMC 250 and the SMP 750. It also provides exhibitor 500 back-office operations support such as co-op reconciliation with the movie producer 100 and/or movie distributor 200, electronic ticketing and box-office reporting, scheduling movie projection, and running on-line and print movie marketing and promotion programs.

Distributor Movie Station 900

Distributor movie station 900 is a collection of distributor applications on the hub 400. These applications can be executed on distributor 200 premises on a personal computer class hardware system that can run a browser and connect to the hub 400. The distributor movie station 900 allows the distributor 200 to collaborate with the movie producer 100 in securing the distribution rights to a movie. It also allows the distributor 200 to monitor the usage reports 850 and interact with the movie storage service provider 300. It also provides the distributor back-office operations support such as co-op reconciliation and credit and collection from the exhibitor 500 and running on-line and print movie marketing and promotion programs.

Producer Movie Station 1000

Producer movie station 1000 is a collection of producer applications on the hub 400. These applications can be executed on producer premises on a personal computer class hardware system that can run a browser and connect to the hub 400. The producer movie station 1000 allows the producer 100 to collaborate with the movie distributor 200 and the storage service provider 300 in

finalizing the distribution rights to a movie. It also allows the producer 100 to interact with the hub 400 for example in submitting the movie preview 50 and monitoring the usage report 850. It also provides producer back-office operations support such as managing secure movie key database 700.

SSP Movie Station 1100

SSP movie station 1100 is a collection of storage service provider applications on the hub 400. These applications can be executed on movie storage service provider 300 premises on a personal computer class hardware system that can run a browser and connect to the hub 400. These applications will allow the movie storage service provider 300 to negotiate the rights to store the SMC 250 of a movie. They will also allow a movie storage service provider to perform movie asset management and delivery of the movies purchased to the intended exhibitor 500.

Movie Preview 50

Movie preview 50 is the trailer of a movie that is used for marketing and advertising the movie. Under program control a movie producer 100 or a movie distributor 200 can include specific movie previews 50 in a specific SMC 250 or SMP 750 by integrating their existing systems with the distributor movie station 900 or the producer movie station 1000 respectively.

Movie Decryption Key 150

The movie decryption key 150 of a digital movie 10 includes the movie title and a reference to a corresponding entry in the secure movie key database 700.

Secure Movie Container 250

A movie container is a software object that contains movie bits in a specific format. This format contains information about audio, video and special effects (like background music or video, closed caption and dubbing.) These formats can be open and publicly available or can be proprietary to a filmmaker or

studio. Movie bits are present in the movie container according to this specific format. For example the JAVA Media Format Version 2.0, a publicly available application programming interface, will allow content providers to capture digital content in multiple open or proprietary formats.

Once the contents of a movie container are encrypted according to a specific known cipher algorithm, it becomes a secure movie container (SMC) 250. One or more encryption keys (for example an encryption key may be used for every two minute segment of a movie) are involved in generating a SMC 250. Only the movie producer 100 knows the corresponding decryption keys of a SMC 250.

Each secure movie container SMC 250 has the source information (originating studio/filmmaker), release information (date released and authorized name and signature) and credits information (casting). This information can be contained in the header of the SMC 250 and need not be encrypted. This will allow the movie storage service provider 300 to create media asset management applications to keep track of SMC 250 by interrogating them to verify their availability. The same information can also be made a part of movie preview 50 so that the hub 400 can account for all the movie previews 50 that the hub 400 has available. Such movie information in an SMC 250 can be left unencrypted and can prevent inadvertent delivery and exhibition of wrong content.

Electronic Movie Ticket 350

An electronic movie ticket 350 contains an authorization code to unlock the SMP 750 of an SMC 250 and to verify the secure movie projection system 600. Upon completing an electronic commerce transaction for exhibiting a movie the hub 400 issues an electronic movie ticket 350 to the exhibitor/consumer 500. This authorization code in the electronic movie ticket 350 is used in programming the SMP 750 that is subsequently downloaded by the

exhibitor movie station 800. This authorization code is electronically stored in the exhibitor movie station 800 and is used by the SMP 750 to authenticate the secure movie projection system 600.

Movie Purchase Authorization Request (MPAR) 450

The MPAR 450 contains the following information:

- Credit card number or account number (if the exhibitor is a preferred customer at the Hub 400) or the negotiated box office revenue split arrangement.
- Username
- Password
- Expiration timer T days from the time of purchase, and
- Number of times N the movie will be exhibited

Projector Identification Descriptor (PID) 550

This is a unique identifier of secure movie projection system 600 much like the host-id of a computer system connected on the Internet.

Movie Purchase Request (MPR) 650

The MPR 650 contains the following information:

- Title of the movie
- Movie decryption key 150
- Username and password of the exhibitor 500
- Electronic movie ticket 350
- Unique PID 550 of the projection system 600 at the exhibitor premises
- Number of screenings N and the expiration timer T

Secure Movie Player (SMP) 750

A movie player is a software program. This program understands a movie container object and its structure and can process its content - including audio, video and special effects - to render audio and images on a speaker processor and a video projector

respectively. A movie player provides standard controls to play, pause, restart, fast forward and rewind the movie.

More specifically, a SMP 750 is a movie player that understands a specific secure movie container (SMC) 250 and enables only those controls that are allowed by its manufacturer. For instance a movie producer 100 may manufacture an SMP 750 that understands how to *play* a specific movie on a specific projection system 600 only for a predefined number of times and may disable all other standard movie player controls like *rewind* and *pause*.

The SMP 750 provides the following functions:

1. Understands and interprets the SMC 250 format;
2. Authenticates the exhibitor 500 and the projection system 600;
3. Enables authorized movie player controls;
4. Meters usage; and
5. Provides security against unauthorized access by disabling itself and the SMC 250.

The SMP 750 is one of the most important parts of the above-described preferred embodiment of the invention. As a movie producer 100 evolves its technology to produce more sophisticated SMP 750 one can envision the following scenarios where a movie producer 100 can release SMPs 750 with increasingly more functionality:

1. Provide a mechanism for refund of unused usage. For example, if the exhibitor 500 has purchased a SMP 750 for two screenings and has exhibited the movie only once, the SMP 750 can be returned or self-disabled for a refund of the second exhibition.

   The concept of refund can be evolved to implement *pay as you go* schemes. For example, in a specific SMP 750 implementation the usage may be monitored every 15 minutes and if the viewer does not like the movie after 15 minutes she may

return/disable the SMP 750 for a full refund. However, if the viewer has watched more than 50% of the movie she cannot get any refund, or in the alternative, obtain a 50% refund.

2. Provide a mechanism for exhibiting interactive movies. Since the SMP 750 understands the format of the SMC 250, it can be programmed to create interactive movies. For example, based on the exhibitor or viewer preference entered in the beginning of a movie the SMP 750 can play or not-play certain parts of a movie. This will allow:
    - The creation of happy or sad endings
    - The creation of multiple story lines
    - The introduction of new scenes or characters

3. Provide a mechanism for releasing multiple version of the same movie. The movie producer 100 may release the entire encrypted content all at once and add various new features to the SMP 750 to create multiple versions of the same movie. This extends the box office shelf life of a movie. This also allows the movie producer 100 to test market a movie by releasing different versions of the same movie in different markets.

With standardized SMC 250 formats, like MPEG2, the hub 400 may offer a generic SMP 750 with the purchase of a movie, or in the alternative, a movie producer 100 may want to release his or her own SMP 750 with the release of a SMC 250.

Usage Report 850

Referring to FIG. 1, when a SMP 750 completes playing an SMC 250 a message is sent to the hub 400. This message is the usage report 850, which contains information about exhibition location (local theater details), exhibition time and other viewer feedback details on the digital movie 10. A specified credit may be given to the exhibitor 500 for providing a complete usage report 850.

Unauthorized Attempt Report 950

Only an authorized person can open a SMC 250 and a SMP 750. If an attempt is made to open a SMP 750 or a SMC 250 by an unauthorized person or a program, a message will be sent to the movie storage service provider 300 and the hub 400.

Secure Movie Container Generator

FIG. 2 is a flowchart of a SMC 250 generator. It is a software system that creates SMCs 250. It uses a movie key K to encrypt a movie to create a particular SMC 250. The movie key K is stored in the secure movie key database 700 and is used by the secure movie player generator to create SMPs 750. A step by step description of the flowchart in FIG. 2 is a as follows:

1. Start SMC generator.
2. Obtain digital movie 10 content.
3. Store movie content in a proprietary or open format.
4. Encrypt using Level I encryption algorithm.
5. Compress encrypted movie using proprietary or open compression algorithm.
6. Encrypt compressed movie using Level II and Level III encryption algorithms.
7. Store secure movie container SMC 250 of the digital movie 10.
8. Enter corresponding Level I, Level II and Level III decryption key and methods into the secure movie key database 700.
9. Stop SMC generator.

For example, Java Media Framework (JMF), a publicly available application programming interface, allows a software developer to write a secure movie container generator that can create SMCs using customized coder-decoders and formats.

Secure Movie Player Generator

FIG. 3 is a flowchart of a SMP 750 generator. It is a software system that creates SMPs 750. It uses information from the movie purchase request MPR 650 and the movie key K of the purchased movie from the secure movie key database 700 to create an SMP

750. SMPs 750 can exhibit a pre-programmed movie on a pre-programmed digital projection system 600 for N times during a pre-programmed duration T. A step by step description of the flowchart in FIG. 3 is a as follows:

1. Start SMP generator.
2. Obtain the following information from the movie purchase order 650: movie title, exhibitor username and password, authorized usage parameters N and T, unique PID 550, electronic movie ticket 350 and movie decryption key 150.
3. Using the movie decryption key 150 obtain the movie key K from the secure movie key database 700.
4. Create SMP 750 and use key K to program the following information in it: where to obtain the SMC 250 of the movie, Level I, Level II and Level III decryption keys and methods of the SMC 250.
5. Store SMP 750
6. Stop SMP generator.

For example, JAVA Media Framework (JMF), a publicly available application programming interface, allows a software developer to write a secure movie player generator to create SMPs 750 that can play SMCs 250.

FIG. 4 is a flowchart of various steps involved in executing a SMP 750. These steps are described below:

1. SMP 750 authenticates the exhibitor 500 by verifying the username and the password that was entered during purchasing electronic movie ticket 350.
2. SMP 750 reads the electronic movie ticket 350 from the exhibitor movie station 800.
3. SMP 750 authenticates the movie projection system 600 by verifying the unique PID 550.
4. SMP 750 verifies the movie title, number of screenings N and the expiration time period T.
5. SMP 750 provides and confirms one or more of the following options to load the SMC 250:

- Over a fiber optic cable connection
- Over a satellite broadcast medium at a specified time
- Using a locally attached DCD

6. SMP 750 obtains SMC 250.
7. SMP 750 unlocks the SMC 250 using the movie key K that was programmed in the SMP 750. This movie key K was obtained from the secure movie key database 700 during creation of SMP 750.
8. SMP 750 checks the expiration timer and updates the remaining time and the screening count.
9. SMP 750 plays the secure movie container SMC 250 onto the movie projection system 600.
10. SMP 750 meters Usage: If expiration timer T or screening count N is not valid, disable SMP 750 and SMC 250.

The above description of this invention when taken together with FIG. 1-6 describe the methodology needed to create a software architecture that can be deployed to significantly enhance the distribution and exhibition of digital content including digital movies 10. This methodology defines the building blocks for creating, storing, distributing and exhibiting a digital movie 10. On the basis of these building blocks a digital movie distribution network is defined using software and hardware components as described above. For example, hardware components of the type available from IBM, SUN and others; and software components of the type available from Microsoft, SUN and others can be used to implement digital movie distribution methods and systems described in this invention.

Although the invention has been described with respect to digital movie embodiments, it should be realized that this invention is also capable of a wide variety of other embodiments within the spirit and scope of the appended claims.

What is claimed is:

CLAIMS

1. A method for secure distribution of material from a provider over a network to a destination comprising the steps of:
   digitizing the material;
   encrypting the digitized material;
   forming a corresponding decryption key;
   authorizing the destination to receive the material;
   setting at least one limitation on presentation of the material;
   creating a software program containing said decryption key and said at least one limitation;
   providing the software program to the destination;
   permitting the destination access to the encrypted digitized material;
   receiving the encrypted digitized material at the destination;
   using said decryption key to enable presentation of the digitized material within said at least one limitation.

2. The method as defined in claim 1 further comprising the steps of:
   providing a user at the destination;
   said authorizing step being accomplished with a password;
   providing payment for the presentation of the digitized material;
   presenting the digitized material;
   determining if said at least one limitation has been exceeded, and if so, disabling the presentation of the digitized material; and
   providing information representative thereof.

3. The method as defined in claim 2 wherein said user is an exhibitor.

4. The method as defined in claim 2 wherein said authorizing step is further accomplished with a username.

5. The method as defined in claim 2 further comprising the step of forwarding said information to the provider.

6. The method as defined in claim 2 further comprising the step of issuing a ticket to said user upon said payment and said ticket effecting said authorizing step.

7. The method as defined in claim 1 wherein the material includes anyone of or combination of the following: movies, videos, music, recitations, pictures, printed books, audio books.

8. The method as defined in claim 1 wherein said at least one limitation comprises any one or more of the following: a number of presentations, a time window for presentations, a geographical restriction for presentations, a restriction to a particular entity for presentations, restriction to a type of audience for presentations.

9. The method as defined in claim 2 further comprising the step of:
monitoring said user, and if determined not to be authorized, sending a message representative thereof to the provider.

10. The method as defined in claim 1 further comprising the steps of:
enabling a player for presenting the digitized material within said at least one limitation; and
monitoring said player.

11. The method as defined in claim 1 further comprising the step of:
distributing the material to multiple users at one or more destinations.

12. The method as defined in claim 1 wherein the step of permitting the destination access includes the steps of transmitting the material via the network and storing the material, or sending the material on an optical or magnetic disk via a delivery service or a combination of the two.

13. The method as defined in claim 10 further comprising the step of disabling said digitized material based upon information garnered from said monitoring of said player.

14. The method as defined in claim 10 further comprising the step of accumulating information on any one or more of the following: usage of the digitized material, audience for the digitized material, gross proceeds and profits from the presentation.

15. The method as defined in claim 1 further comprising the step of:

storing the encrypted digitized material at a location separate from the provider and the destination.

16. A method for organizing and presenting material of a provider comprising the steps of:

forming a digital content container of the material encrypted by at least one encryption key;

permitting the digital content container to be accessed by a software program;

setting at least one limitation on presentation of the material;

utilizing said software program to present the said digital content container material, wherein said software program authenticates a user of the material, and monitors said at least one limitation, and if said at least one limitation is exceeded providing information with respect thereto to said provider and to said user.

17. The method as defined in claim 16 wherein the step of forming a digital content container encrypted by said at least one encryption key further comprises the step of encrypting the said digital content container material at preselected time intervals by a different encryption key, respectively.

18. The method as defined in claim 16 further comprising the steps of:
verifying authorization by said software program; and
generating identification information based upon said verification.

19. The method as defined in claim 16 wherein said at least one limitation comprises any one or more of the following: a number of presentations, a time window for presentations, a geographical restriction for presentations, a restriction to a particular entity for presentations, restriction to a type of audience for presentations.

20. A system for secure distribution of material from a provider over a network comprising:
a digitized and encrypted version of the material;
an encryption key;
said encryption key utilized to encrypt the material;
a corresponding decryption key;
at lease one authorized destination for receiving the encrypted digitized material;
means for providing at least one limitation on the presentation of the said encrypted digitized material;
a software program;
said software program containing said decryption key and said at least one limitation;
means for providing said software program to said at least one authorized destination; and

means for permitting said at least one authorized destination access to the said encrypted digitized material;

said software program being utilized at said at least one authorized destination to decrypt and present the digitized material within said at least one limitation.

21. The system as defined in claim 20 further comprising:

means for authorizing a user at the destination to present the material;

means for detecting and reporting information with respect to the presentation; and

means for disabling the presentation if unauthorized access to the material is detected.

22. The system as defined in claim 20 wherein said means for authorizing said user includes at least one of the following: a user name, a password, a ticket, a specific presentation system.

23. A system for secure distribution of material from a provider over a network comprising:

at least one encryption key;

a digital content container of the material as encrypted by said at least one encryption key;

means for setting at least one limitation on presentation of the digital content container material;

a software program to access the digital content container material and present the material;

said software program authenticates a user of said digitized material and permits presentation of the material on a player, monitors said at least one limitation; and

notifies the provider and said user if said at least one limitation is exceeded.

24. The system as defined in claim 23 further comprising:
means for requesting verification of the presentation of the material by said user and if verification is correct, sending usage information to the provider, and if verification is incorrect disabling the presentation and sending said user identification information to the provider.

25. The method as defined in claim 1 wherein said encrypting step is accomplished by:
dividing the material into frames;
encrypting at least one of said frames with an encryption key; and
storing the corresponding decryption key.

26. The method as defined in claim 25 wherein said encrypting step is further accomplished by:
dividing said at least one of said encrypted frame into two or more parts;
encrypting one part by using another part as the encryption key in a round robin fashion; and
storing a corresponding decryption algorithm in said decryption key.

27. The method as defined in claim 1 wherein said encrypting step is further accomplished by:
storing the digitized material on an optical media using an optical filter; and
storing a corresponding decryption algorithm in said decryption key;

29. The method as defined in claim 1 wherein the network is a communications network.

30. The method as defined in claim 1 wherein the network is a distribution network.

31. The method as defined in claim 1 wherein said receiving step comprises any one or a combination of more than one of the following: receiving the material over a fiber optic connection, receiving the material over a satellite connection, receiving the material on an optical or magnetic disk via a delivery service.

32. The system as defined in claim 20 wherein the network is a communications network.

33. The system as defined in claim 23 wherein the network is a communications network.

34. The system as defined in claim 20 wherein the network is a distribution network.

35. The system as defined in claim 23 wherein the network is a distribution network.

36. The system as defined in claim 1 wherein the network is the Internet.

37. The system as defined in claim 20 wherein the network is the Internet.

38. The system as defined in claim 23 wherein the network is the Internet.

FIG. 1

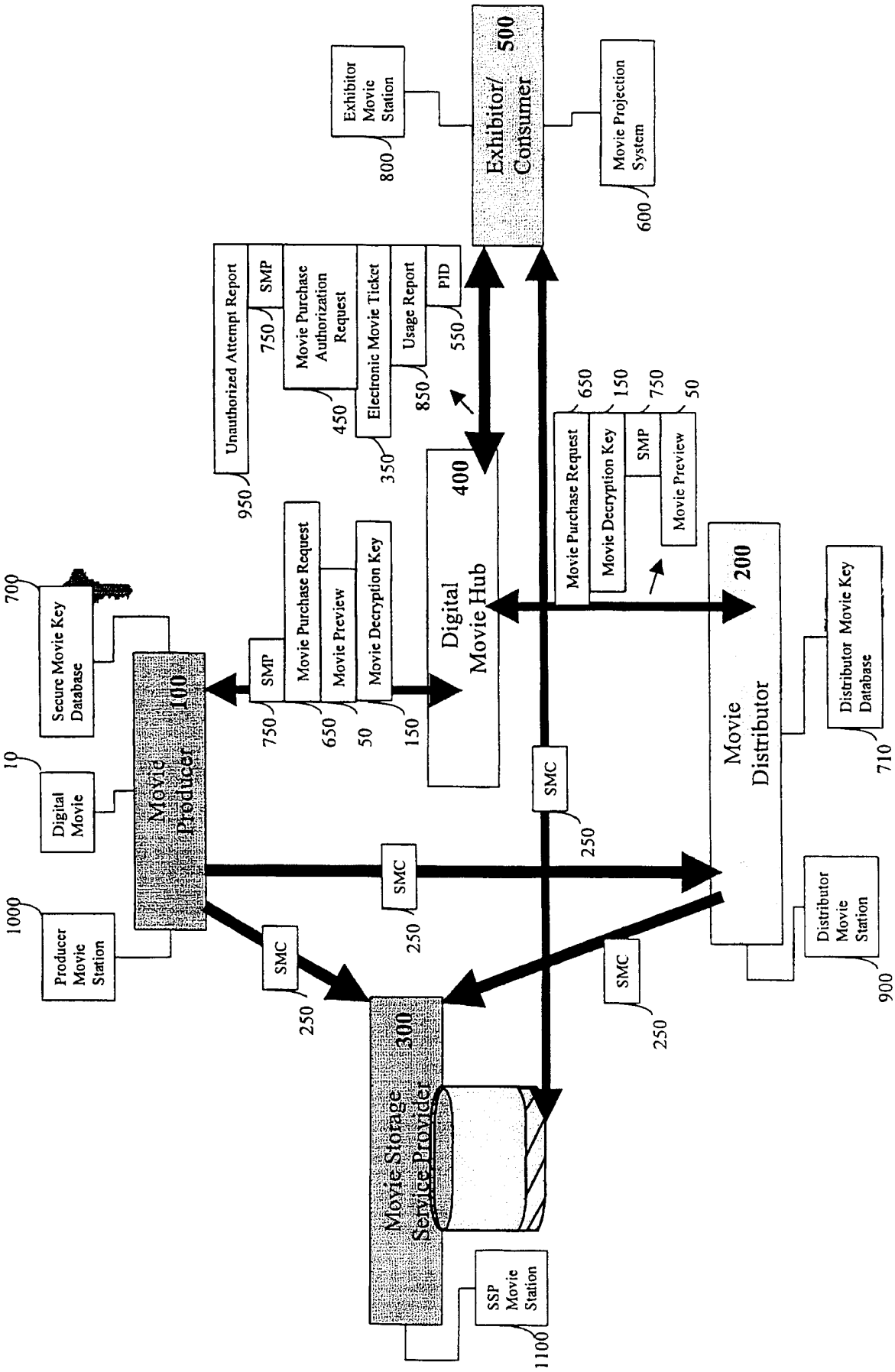

Exhibitor/ Consumer 500
Exhibitor Movie Station
800
Movie Projection System
600
Unauthorized Attempt Report
950
SMP
750
Movie Purchase Authorization Request
450
Electronic Movie Ticket
350
Usage Report
850
PID
550
Digital Movie Hub 400
Movie Purchase Request
650
Movie Decryption Key
150
SMP
750
Movie Preview
50
Movie Distributor 200
Distributor Movie Key Database
710
Distributor Movie Station
900
Secure Movie Key Database
700
Digital Movie
10
Movie Producer 100
Producer Movie Station
1000
SMP
750
Movie Purchase Request
650
Movie Preview
50
Movie Decryption Key
150
SMC
250
SMC
250
SMC
250
SMC
250
Movie Storage Service Provider 300
SSP Movie Station
1100

FIG. 2

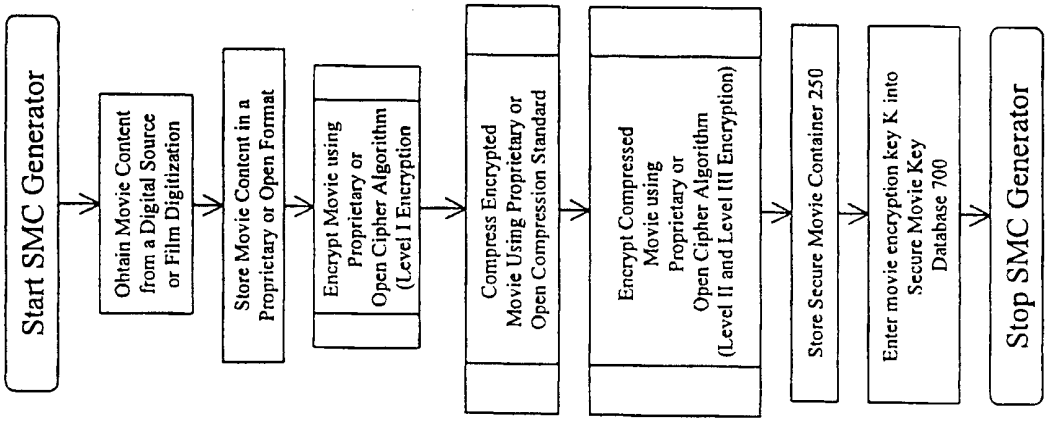

Start SMC Generator
Obtain Movie Content from a Digital Source or Film Digitization
Store Movie Content in a Proprietary or Open Format
Encrypt Movie using Proprietary or Open Cipher Algorithm (Level I Encryption
Compress Encrypted Movie Using Proprietary or Open Compression Standard
Encrypt Compressed Movie using Proprietary or Open Cipher Algorithm (Level II and Level III Encryption)
Store Secure Movie Container 250
Enter movie encryption key K into Secure Movie Key Database 700
Stop SMC Generator

FIG. 3

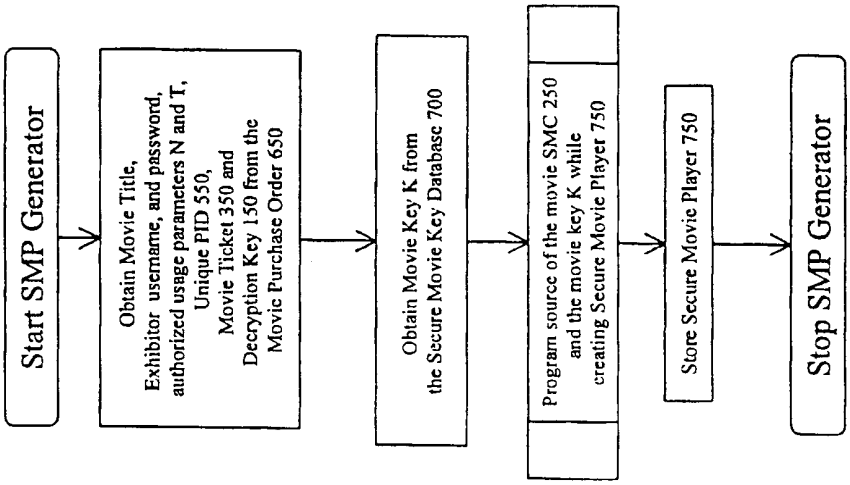

Start SMP Generator
Obtain Movie Title, Exhibitor username, and password, authorized usage parameters N and T, Unique PID 550, Movie Ticket 350 and Decryption Key 150 from the Movie Purchase Order 650
Obtain Movie Key K from the Secure Movie Key Database 700
Program source of the movie SMC 250 and the movie key K while creating Secure Movie Player 750
Store Secure Movie Player 750
Stop SMP Generator

FIG. 4

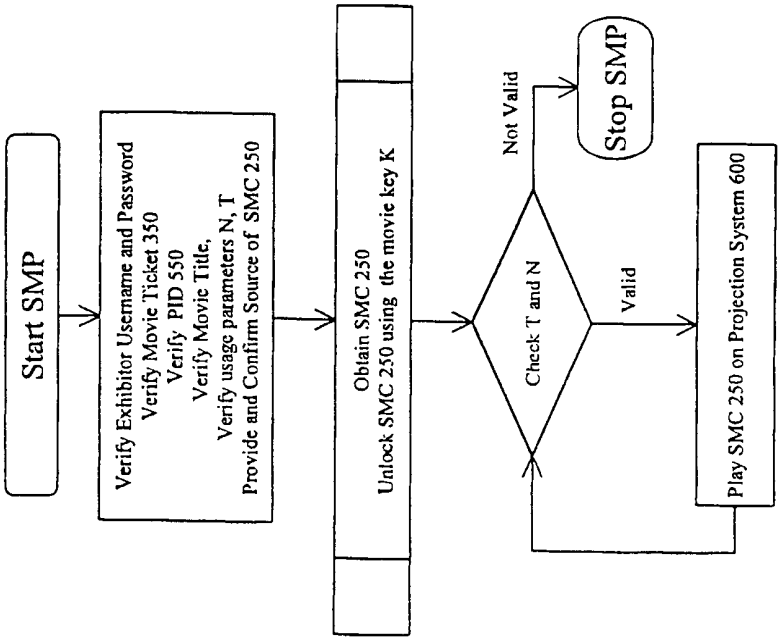
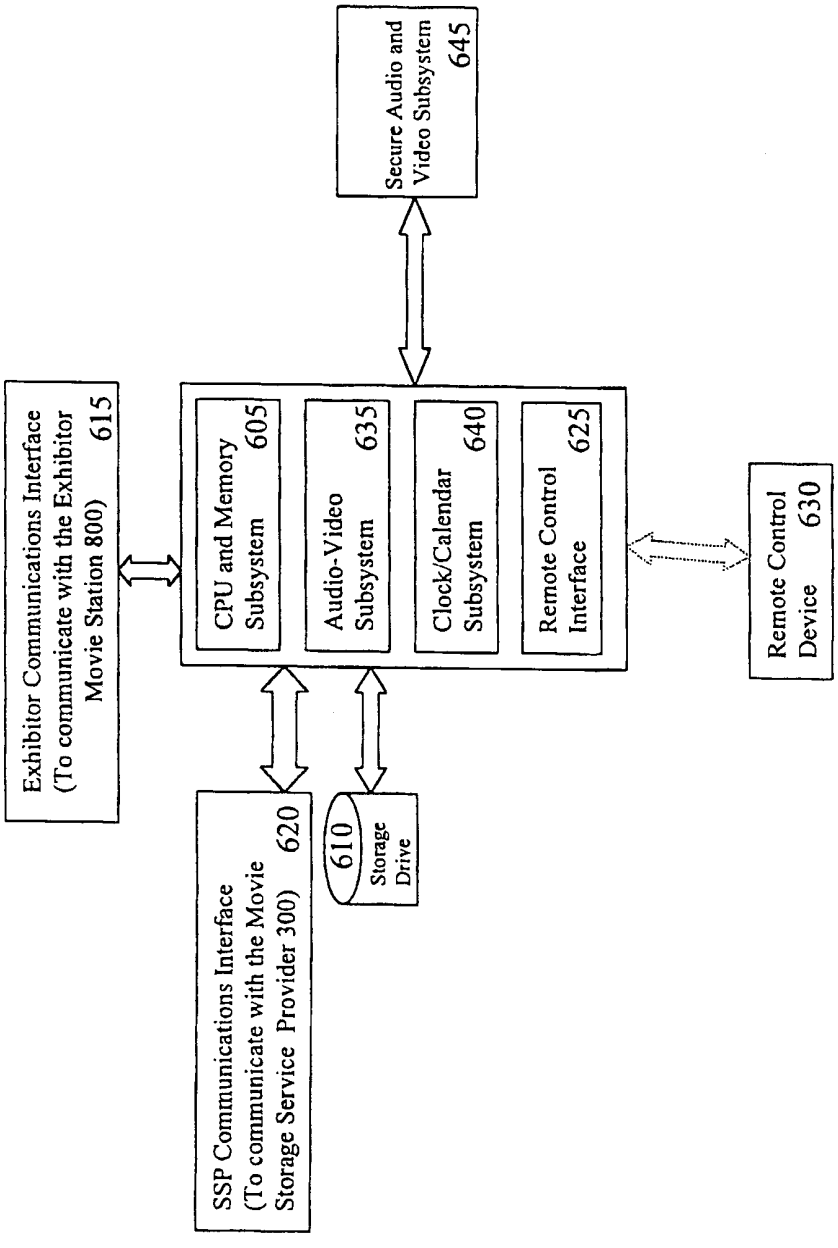

Start SMP
Verify Exhibitor Username and Password
Verify Movie Ticket 350
Verify PID 550
Verify Movie Title,
Verify usage parameters N, T
Provide and Confirm Source of SMC 250
Obtain SMC 250
Unlock SMC 250 using the movie key K
Check T and N
Not Valid
Stop SMP
Valid
Play SMC 250 on Projection System 600

FIG. 5


Secure Audio and Video Subsystem 645
Exhibitor Communications Interface (To communicate with the Exhibitor Movie Station 800) 615
CPU and Memory Subsystem 605
Audio-Video Subsystem 635
Clock/Calendar Subsystem 640
Remote Control Interface 625
Remote Control Device 630
SSP Communications Interface (To communicate with the Movie Storage Service Provider 300) 620
610 Storage Drive

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22823

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/50

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/50, 51,52

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,671,276 A (EYER et al) 23 September 1997 (23.09.1997), Column 4, line 50-Column 12, line 3.	1,7,8,11,12,20,22,25, 29,30,32,34 ---------- 10,13,14,15,27,31,36, 37
Y	US 5,809,145 A (SLIK et al) 15 September 1998 (15.09.1998), Column 5, line 55 - Column 18, line 58	36,37
Y	US 5,825,876 A (PETERSON JR) 20 October 1998 (20.10.1998), Column 2, line 20 - Column 11, line 65.	10,13,14,15,27,31
A	US 4,558,176 A (ARNOLD et al) 10 December 1985 (10.12.1985), Column 4, line 14 - Column 88, line 39	1-38
A	US 4,677,434 A (FASCENDA) 30 June 1987 (30.06.1987), Column 2, line 13 - Column 7, line 10	1-38
A, P	US 5,995,625 A (SUDIA et al) 30 November 1999 (30.11.1999), Column 4, line 30 - Column 20, line 20.	1-38
A, P	US 6,073,122 A (WOOL) 06 June 2000 (06.06.2000), Column 3, line 45 - Column 7, line 20.	1-38

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 December 2000 (07.12.2000)	04 JAN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer James Trammell James R. Matthews Telephone No. (703) 305-9700

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22823

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 6,128,605 A (SAITO et al) 03 October 2000 (03.10.2000), Column 10, line 33 - Column 29, line 67.	1-38
A, P	US 6,092,196 A (REICHE) 18 July 2000 (18.07.2000), Column 8, line 1 - Column 12, line 24.	1-38
A, E	US 6,144,946 A (IWAMURA) 07 November 2000 (07.11.2000) Column 4, line 26 - Column 27, line 67.	1-38

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/22823

Continuation of Item 4 of the first sheet: SYSTEM AND METHOD FOR SECURE DISTRIBUTION AND ON-LINE ELECTRONIC USAGE MANAGEMENT