US 20130185805A1

(19) **United States**

(12) **Patent Application Publication**

Raley et al.

(10) **Pub. No.: US 2013/0185805 A1**

(43) **Pub. Date: Jul. 18, 2013**

(54) **METHOD AND APPARATUS FOR ESTABLISHING USAGE RIGHTS FOR DIGITAL CONTENT TO BE CREATED IN THE FUTURE**

(71) Applicant: **ContentGuard Holdings, Inc.**, Wilmington (DE)

(72) Inventors: **Michael C. Raley**, Downey, CA (US); **Edgardo Valenzuela**, South Gate, CA (US); **Bijan Tadayon**, Potomac, MD (US); **Aram Nahidipour**, Laguna Niguel, CA (US); **Xin Wang**, Torrance, CA (US); **Guillermo Lao**, Torrance, CA (US); **Thanh Ta**, Huntington Beach (AU)

(73) Assignee: **CONTENTGUARD HOLDINGS, INC.**, Wilmington, DE (US)

(21) Appl. No.: **13/785,479**

(22) Filed: **Mar. 5, 2013**

Related U.S. Application Data

(63) Continuation of application No. 12/768,238, filed on Apr. 27, 2010, now Pat. No. 8,412,644, which is a continuation of application No. 11/052,209, filed on Feb. 8, 2005, now Pat. No. 7,725,401, which is a continuation-in-part of application No. 09/867,747, filed on May 31, 2001, now Pat. No. 6,876,984.

Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 21/60*** (2013.01)
USPC **726/27**

(57) **ABSTRACT**

Usage rights for a digital work are established prior to creation of the corresponding content. The rights can be associated with the content after the content is created. A content creation, such as a video recorder or a still camera, device can store labels of the rights and can associate usage rights with content in real time as the content is created.

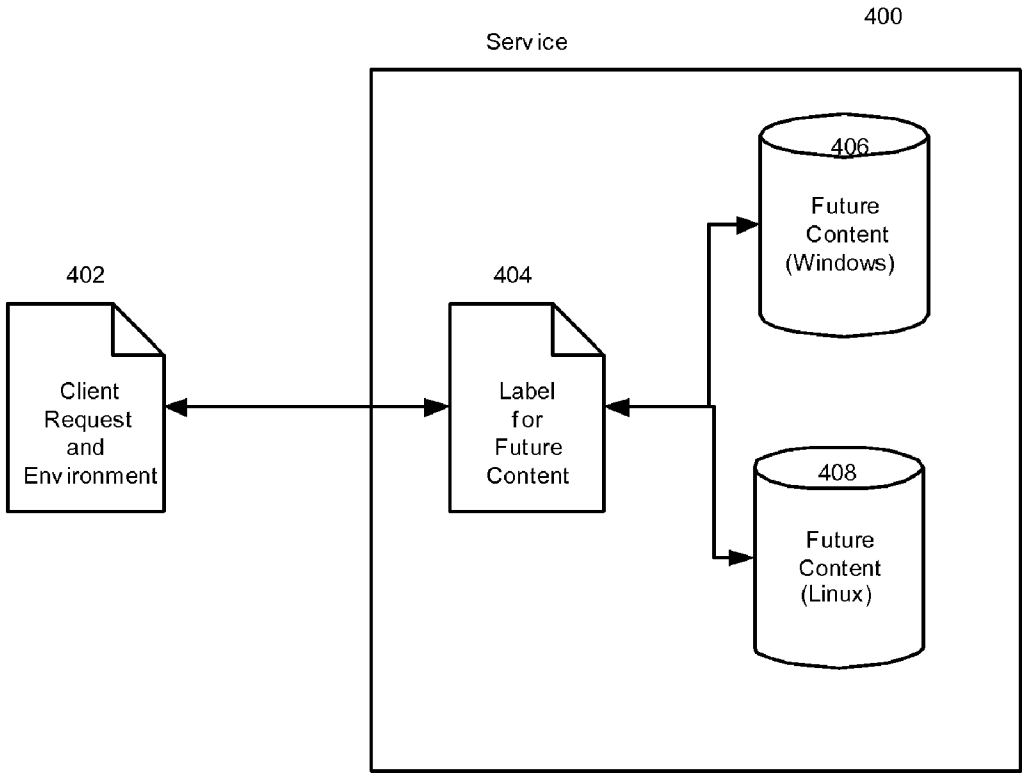


Fig. 1

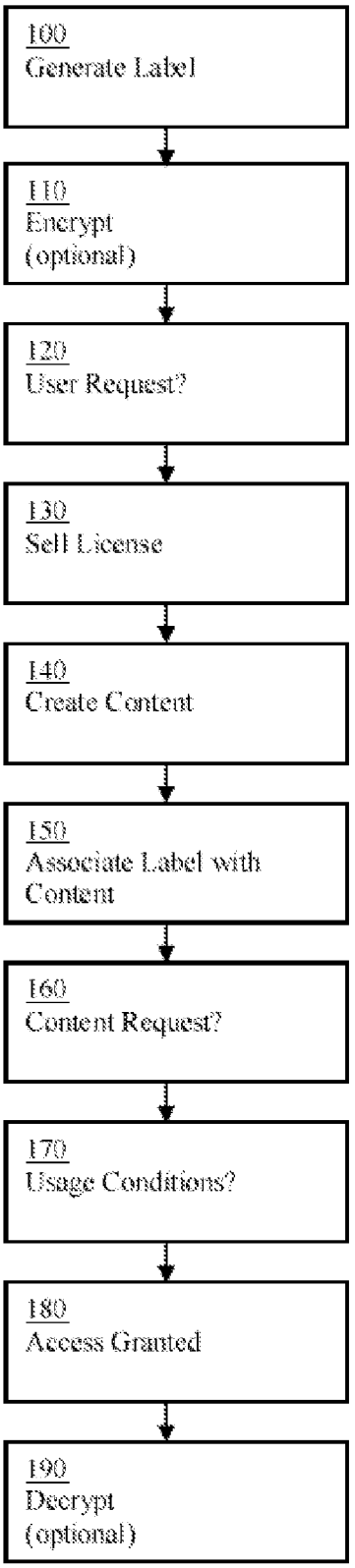

100
Generate Label
110
Encrypt
(optional)
120
User Request?
130
Sell License
140
Create Content
150
Associate Label with
Content
160
Content Request?
170
Usage Conditions?
180
Access Granted
190
Decrypt
(optional)

Fig. 2

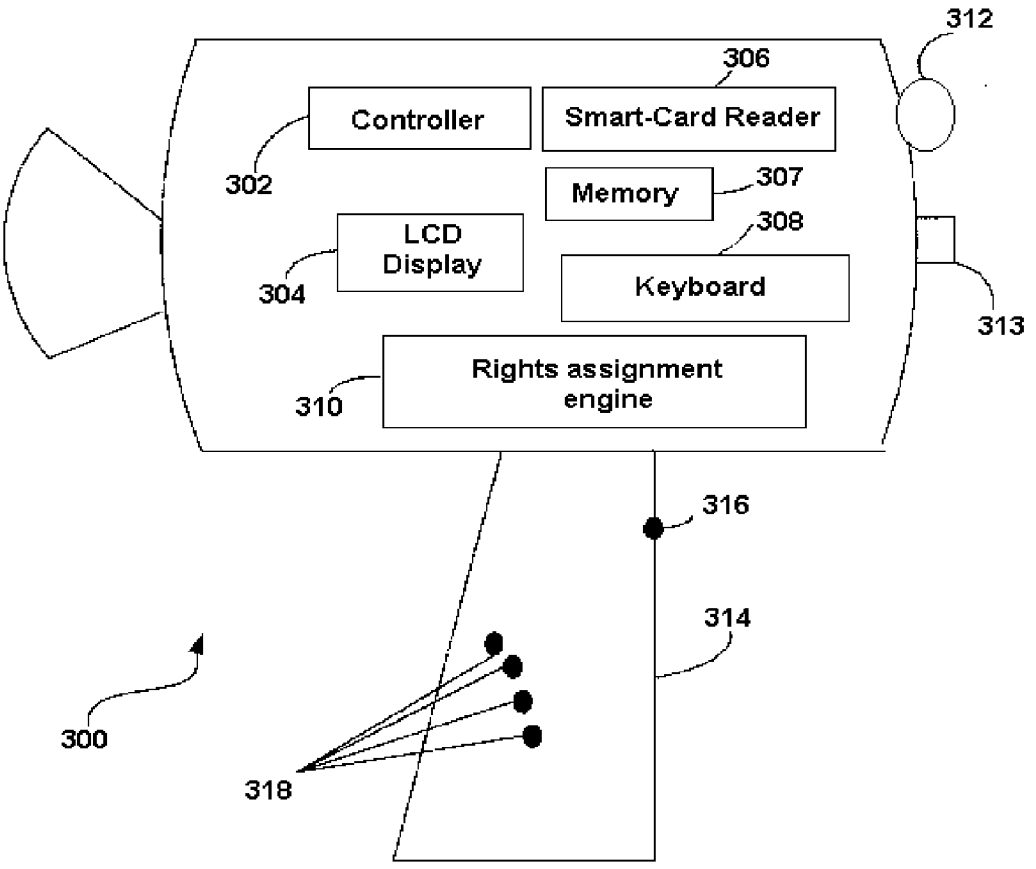

312
306
Controller
Smart-Card Reader
302
Memory
307
LCD Display
308
304
Keyboard
313
Rights assignment engine
310
316
314
300
318

Fig. 3

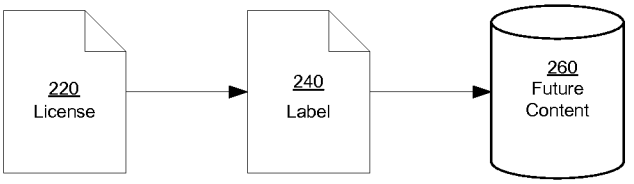


Fig. 4

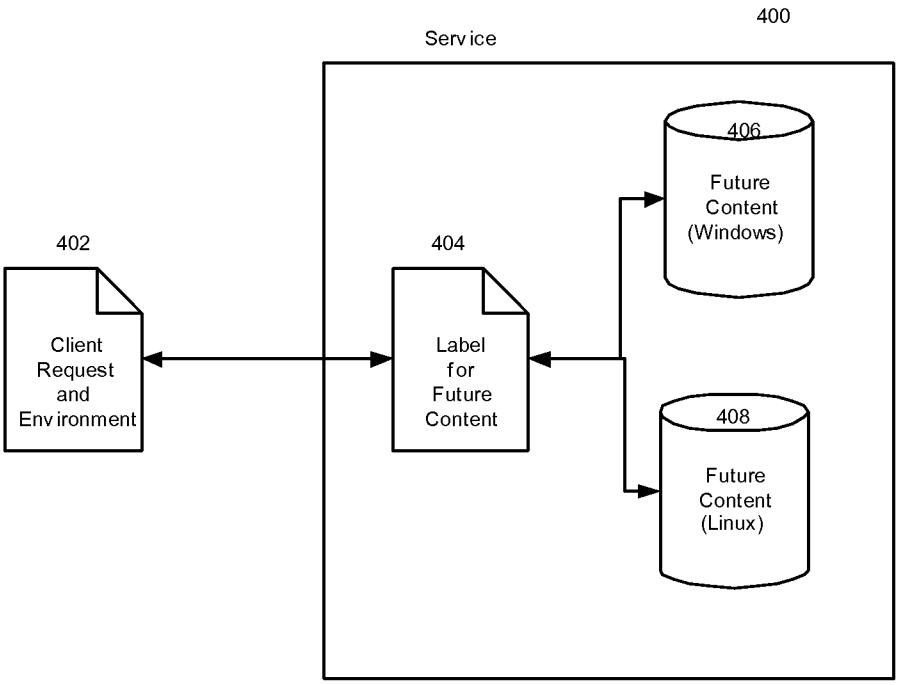
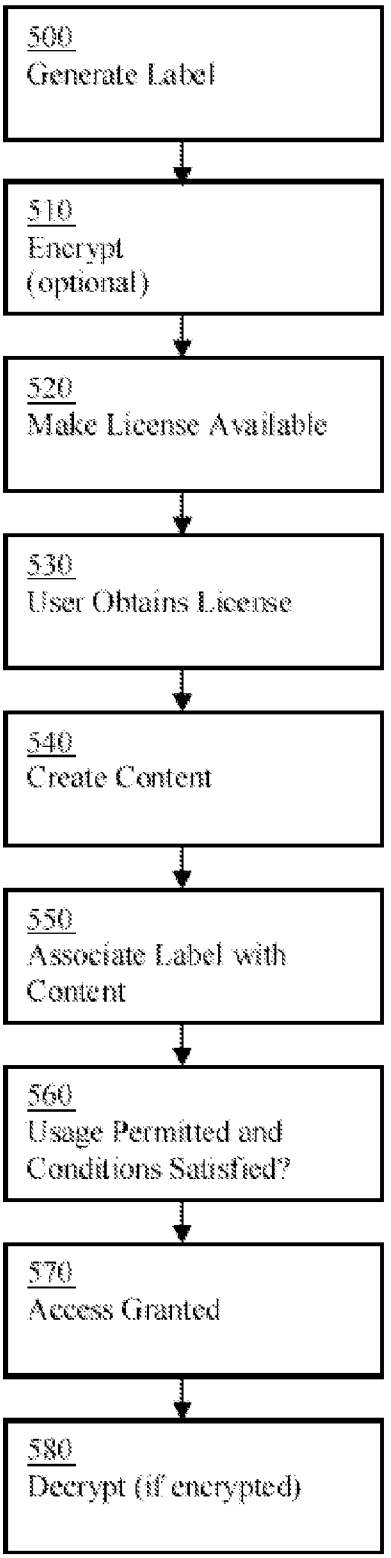

400
Service
406
Future Content (Windows)
402
404
Client Request and Environment
Label for Future Content
408
Future Content (Linux)

Fig. 5


500
Generate Label
510
Encrypt
(optional)
520
Make License Available
530
User Obtains License
540
Create Content
550
Associate Label with
Content
560
Usage Permitted and
Conditions Satisfied?
570
Access Granted
580
Decrypt (if encrypted)

METHOD AND APPARATUS FOR ESTABLISHING USAGE RIGHTS FOR DIGITAL CONTENT TO BE CREATED IN THE FUTURE

RELATED APPLICATION DATA

[0001] This application is a continuation of U.S. patent application Ser. No. 12/768,238, filed Apr. 27, 2010, which is a continuation of U.S. patent application Ser. No. 11/052,209, filed Feb. 8, 2005, now U.S. Pat. No. 7,725,401, which is a continuation-in-part of U.S. patent application Ser. No. 09/867,747, filed May 31, 2001, now U.S. Pat. No. 6,876,984, the disclosures of which are hereby incorporated by reference in their entireties.

BACKGROUND OF THE INVENTION

[0002] This invention relates generally to assignment of usage rights for digital works. In particular, this invention relates to establishing usage rights for before the content is created. Content that has not yet been created can be, for example, a live event (such as a sports event) that has not yet happened. It can also be, for example, a movie that has not yet been filmed or a book that has not yet been written. Moreover, the content in question could be, for example, a movie created many years ago. In that example this invention would pertain to the version of that movie in digital form, prepared and packaged for distribution in a manner described in this invention. Similarly, a two thousand year old book prepared as a new digital work can be content to be created in the future equally as with the case of the book that has not yet been written. Further, an item of content already in digital form can be content that has not been created where a new digital instantiation of the content is created.

[0003] One of the most important issues impeding the widespread distribution of digital works via electronic means, and the Internet in particular, is the current lack of protection of intellectual property rights of content owners during the distribution and the usage of the digital content. Efforts to resolve these issues have been termed "Intellectual Property Rights Management" ("IPRM"), "Digital Property Rights Management" ("DPRM"), "Intellectual Property Management" ("IPM"), "Rights Management" ("RM"), and "Electronic Copyright Management" ("ECM"), collectively referred to as "Digital Rights Management" ("DRM") herein.

[0004] Due to the expansion of the Internet in the recent years, and the issues relating to privacy, authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, document protection, and collection of licensing fees DRM has become even more important. Because the Internet is such a widely used network whereby many computer users communicate and trade ideas and information, the freedom at which electronically published works are reproduced and distributed is widespread and commonplace.

[0005] Two basic types DRM of schemes have been employed to attempt to solve the document protection problem: secure containers and trusted systems. A "secure container" (or simply an encrypted document) offers a way to keep document contents encrypted until a set of authorization conditions are met and some copyright terms are honored (e.g., payment for use). After the various conditions and terms are verified with the document provider, the document is released to the user in clear form. Commercial products such as IBM's CRYPTOLOPES™ and InterTrust's DIGIBOXES™ fall into this category. Clearly, the secure container approach provides a solution to protecting the document during delivery over insecure channels, but does not provide any mechanism to prevent legitimate users from obtaining the clear document and then using and redistributing it in violation of content owners' intellectual property.

[0006] Cryptographic mechanisms are typically used to encrypt (or "encipher") documents that are then distributed and stored publicly, and ultimately privately deciphered by authorized users. This provides a basic form of protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium.

[0007] In the "trusted system" approach, the entire system is responsible for preventing unauthorized use and distribution of the document. Building a trusted system usually entails introducing new hardware such as a secure processor, secure storage and secure rendering devices. This also requires that all software applications that run on trusted systems be certified to be trusted. While building tamper-proof trusted systems is a real challenge to existing technologies, current market trends suggest that open and untrusted systems such as PC and workstations using browsers to access the Web, will be the dominant systems used to access digital works. In this sense, existing computing environments such as PCs and workstations equipped with popular operating systems (e.g., Windows™, Linux™, and UNIX) and rendering applications such as browsers are not trusted systems and cannot be made trusted without significantly altering their architectures. Of course, alteration of the architecture defeats a primary purpose of the Web, i.e. flexibility and compatibility.

[0008] U.S. Pat. Nos. 5,530,235, 5,634,012, 5,715,403, 5,638,443, and 5,629,980 introduced many basic concept of DRM. All of these patents are hereby incorporated herein by reference in their entirety. U.S. Pat. No. 5,634,012 discloses a system for controlling the distribution of digital documents. Each rendering device has a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for carrying out usage rights associated with a document. Usage rights are encapsulated with the content or otherwise associated with the digital work to travel with the content. The usage rights can permit various types of use such as, viewing only, use once, distribution, and the like. Rights can be granted based on payment or other conditions.

[0009] In conventional DRM techniques, a content owner, or other authorized party, specifies the rights after the content has been created and protects, e.g. encrypts, the content at the same time. A private key is used to encrypt the content, and a label is generated which specifies the usage rights. The rights label and the protected content are then associated and stored. A license to the content can later be generated for a user to permit the user to use or access the content. The license includes a private key which has been encrypted using a public key in known manner.

[0010] To access the content, the private key can be used to decrypt the encrypted public key, allowing the user to decrypt the content. This technique works well if the content is available at the time of the rights specification. However, this technique breaks-down if one wants to specify rights for content and issue a license for the content before the content is available. For example, a distributor of streaming video to

a live future event, or of photographs to a future event, may want to begin selling licenses to the content prior to the event. Conventional DRM systems fall short of presenting processes for improving the security, user interface, organization, structure, and accuracy of the DRM system, particularly for those works that are not yet in existence.

SUMMARY

[0011] An object of the invention is to obviate the problems noted above in the prior technology and permit usage rights to be assigned to a work prior to creation of the work.

[0012] A first aspect of the invention is a method for creating a digital work having content and usage rights related to the content. The method comprises generating a label associated with content of a digital work before the content is created, associating the label with the content and securing the content and the label.

BRIEF DESCRIPTION OF THE DRAWING

[0013] Various embodiments of this invention will be described in detail, with reference to the following figures, wherein:

[0014] FIG. **1** is a flowchart of a method for providing usage rights for digital content before creation of the content in accordance with the an embodiment of the invention; and

[0015] FIG. **2** is a content creation device for providing usage rights for digital content to be created in the future in accordance with an embodiment of the invention.

[0016] FIG. **3** illustrates the relationship between usage rights, a label and future digital content in accordance with an embodiment for this invention.

[0017] FIG. **4** is a black diagram of a service which selects appropriate protected digital content based on the client's environment in accordance with an embodiment of the invention.

[0018] FIG. **5** is a flowchart of a method for providing usage rights for digital content to be created in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0019] The phrase "digital work" as used herein refers to any type of element having content in computed readable form. "Content" as used herein refers to the viewable or otherwise usable portion of a digital work. The phrase "usage rights" refers to permissions, in the form of a manner of use, granted to a user of an existing digital work or a digital work to be created in the future with respect to use, access, distribution, and the like of the content of the work. In addition, usage rights may have one or more conditions which must be satisfied before the permissions may be exercised.

[0020] FIG. **1** illustrates an embodiment of a method for providing usage rights for content of a digital work before the content is created. For each step in this illustration, it is possible that the content, license, label, keys or other data used may be encrypted for added security. In step **100** a label specifying usage rights, to be associated with digital content that is not yet created, is generated. The usage rights label can include usage rights, such as the right to print, copy, alter, edit or view the digital work or any other right, permission, or restriction, such as those contained in the XrML™ language or other usage rights grammar. Alternatively, the usage rights label may include merely an identification of the work and other descriptive data and the specific granted usage rights can be contained in the license discussed below. In the case of using the XrML™ language, the label can be an extensible markup language (XML) document specifying the usage rights. In addition, the future content can have many different versions of usage rights and thus a label can be generated for each version. In step **110**, a key, such as a conventional public key, is generated in a known manner and associated with the label.

[0021] In step **120**, a user request for use of, i.e. a license to, the content to be created is received. Keep in mind that the content itself need not be in existence yet. For example, the content can be a video recording or stream of a sporting event to occur in the future. In step **130**, a distributor of the content, or another authorized party, issues a license to the user. The license can include a private key corresponding to the public key generated in step **110** and may include usage rights or other descriptive data. Once, again, keep in mind that the content itself need not be in existence yet. Accordingly, the distributor is able to sell a license to view the event prior to the event.

[0022] In step **140**, the content is created. Of course, this step can be accomplished by another party. However the content is created, the salient point is that the content somehow comes into existence after rights are assigned for it. The usage rights label can be encapsulated with or attached to the content whereby copies of the digital work will also carry the usage rights label. Alternatively, the label can be stored separately from the content but be associated through flags, calls, or the like. Therefore, the term "associated" as used herein refers broadly to creating a correspondence between the content and the label so the label will be applied to the content. Once the usage rights label is associated with the content, the content can be secured using the key generated in step **110**. The digital content can be secured through any form of encryption or other known technique. For example pretty good privacy (PGP) encryption procedures can be used.

[0023] In step **160**, the process determines whether there is a request for access to the secured digital content. If there are no requests, the process waits for a request. However, if there is a request for access, the process proceeds to step **170** where the usage rights associated with the digital work and/or license are checked to determine whether all the conditions, such as payment, associated with the usage rights have been satisfied. If all the conditions have been satisfied, the process proceeds to step **180** in which access to the content is granted, i.e., the content is downloaded, streamed, or otherwise transferred to the user. In step **190**, the user's private key is used to decrypt the content in a known manner.

[0024] The association of the usage rights with the content may occur in a variety of ways. For example, if the usage rights will be the same for the entire content of a digital work, the usage rights can be attached when the digital work is processed for deposit in a distribution server of other device. However, if the content of the digital work has a variety of different usage rights for various components, the usage rights can be attached as the work is being created. Various authoring tools and/or digital work assembling tools can be utilized for providing an automated process of attaching the usage rights. Because each part of a digital work can have its own usage rights, there can be instances where the usage rights of a "part" will be different from its parent. As such, conflict rules can be established to dictate when and how a right may be exercised.

[0025] FIG. **2** illustrates a content creation device, a video recorder, in accordance with a preferred embodiment of the invention. The content creation device **300** includes a controller **302**, a LCD display **304**, a smart-card reader **306**, a memory **307**, a keypad **308**, a rights assignment engine **310**, eye/iris recognition sensors **312**, a cable connection **313**, a handle **314**, and symmetric finger print recognition sensors **316**,**318**. Also, lens system **320** permits recording of video images. Controller **302** and rights assignment engine **310** of the preferred embodiment are accomplished through a microprocessor based device programmed in a desired manner.

[0026] While FIG. **2** shows the controller **302** and the rights assignment engine **310** as separate units, the functions performed by these units may be combined in one processor or may be further divided among plural processors such as digital signal processors and/or performed by dedicated hardware such as application specific integrated circuits (ASIC), e.g., hard-wired electronic or logic circuits or programmable logic devices., or other hardware or software implementations.

[0027] The smart-card reader **306** can be used for reading cards inserted therein. For example, a license, usage rights, or identification can be embedded in the card and communicated to the controller **302** and/or the rights assignment engine **310**. LCD display **304**, the smart card reader **306**, keypad **308** and software interfaces constitute a user interface of creation server **300**. The user interface permits a user to input information such as identification data, and access requests and provides feedback as to operation of creation device **300**. The content creation device **300** of the preferred embodiment is a video recorder; however, it can be any type of recording device, for example, a still-image camera, an animation generator, or an audio recorder.

[0028] The rights assignment engine **310** can be accessed via the cable connection **313**. For example, a rights assignment computer (not illustrated), such as any computer running XrML™ and related tools, can be coupled to the rights assignment engine **310** via cable connection **313** to download a usage rights label or template, similar to the label described above, indicating usage rights for content to be created by the content creation device **300** in the future. Any content created by the content creation device **300** will automatically be associated with the usage rights label or labels stored in rights assignment engine **310**. Alternatively, the usage rights label can be composed using the user interface of creation device **300**. In either case, one or more labels are and corresponding keys generated and stored in rights assignment engine **310** along with instructions indicating how the labels are to be assigned to content recorded by creation device **300**.

[0029] The instructions can cause the usage rights labels to be assigned in any manner and can include any permissions and/or restrictions. For example, in the case of a video recorder, each part of the video sequence or frames can selectively be assigned different rights. This makes the rights assignment process very flexible and dynamic and permits rights assignment to be made in real time as content is created or prior to creation.

[0030] The content creation device **300** can utilize a unique device ID, a user's smart card, encryption (e.g. PKI) technology, a PIN, or any biometrics system to assign rights based on the identity of the user, the recording device itself, the data on the smart card, or the like. For example, fingerprint recognition sensors **316**, **318** or iris recognition sensor **312** can be used for recognition or authentication of the user's identify to permit rights assignment engine **310** to use a corresponding set of rights associated with the user. For example, all content recorded by person A will have one set of rights and all content recorded by person B will have a different set of rights.

[0031] The content creation device **300** records content in a conventional manner. However, labels and keys generated in steps **100** and **110** described above are stored and associated with content recorded by content recorder **300** during or soon after recording. Accordingly, steps **140** and **150** described above are also accomplished by content creation device **300**. For security purposes, a token or pre-paid card (or magnetic card and smart card, or any of its variations, such as memory-type or synchronous communication card, ISO 7816-compliant card, EMV-type card) can be used for the storage of fees and micro-payments, or keeping track of those fees with associated rights. Such cards can be read using the smart card reader **306**.

[0032] It can be seen that the invention permits usage rights for a work to be created and associated with content prior to the creation of the content. The usage rights define how the future digital work may be used and distributed. These pre-established usage rights become apart of the future digital work and controls the usage and distribution of the content of such work.

[0033] In the preferred embodiment, after the rights have been established for a future content, a private key associated with the future content is assigned and a rights label is generated. This private key, along with the rights label, is stored. A user can purchase the content (present or future) after the label has been inserted into the main server or other devices. After the content is purchased, the content owner can get a license for encryption which contains the public key encrypted by a private key. Alternatively, a single symmetric key can be used.

[0034] The label represented by step **100** in FIG. **1** may serve as a reference to another work. The label in this case would serve as a placeholder for future content. The label may be an empty file or contain computer interpretable or human interpretable data that may be used to later associate it with the future digital content. When it is created the label may include usage right information but it does not need to. The usage rights information can be supplied later. When the usage rights are generated, as represented by step **130** in FIG. **1**, the content referred to by the usage rights would be the label, and need not be the actual digital content. The label could then be referenced to determine which digital content the user is requesting access to. The means of associating the label with the actual content may be done in a variety of ways including the use of human-interpretable text, numeric references, pointers, markup languages such as HTML and XML, programmable scripts or even SQL queries.

[0035] FIG. **3** illustrates this embodiment. In FIG. **3**, license **220** containing usage rights is issued to a user. Since digital content **260** for the license does not yet exist, label **240** is created to act as a placeholder for the future content. The label would contain or imply a relationship between itself and digital content to be created in the future. This relationship may be implied such as naming the label using a product ID or other reference that can later be associated with the digital content, or it may be an actual reference such as human-interpretable text containing the name of the future content or content within the label that can later be used to derive the actual digital content. The label to which the license is bound is used in the appropriate manner to determine the actual

digital content with which the label is associated. The rights and any conditions specified in the usage rights would apply to the actual content, not the label that it represents. The steps discussed above do not necessarily have to be performed in the order shown in the figure. For example, the label can be created before or after the license and before or after the content.

[0036] Usage rights associated with the future digital content may be specified within a license, the label or even the content itself. These usage rights apply to the digital content pointed to by the label, regardless of where they are stored and the method used for storage.

[0037] FIG. **5** illustrates an embodiment of a method for providing usage rights for content of a digital work that is created dynamically at the time the user requests it. The steps illustrated in FIG. **5** do not necessarily have to be performed in the order shown in the figure. For example the label can be created before or after the license and before or after the content. In step **500** a label representing digital content that is not yet created, is generated. The label can include usage rights, such as the right to print, copy, alter, edit or view the digital work or any other right, permission, condition or restriction, such as those contained in the ISO MPEG REL, XrML, ODRL, the Open Mobile Alliance REL or any other usage rights grammar. Alternatively, the usage rights label may include merely an identification of the work and other descriptive data and the specific granted usage rights can be contained in the license discussed below. In the case of using the ISO MPEG REL for example, the label can be an extensible markup language (XML) document specifying the usage rights. In addition, the future content can have many different versions of usage rights and thus a label can be generated for each version. In step **510**, the label may be protected by using known encryption techniques.

[0038] In step **520**, a distributor of the content, or another authorized party, makes available a license to a user. The license can be protected using a private key such as the one corresponding to the public key generated in step **110** and may include usage rights or other descriptive data. Once, again, keep in mind that the content itself need not be in existence yet. Accordingly, for example, a distributor is able to offer a license to view an event prior to the event occurring.

[0039] In step **530**, a user obtains a license to (i.e. receives the right to use) the content to be created. The user may request the license or may receive the license without requesting it. Keep in mind that the content itself need not be in existence yet. For example, the content can be a video recording or stream of a sporting event to occur in the future.

[0040] In step **540**, the content is created. Of course, this step can be accomplished by another party. However the content is created, the salient point is that the content somehow comes into existence after rights are assigned for it. In this embodiment, the content is created in response to the request for content performed previously in step **530**. After the content is created, the label is associated with the content in step **550**. The label can be encapsulated with or attached to the content whereby copies of the digital work will also carry the label. Alternatively, the label can be stored separately from the content but be associated through flags, calls, or the like. Therefore, the term "associated" as used herein refers broadly to creating a correspondence between the content and the label so the label will be applied to represent the content. Once the usage rights label is associated with the content, the content may or may not be secured using the key generated in step **510**. The digital content can be secured through any form of encryption or other known technique. For example pretty good privacy (PGP) encryption procedures can be used.

[0041] In step **560** the usage rights associated with the digital work and/or license are checked to determine whether the use of the digital work is permitted by the usage rights and if there are conditions to the use, all the conditions, such as payment, associated with the usage rights whether the conditions have been satisfied. If the use attempted by the user is permitted and all the conditions, if any, have been satisfied, the process proceeds to step **570** in which access to the content is granted (e.g., the content is downloaded, streamed, or otherwise transferred to the user or the user is permitted to render the content or otherwise use the content in the permitted manner). In step **580**, if the content was encrypted the user's private key is used to decrypt the content in a known manner.

[0042] The invention can be used in a subscription model (for example, for magazine or marketing reports) in which the future issues of the content have not been published, but the rights for those issues have already been assigned and stored. At an appropriate future time, the rights will be associated with the corresponding content. For example, by selling the content of a future event on a web site before the actual event, the traffic of the Web site can be drastically reduced and distributed over a longer period of time, making the requirements for the servers and the Web site easier to satisfy and less expensive to operate. Note, however, that the Web site selling the rights or tickets, i.e. the license, might be different from the Web site providing the content later on.

[0043] The invention may also be used in a flexible subscription model such as identifying multiple issues of a periodical. In this case, the label might contain human-readable text such as "Issues 34-56 of Newsweek Online" with the usage rights to the content specified in a separate license. The label in this case could represent multiple digital works with a single label.

[0044] Another possible use for this invention is the area of services. Some services take an instruction and then generate content as a return value. For example; a user may send a request to a service which contains some information about their operating system, platform or environment. The service could utilize this information to generate or select content appropriate to the user from plural instances of content and return both the content and usage rights that would allow the user to utilize the content. In other words, the service could generate protected digital content customized to a user service **400** receivers environment, such as the user's identity preferences, or computer system.

[0045] FIG. **4** illustrates this embodiment. Client request **402**, consisting of a set of usage rights, along with information about the client environment. The request or usage rights are bound to label which exists within the service. When the service receives the request, it references the indicated label, combined with the client environment information to determine which content, Windows content **406** or Linux content **407** for example, is best suited to the user. As in previous embodiments, the usage rights and label were created prior to the existence of the digital content. Simply put, this embodiment allows the pre-sale and licensing of protected digital content.

[0046] This invention may even be used to help manage limited distribution where digital content is regulated or limited in some fashion. Imagine a content creator that wishes to

restrict the number of copies a particular distributor is capable to selling. Such a business model might be created by placing a unique identifier on each copy of the digital content the creator gives to the distributor. This identifier might be a unique serial number or simply a date & time stamp. The distributor is given only the number of individualized copies of the digital content that they are authorized to sell each month. Once the quantity has been distributed, rather than turning away customers, the distributor might choose to use a label to represent the content they will receive the following month. This would allow them to better serve their customers, continue distribution of the content while at the same time honoring the content creator's desires by only distributing a limited amount each month.

[0047] Also, the invention allows a newspaper editor, for example, to send a camera crew to record content without worrying about the pictures being compromised in any way (for example, altered, edited, viewed by unauthorized personnel, or hidden and separately sold to another newspaper organization). In fact, the camera crew may have no rights whatsoever in the content as soon as the content is recorded.

[0048] Alternatively the editor can set the rights in such a way that the first **10** pictures, for example, will belong to the newspaper (work-related), and the next five pictures will belong to the cameraman (for personal use). This example illustrates the flexibility, security, confidence, certainty, and multiple relationships that can be arranged between parties (the cameraman and the editor in this example).

[0049] All future content may be assigned a content ID prior to existence of the content. Given the content ID information and the license for encryption, the content can be encrypted after creation in a manner that is available to be used by the users who have purchased the license. However, if the content ID information and the license for encryption are not available, access to the content shall be denied.

[0050] Further, a predetermined symmetric key can be generated in advance of content creation, and stored with the rights label. Afterwards, the same key can be used to encrypt the content once it is created. However, as noted above every user can receive a different key. In another alternative, the user can be given an authorization token, which the user can exchange for the license later on.

[0051] The controller **302** can process the security parameters and the rights management steps. Lost-card verification, lost-card reports, card-usage reports, security alert reports, and tracking reports can be associated or combined with the rights management reports, such as reports for revoked rights, denied rights, renewed rights, usage patterns, and micropayments.

[0052] In the preferred embodiments, the label is a placeholder. the label need not have to have specific content or usage rights. The label can be a placeholder for both usage rights and content. Or for just one of these two. For example, the label can be a file with a pointer (or empty data portion) for three things: content, usage rights and an association means. The association means can be supplied first. The other two pieces of information can be supplied subsequently in any order. Conventionally, content is created first and then rights are associated with the content. With the invention, an association of content to rights can be created before the content is even created.

[0053] The invention may be readily implemented in software using object or object-oriented software development environment that provides portable source code that can be used on a variety of computer hardware platforms. For example the software can be written in the JAVA™ language and run in a JAVA™ virtual machine. Alternatively, the disclosed operations may be implemented partially or fully in a hardware using standard logic circuits or VLSI designs. The hardware can include any type of general purpose computer, dedicated computer, or other devices.

[0054] The distribution, accounting, and other functions of the distributor and clearinghouse can be accomplished by any party on any device. For example, the content can be rendered on an eBook reader or PDA in response to entry of a code or insertion of a smartcard into a reader and accounting can be accomplished when the digital work or accounting data is returned to a specific source. The division of tasks disclosed herein is only an example. Usage rights and or accounting data can be encapsulated with the digital work or can be stored separately. Code for rendering, decrypting, or otherwise permitting or limiting use of the content can be stored on any device or can be encapsulated with the digital work. Any distribution arrangement can be used with the invention and such arrangements can include any combination of devices, such as personal computers, servers, PDAs, and the like communicating with one another in any manner as is necessary to transfer the desired information.

[0055] The invention has been described in connection with the above embodiments. However, it should be appreciated that many alternates, modifications and variations may be made to the embodiments of the invention without departing from the scope of the invention as defined by the appended claims and legal equivalents.

What is claimed is:

1. A computer-implemented method executed by one or more computing devices for creating a digital work, the method comprising:

before content is created, associating, by at least one of the one or more computing devices, a usage right with a label associated with the content;

selecting, by at least one of the one or more computing devices, an instance of the content appropriate for a user environment; and

after the content is created, associating, by at least one of the one or more computing devices, the usage right with the selected instance of the content, thereby creating the digital work.

2. An apparatus for creating a digital work, the apparatus comprising:

one or more processors; and

one or more memories operatively coupled to at least one of the one or more processors and having instructions stored thereon that, when executed by at least one of the one or more processors, cause at least one of the one or more processors to:

before content is created, associate a usage right with a label associated with the content;

select an instance of the content appropriate for a user environment; and

after the content is created, associate the usage right with the selected instance of the content, thereby creating the digital work.

3. At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by one or more computing devices, cause at least one of the one or more computing devices to:

before content is created, associate a usage right with a label associated with the content;

select an instance of the content appropriate for a user environment; and

after the content is created, associate the usage right with the selected instance of the content, thereby creating the digital work.

* * * * *