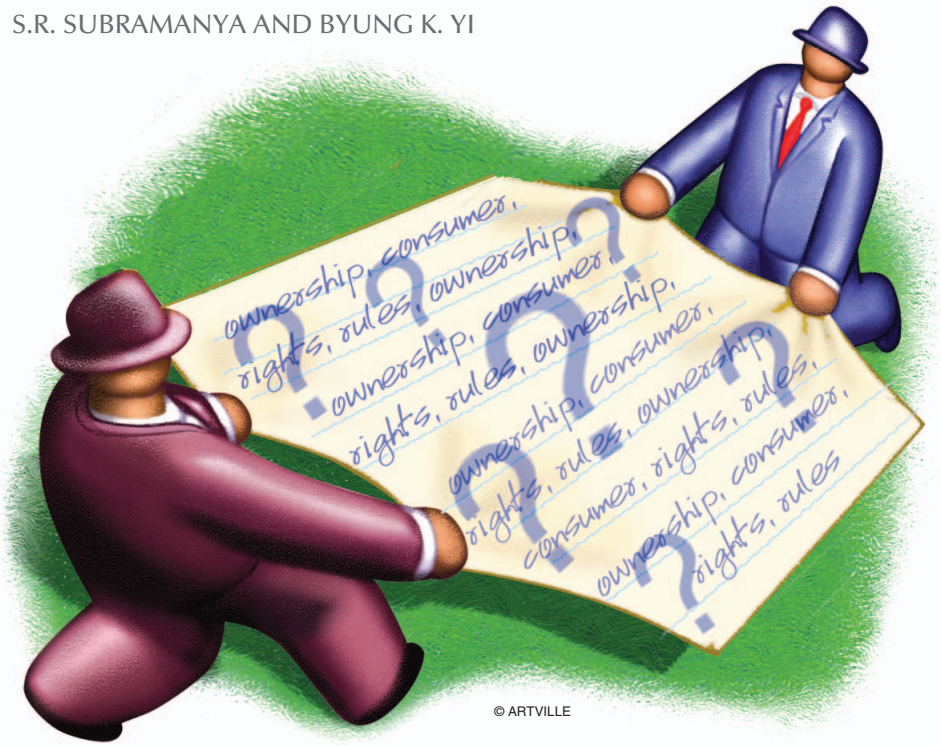
Digital rights management

S.R. SUBRAMANYA AND BYUNG K. YI



TECHNOLOGICAL ADVANCES IN computing, communications, consumer electronics, and their convergence have resulted in phenomenal increases in the amounts of digital content that have been generated, stored, distributed, and consumed. The term "content" broadly refers to any processed and packaged digital information, such as digital audio, video, graphics, animation, images, text, or any combinations of these types. The explosive increases in the generation and consumption of digital content has raised several questions about the rights of the content creator, producer, and distributor as well as the rights and responsibilities of the consumer. The rules governing the appropriate use of content is also open to question.

Overview of DRM

The term digital rights management (DRM) broadly refers to a set of policies, techniques and tools that guide the proper use of digital content. A high-level view of the flow of content from the creator to the consumer via the producer is shown in Fig. 1. The content creator is mainly concerned with the core data/information that goes into the content. This could be viewed as raw content, which needs to be processed further with respect to adhering to certain formats, the suitable integration of different kinds of media, quality enhancement, additions of possible special effects, and derivation and addition of metadata (information about the data). The producer of the content performs the necessary processing and generates the packaged content. The packaged content is in a form that is suitable for consumption and for the tracking and management of content usage. The consumer is the ultimate user of the content.

A DRM system plays important roles in several processes that are involved in the flow of content, as shown in Fig. 1. Very broadly, it facilitates the creator to specify the desired ownership rights of the content. It enables the producer to derive appropriate metadata from the content and specify the producer's rights. It allows the consumer to specify the desired content and the various options in the use of content. It also allows the producer to monitor the content usage and track payment information.

There are several techniques to monitor appropriate content use and to prevent its illegal use. The choice of a particular technique depends on the content type, application needs, and tolerance to inappropriate use of content. It must be understood, however, that no content protection and monitoring technique guarantees absolute security and fool-proof operation. There is always the possibility that desirable features and functionalities of a DRM system will be circumvented. The design and operation of the DRM system should take these factors into account.

Major functionalities of DRM

Simply put, a DRM system manages the appropriate use of content. The major functionalities of this system are numerous. They include facilitating the packaging of raw content into an appropriate form for easy distribution and tracking, protecting the content for tamper-proof transmission, protecting content from unauthorized use, and enabling specifications of suitable rights, which define the modes of content consumption. DRM systems must also facilitate the delivery of content offline on CDs and DVDs; deliver content on-demand over peer-to-peer networks, enterprise networks, or the Internet; and provide ways of determining the authenticity of content and of rendering devices. Supporting payment over the Internet for content usage is another function of DRM as is providing appropriate remuneration for content creators and producers. DRM systems must also monitor the usage of content and ensure that they are in accordance with the rights, track payment and ensure they are in accordance with the usage of content, and manage security and privacy issues appropriately.

In addition, a DRM system should facilitate the personalization of the content, tailoring content to certain preferences of the consumer; be interoperable; supporting different formats of content in a transparent manner; and should handle various levels of content granularity. Granularity of a DRM system refers to the size of the unit (chunk) of content that can be independently selected, delivered, and consumed (e.g., a chapter from a book, a particular song/track from an audio album, or a scene from a video).

Among the major desired features of a DRM system are ease of use by content creators, producers, and consumers; robustness to the circumvention of usage rules; fairness of content usage policies; transparency in the use of content from a variety of content providers and services; fair tariff for different types of content consumption; and innovative means of pricing and payments (e.g., micropayments).

0278-6648/06/$20.00 © 2006 IEEE

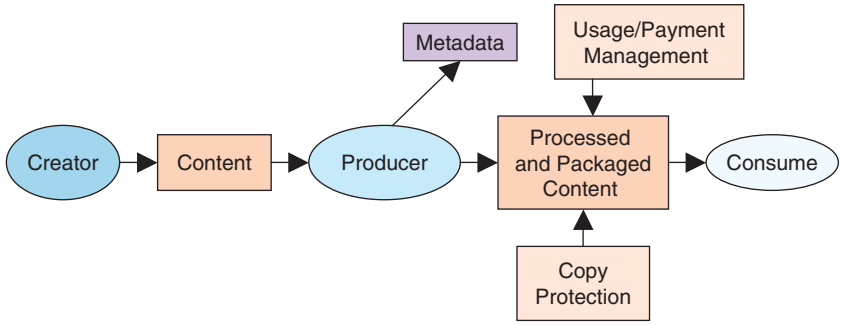


Fig. 1 Broad overview of flow of content from creator to consumer

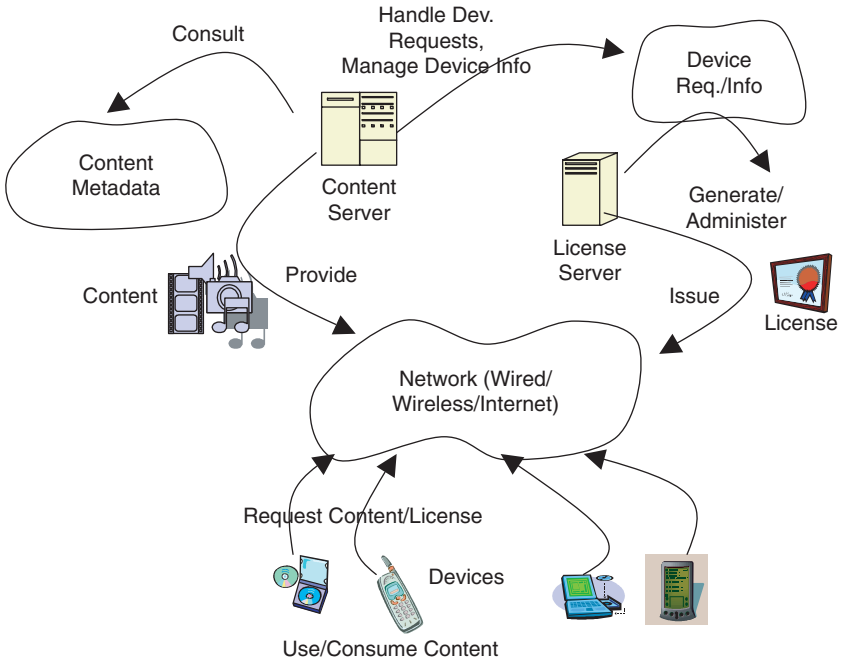


Fig. 2 High-level architecture and major components of a typical DRM system

Architecture and major components of a typical DRM system

One of the main design philosophies of a DRM system is the separation of content from the rights. This allows the content to be distributed or downloaded freely. However, it cannot be consumed without a valid license, which has a proper rights object. The rights object, or just rights, specifies the permission for the various ways the associated content can be used. The same content could be associated with different usage rights specifying different modes of content consumption. This provides flexibility, ease of management, and use of content.

The high-level architecture and major components of a typical DRM system are shown in Fig. 2. It consists of the rendering devices (consumers) that communicate with the content server and license server via a network. The network could be a local area network, a metropolitan area network, the Internet, or a mobile/wireless network. The content server contains the packaged content (media) of appropriate formats that can be played back on suitable content rendering devices. The license server generates and manages licenses that contain the rights—what rights are associated with what content and which users/devices.

The devices are classified into two broad categories: portable devices and network devices. Typical portable devices include audio players (MP3), DVD players, cell phones, laptops and PDAs. Some of the network devices are digital media receivers, HDTVs with set-top-boxes that can receive content over a network. The rendering devices must support the DRM system and be able to properly interpret the rules/rights specified in the license.

Content delivery

Content delivery, or distribution, falls into two major categories: offline and online. Offline distribution consists of distributing packaged content on a portable media such a CD or a DVD. Online content delivery could consist of e-mailing to consumers or being placed on a content server. The content and rights could be combined together into a DRM message or sent separately in an e-mail. The delivery of the content from the content server can be one of two modes: download or streaming. In the download mode, the content is obtained by the device either along with the rights object or separately from it. It is stored locally and then rendered in accordance with its associated rights object. In the streaming mode, there is no storage of the content at the device. The content stream is appropriately protected using stream encryption mechanisms before delivery. The streams are decoded and then rendered by the devices. The device could have a DRM agent, which is responsible for enforcing the rights and controlling the content consumption in accordance with the rights.

Superdistribution refers to the transmission or forwarding of content from one device to another rather than from a content server to a device. However, the rights object cannot be transferred across devices. Thus, superdistribution minimizes the traffic from the server to several devices, while the rights management ensures that the superdistributed contents are not misused.

Security and content protection

Many of the DRM schemes allow the content to be unencrypted and to be freely distributed. They ensure the legitimate and proper use of content by making the consumption of content only in conjunction with appropriate rights objects. There are several other schemes that use added measures of security to protect the content against unauthorized access and use. A simple protection technique is to use encryption of the content. Encryption uses an algorithm and a key to scramble the information. The key for decryption to recover the original information is provided to legitimate consumers. The complexity of the encryption algorithm

and the key size are suitably selected based on the requirements of the particular application. Digital signatures are used for the authentication of content providers as well as content consumers. For example, the content header and a hash of the content, which is a fixed-length data obtained by applying a hash function, could be signed using the private key of the content owner/producer to generate a digital signature. The signature can be verified when issuing the license or when a device contacts the license server to obtain the license to play the content that it already has or to renew the license. For verification, the public key of the content owner/producer is used. Digital certificates are used for DRM client devices to ensure their validity.

The other content protection technique is digital watermarking. Digital watermarking essentially embeds information about content creator, content producer, and conditions of use into the content. Any attempt to remove the watermark would result in degradation of the quality of the content. Watermarks could also be used to personalize content to a given consumer or a set of consumers.

Metadata

In addition to the actual content, the DRM derives and maintains metadata, which refers to information about the content. It contains information such as content type, content ID, encryption details, and information about the rights. Metadata can be broadly classified as content-descriptive metadata and content-dependent metadata. The content-descriptive metadata contains information such as data format, layout format, the various components that the content is made of, and author information. The content-dependent metadata contains information pertaining to what is in the content, such as the keywords for the topical coverage of an e-book or the type of video documentary. The metadata is used for locating the content and management of content usage. There are several issues related to the format and structure of the metadata itself and their standardization. The Dublin Core Metadata Initiative (DCMI) is a prominent metadata standardization effort. Other initiatives are focused on interoperability (e.g., Information Content Exchange—ICE) and educational content (e.g., Instructional Management Specification—IMS).

Rights object and usage rights

A rights object, or rights, clearly specifies the permitted ways the associated content can be used by the consumer or device. Each rights object has an associated syntax and semantics, which is specified by a rights expression language. Rights expression languages enable expressing the terms and conditions of content usage in a clear and unambiguous manner. Prominent efforts in the development of such languages are the Open Digital Rights Language (ODRL) initiative and the Extensible Rights Markup Language (XrML). The rights manager is responsible for creating the rights objects and for packaging the rights with a key.

The content adheres to a format, known as DRM content format. The content, together with an associated rights object, is referred to as a DRM message. The consuming device renders the content in a form based on the rights object included in the message. In the absence of a rights object, a default set of rights is applied. The content provider can define explicit rights for various cases.

There are several different types of usage rights: expiration date, which specifies the date beyond which the content cannot be rendered (played); starting date, before which the content cannot be played; ending date tied to starting date, which specifies that the content is valid for a certain number of days from the date the content is first used; counted playback, which specifies a certain number of times the content can be played back; device types, which specifies the devices on which the content can be played; and media operations, which specify if the media could be transferred to a CD or transferred over the network to another device.

License generation

The license contains the rights object, which contains the terms and conditions related to the usage of the content. The license also contains the key required to unlock the content in case it is protected. Using a key seed, which is known only to the content owner (producer) and license provider (manager), and a key ID, a key is produced using a key-generation process. This key is used by the content owner/producer to encrypt the content when needed. The key is also packaged along with the rights object to generate the license. An overview of this process is shown in Fig. 3.

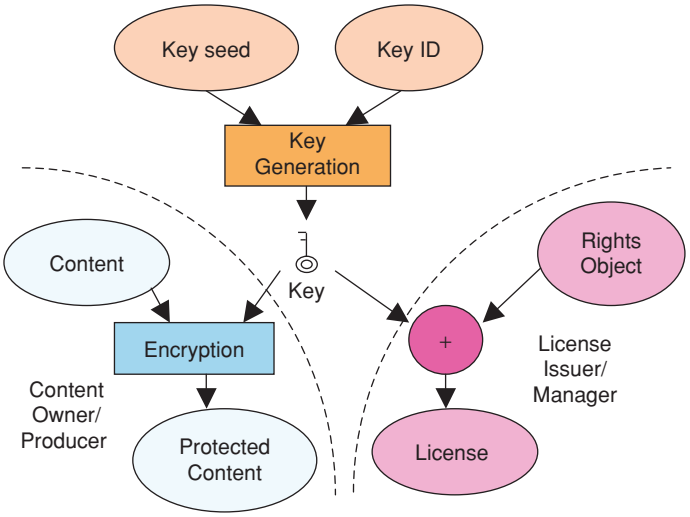


Fig. 3 Key generation and use of key in content protection and license generation

Only upon meeting the terms and conditions in the license is the use of content enabled. The license could be packaged along with the content or sent separately. The delivery of the license could be implicit, in which case the user will not be aware of the license delivery process. Or it could be explicit, in which case the user has to actively participate, perhaps by filling out some forms and providing relevant information. The license is nontransferable. The license could be renewed upon a request, subject to satisfactory conditions of content usage and payment. The license could be revoked when the terms of the license are violated, which renders the content unusable.

Broad outline of a DRM system operation

An overview of the major operations in a typical DRM system is shown in Fig. 4. Some of the information in the content metadata, which are required for license generation, is sent from the content server to the license server.

The devices (users) make a request to the content server for the desired content. If the content is packaged with the license, which is possible in case the device/user characteristics, requirements, credentials, and payment information are known beforehand, then it could be used by the devices immediately. Otherwise, a license needs to be generated after getting the required information from the user/device and before the content can be used. The content has a header that typically could consist of the license acquisition URL (the URL of the Web page of the license provider); the content ID, which uniquely identifies the content; content metadata such as author, title, descriptions, types of license; some user defined attributes; DRM version information; and the key ID. These are used by the devices and applications for appropriate rendering of content.

The license can be obtained explicitly, when the device makes a license request, or implicitly, when the device attempts use the content. The device sends information about its characteristics (such as resolution and read/write capabilities), credentials (device serial number, IP address, if any), intended usage (number of times to play, to make a backup copy), and payment information. The license server uses the above information received from the device together with relevant information from content metadata to generate the rights object for the particular combination of content and intended usage. It then packages the rights object and the key (required to recover the content in case it is protected), produces the license, and sends it to the device. The device will now be able to consume the content based on the rules specified in the license.

The major issues that need to be addressed include the interoperability of content format, secure delivery of content, the privacy of consumers, unambiguous specification of the rights objects (for example, in the case of counted operations, what happens if the content playback is stopped half-way through?

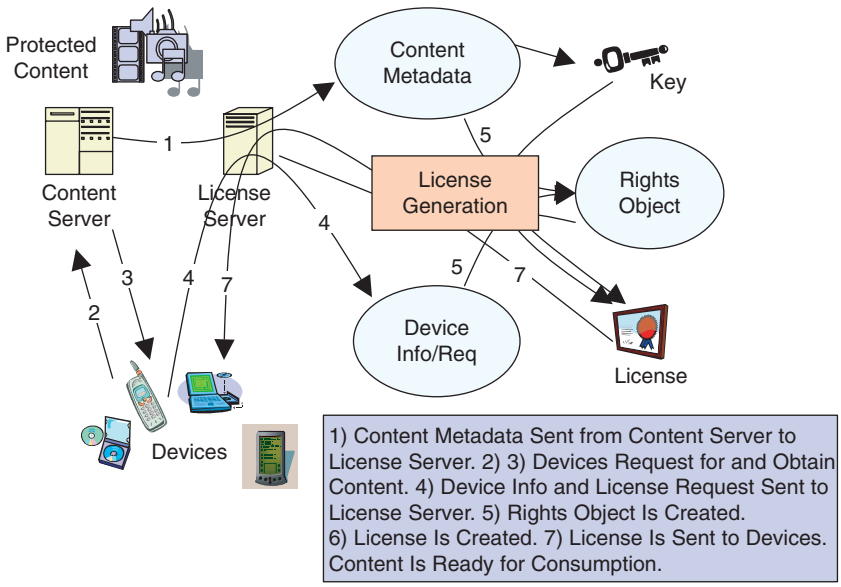


Fig. 4 Overview of major operations in a typical DRM system

Will it be counted as a play back or not?), and the evolution of standards.

Conclusions

DRM is intended to provide a framework and a set of policies, technologies, techniques, and tools for the management of the appropriate and fair uses of digital content. It could be a valuable tool for content creators, developers, and producers as well as for consumers. There are not many commercial systems currently in operation. There are many open issues related to DRM that need to be addressed before it can have widespread use. A set of standards related to various aspects of DRM are still being worked on in order to ensure fairness, interoperability, and consumer confidence.

Read more about it

- B. Rosenblatt, B. Trippe, and S. Mooney, *Digital Rights Management: Business and Technology*. New York: M&T Books, 2002.
- D. Austerberry, *Digital Assent Management*. New York: Focal Press, 2004.
- A. Mauthe and P. Thomas, *Professional Content Management Systems: Handling Digital Media Assets*. New York: Wiley, 2004.
- J.S. Erickson, (2001, Apr.). "Information objects and rights management," *D-Lib Mag.*, [Online]. www.dlib.org/dlib/april01/erickson/04erickson.html
- R. Iannella (2001, June). "Digital rights management architectures" *D-Lib Mag.*, [Online]. www.dlib.org/dlib/june01/iannella/06iannella.html
- M. Stefik, "Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing," *Berkeley Law J.*, vol. 12, no. 1, pp. 137-159, 1997.
- K. Coyle, *The Technology of Rights: Digital Rights Management*. [Online]. Available: *http://www.kcoyle.net/drm_basics1.html*
- IETF Internet DRM Working Group. [Online]. Available: http://www.idrm.org.

About the authors

S.R. Subramanya obtained his Ph.D. in computer science from George washington University where he received the Richard Merwin memorial award from the EECS department in 1996. He received the Grant-in-Aid of Research award from Sigma-Xi in 1997 for his research in audio data indexing. He is a senior research scientist at LGE Modile Research in San Diego. His current research interests include mobile multimedia services and content management. He is the author of over 70 research papers and articles. He is a Senior Member of the IEEE.

Byung K. Yi obtained his Ph.D. in electrical engineering from George Washington University. He is the senior executive vice president of LG Electronics in San Diego. Dr. Yi's previous affiliations include Orbital Sciences Corp., Fairchild, and several high technology companies. He is a Senior Member of the IEEE.