A DRM Framework for Distributing Digital Contents through the Internet

Junseok Lee, Seong Oun Hwang, Sang-Won Jeong, Ki Song Yoon, Chang Soon Park, and Jae-Cheol Ryou

This paper describes our design of a contents distribution framework that supports transparent distribution of digital contents on the Internet as well as copyright protection of participants in the contents distribution value chain. Copyright protection must ensure that participants in the distribution channel get the royalties due to them and that purchasers use the contents according to usage rules. It must also prevent illegal draining of digital contents. To design a contents distribution framework satisfying the above requirements, we first present four digital contents distribution models. On the basis of the suggested distribution models, we designed a contract system for distribution of royalties among participants in the contents distribution channel, a license mechanism for enforcement of contents usage to purchasers, and both a packaging mechanism and a secure client system for prevention of illegal draining of digital contents.

Keywords: Digital rights management (DRM), MPEG-21, contract, license, distribution business model, security, packager, usage rule.

Manuscript received Feb. 21, 2003; revised May 7, 2003.

Junseok Lee (phone: +82 42 860 1036, email: leejs@etri.re.kr), Seong Oun Hwang (email: yjjeong@etri.re.kr), Sang-Won Jeong (email: senator@etri.re.kr), Ki Song Yoon (email: ksyoon@etri.re.kr), and Chang Soon Park (email: cpark@etri.re.kr) are with Computer Software Laboratory, ETRI, Daejeon, Korea.

Jae-Cheol Ryou (email: jcryou@home.cnu.ac.kr) is with the Internet Intrusion Response Technology Research Center (IIRTRC), Chungnam National University, Daejeon, Korea.

I. Introduction

The traditional industry for multimedia contents distribution and consumption has focused on physical economy. Movies and music albums have been produced through complex and difficult technologies and delivered to customers through distribution networks using various types of containers, such as reel tapes, videotapes, and CD-ROMs. However, with the introduction of digitized multimedia contents production and the distribution of various production tools, contents production has become easier and faster than ever before. The prevalent use of high speed Internet has also changed the structure of contents consumption. Thus, current efforts are focusing on systematizing the online structure of the production, distribution, and consumption of digital contents.

There are two types of contents distribution systems. Microsoft and Adobe, representing the first type, now produce contents distribution systems that support only their own media types based on their renderers, MS's Window Media Player and Adobe's Acrobat Reader. The makers of the second type of contents distribution systems use their own renderers regardless of the types of contents. InterTrust, ContentGuard, and IBM belong to this category. All the above systems can only support distribution between media distributors and purchasers; they cannot support the whole value chain that includes creators, rights holders, contents providers, media distributors, and purchasers.

Regardless of which digital rights management (DRM) framework is adopted, charge-based content distribution models, such as payout, subscription, and pay per view, have not gained popularity for two reasons. First, creators of contents are not sure that their work is protected under the

copyright. Second, creation of high quality contents is more difficult under these models. For these reasons, it is crucial that the design of a DRM framework guarantees the rights of all parties to the distribution system.

However, existing DRM systems focus on the relationship between media distributors and end consumers. This paper extends the idea of DRM to the complex interactions among all the parties involved in the process of producing content. At this point, even the MPEG-21 framework does not adequately reflect the relationships among all these parties.

Section II.1 defines the terms relating to DRM, which are different from their usual use because they are not yet used commonly in the academic world, and section II.2 explains the relations among the DRM standardization activities. Section III suggests four detailed distribution scenarios for digital contents considering real world distribution channels and explains the difficulty in protecting the rights of the parties of the distribution when the scenarios are implemented on the basis of the MPEG-21 distribution model. We propose a new distribution model to overcome this difficulty. Systems used to implement the DRM framework need many technologies. Section IV explains the designs of the important parts of the systems, section V analyzes the designed DRM framework as to whether it performs the functions, and section VI explains the difference between the DRM framework in this paper and other DRM systems.

II. Related Studies

1. Definition of Terms

This section defines three important terms because these terms have never been clearly defined academically.

• The Digital Rights Management (DRM) Framework

As defined in this paper, a DRM framework enables secure and transparent distribution of digital contents while protecting the rights of creators, rights holders, creation providers, media distributors, and purchasers. Technically, it is defined as a set of technologies and systems that can collectively support the entire life cycle of contents - creation, manipulation, distribution, and consumption - by preventing illegal copying, imposing fees, processing payments, tracking contents, and protecting each principal's rights and profit [1].

• Packaging and Secure Container

Packaging binds contents and metadata; this includes usage rules, distribution information, contract information, and the digital signature [2]-[5]. This means that the contents and the metadata are encrypted or signed using a key that the certificate authority publishes. The result is called a secure container. This function is closely related to certificate authority and license processing.

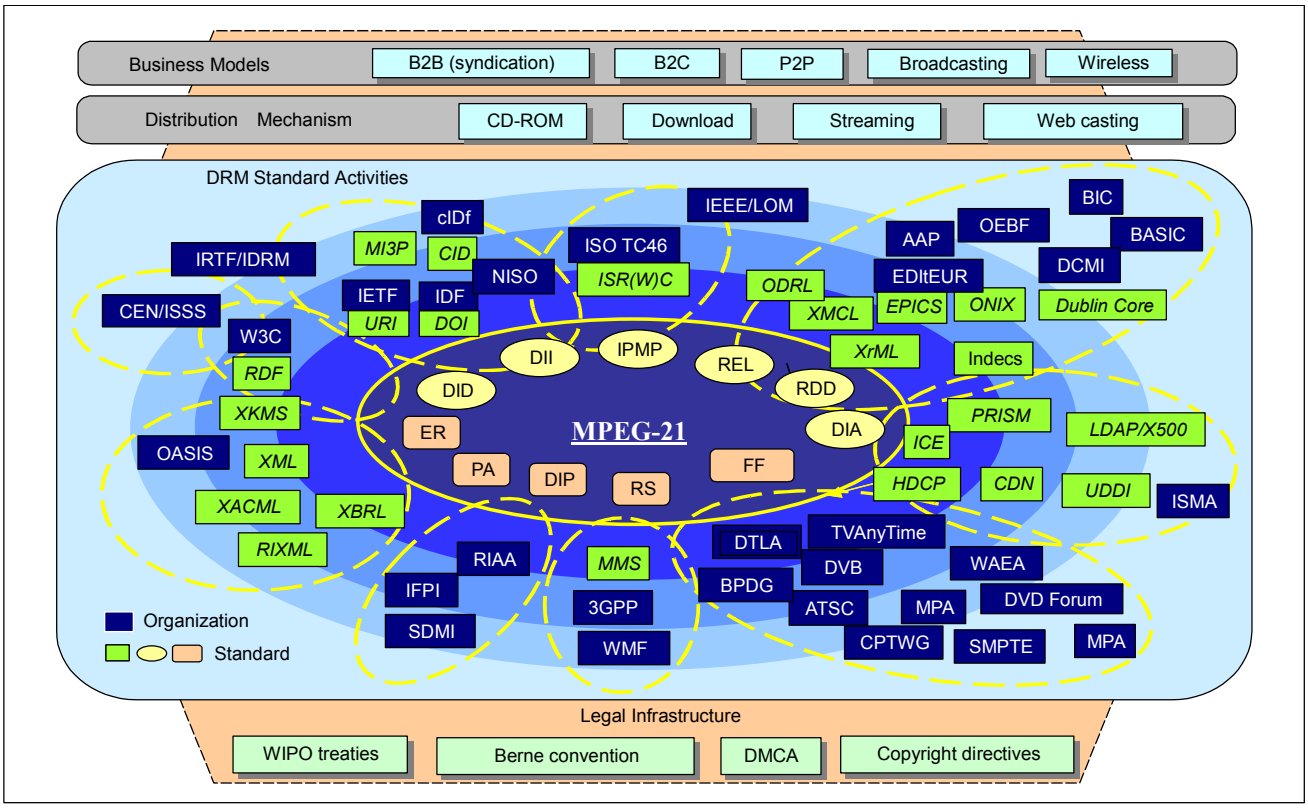

Fig. 1. Standardization schemes in the center of MPEG-21 activities.

• Digital License

A digital license permits a purchaser to do some action (print, play, copy, etc.) using contents. The license includes the key to decrypt the contents, usage rules that describe the period and what kinds of actions the user may make, and so on.

2. Standard

DRM-enabled contents distribution is related to legal infrastructures, standardization, distribution mechanisms, and business models (Fig. 1).

Legal infrastructures such as those of [6]-[9] aim for balance between the appropriate revenue of rights' owners and the interest of individual users.

A DRM framework needs complex technologies as well as standardization to make the parts interoperable. To date, almost all DRM standard activities have been done within various technical areas and genre (media) domains, though some DRM standard activities, like the Open Digital Rights Language Initiative [10] and Extensible Rights Markup Language (XrML) [11] focus on the generic domain. However, there are gaps among these standards and technologies. MPEG-21 deals with these problems. The goal of MPEG-21 is to identify and fill the gaps among various technologies by developing a new standard. Figure 1 depicts various standardization schemes where MPEG-21 is central to the activities.

Part 1 of MPEG-21 starts with setting the vision, technologies, and strategy [12].

Part 2, the digital item declaration, gives the digital items that are objects of transactions [13].

Part 3, the digital item identification, deals with identification of digital items [14].

Part 4 discusses interoperable intellectual property management and protection, which standardizes messages among intellectual property management and protection tools, such as watermarking, authentication, fingerprinting, and so on [15].

Parts 5 and 6 cover rights expression language and the rights data dictionary [16], [17]. Rights expression language defines the standardized syntax and the rights data dictionary defines the standardized terms. These two parts together allow the expression of rights information in a standardized manner.

Digital item adaptation in part 7 allows contents to be adapted while in transit or when offered to users [18].

MPEG-21 goes further to standardize other parts: reference software about implementation in part 8, file format about the structure of MPEG-21 data in part 9 [19], digital item processing in part 10 [20], persistent association for watermarking in part 11 [21], and event reporting [22].

MPEG-21 uses existing standards to integrate the various technologies and fill in gaps. For instance, terms from descriptive schemes such as the online information exchange (ONIX) [23] and Dublin Core [24], are integrated with the rights data dictionary. XML syntax and the resource description framework [25] are exploited by the digital item declaration. Digital item identification allows for existing ID systems, such as content ID [26], the digital object identifier [27], and the unique material identifier [28]. The rights expression language is based on XrML, which is derived from the digital property rights language [29].

A distribution mechanism, which is how to distribute contents from the media distributors to the purchasers, has to be considered to implement the DRM framework. Different distribution mechanisms result in differences, such as different packaging methods, different license mechanisms, and so forth. This paper considers only the download method.

The contents business model includes business to business, business to consumer, peer to peer, broadcasting, and wireless. Each model has various complex business models according to the contents characteristics, established distribution structure, and revenue earning mechanism. Technologies are needed according to the business models. This paper is restricted to the Internet and considers business to business, business to consumer, and peer to peer business models.

III. Proposed Distribution Model

1. Distribution Scenarios

MPEG-21 defines a business model well based on the roles of distribution parties [30], but it cannot support complex and various distribution models of the real world in detail. This section presents in detail four scenarios for digital contents distribution for the Internet based on the business model of MPEG-21. The current DRM system considers superdistribution, but we propose a model that considers the distribution of physical contents.

• Superdistribution [31]

A purchaser provides other purchasers with contents that the purchaser bought from media distributors. This scenario may be implemented with a license mechanism and an ID-based mechanism [32].

• Compound Content Distribution

The role of the creation provider is to create distribution contents. At this time, the creation provider makes a content using several original contents that creators provide. The distribution contents are called compound content in this paper.

• Bundle Content Distribution

Media distributors bundle several distribution contents that creation providers provide.

The difference between compound content and bundle content is as follows. Compound content creates one content where several contents are mixed, for example, an e-book. Only one usage rule exists for the compound content. However, in bundle content, several contents exist independently and are just wrapped in order to make one content including music, musical notes, or the words of a song. Separate usage rules exist for bundle content.

- Many Steps Distribution

Media distributors can sell their distribution contents to other media distributors. We see this scenario in the real world when wholesale merchants sell their contents to retail dealers.

2. Weakness of the MPEG-21 Business Model

The world of digital contents distribution needs a distribution framework that distribution parties can trust, even though they do not know each other. It is very important to ensure that royalty distribution is made fairly among the parties. It is also important to provide detailed information that can serve as evidence in court in case of disputes.

The following explains the problem of considering only royalty distribution in the MEPG-21 business model when the detailed business models in section III.1 are implemented; this case has a complex relation of rights.

- In the relation between the media distributor and rights holder, the media distributor receives payment from purchasers and sends log information to the monitoring service provider. The media distributor distributes royalties to the rights holders. The rights holders get log information from the monitoring service provider. However, we cannot ensure that the rights holders receive their royalties from the media distributors because it is the media distributor that sends log information to the monitoring service provider and also distributes royalties to the rights holders.
- The same problem exists in the relation between rights holders and creation providers and in the relation between rights holders and creators.
- In case of a rights dispute, no distribution party can present legal data in court.

3. Proposed Distribution Model

The proposed model was designed with the following three important considerations.

First, huge quantities of contents exist on the Internet but much of that content is not of high quality. This is a current problem. Before the problem can be solved, the rights of distribution parties have to be protected. This requires that fair and exact royalties be distributed. If this is achieved, distribution parties can open high quality contents on the Internet.

Second, we cannot technically support all possible distribution models, so we need to select and support some of them. In this paper, we consider the four scenarios described earlier.

Third, this paper assumes that the possibility of illegal contents usage increases as the digital contents distribution progresses from the creator to the purchaser. To prevent illegal contents usage, we apply contract, watermark, and encryption mechanisms step by step as in Fig. 2.

Our distribution model is based on MPEG-21 [30] (Fig. 2). The big differences from the MPEG-21 business model are the distribution information management system (DIMS) and the clearing house instead of the monitoring service provider. In some papers, the clearing house is called the broker [33].

- Functions of the distribution information management system
  - Supports a contract mechanism.
  - Maintains programs for interoperability like packaging, metadata editor, client toolkit, and watermarking [34], [35].
- Functions of the clearing house
  - License processing: Enables the purchaser to play contents according to the usage rules in the license and protects contents themselves from illegal attacks.
  - Financial management: Receives payment from the purchaser and distributes royalties to related parties of the contents distribution chain.
  - Event management: Manages usage history.

The following briefly explains digital contents distribution according to the numbered arrows in Fig. 2.

Step 1. The rights holder, creation provider, and media distributor have to get public key certificates from the certificate authority.

Step 2. When a creator provides creations and metadata to a rights holder, they sign a contract. At this time, the DIMS serves as an intermediary in the contract process. The DIMS keeps the contract. When the media distributor sells the contents, the clearing house distributes the royalties to the creator and the rights holder, getting the contract information from the DIMS.

Step 3. In the same way, when the rights holder gives contents to the creation provider, the rights holder and the creation provider sign a contract. The DIMS also provides a mechanism for the rights holder to write metadata. When the mechanism is used, metadata represented as XML is created and loosely coupled with the content.

Step 4. The creation provider receives a unique number from the DIMS and makes the distribution content and metadata, including the unique number, available for sale and inserts a

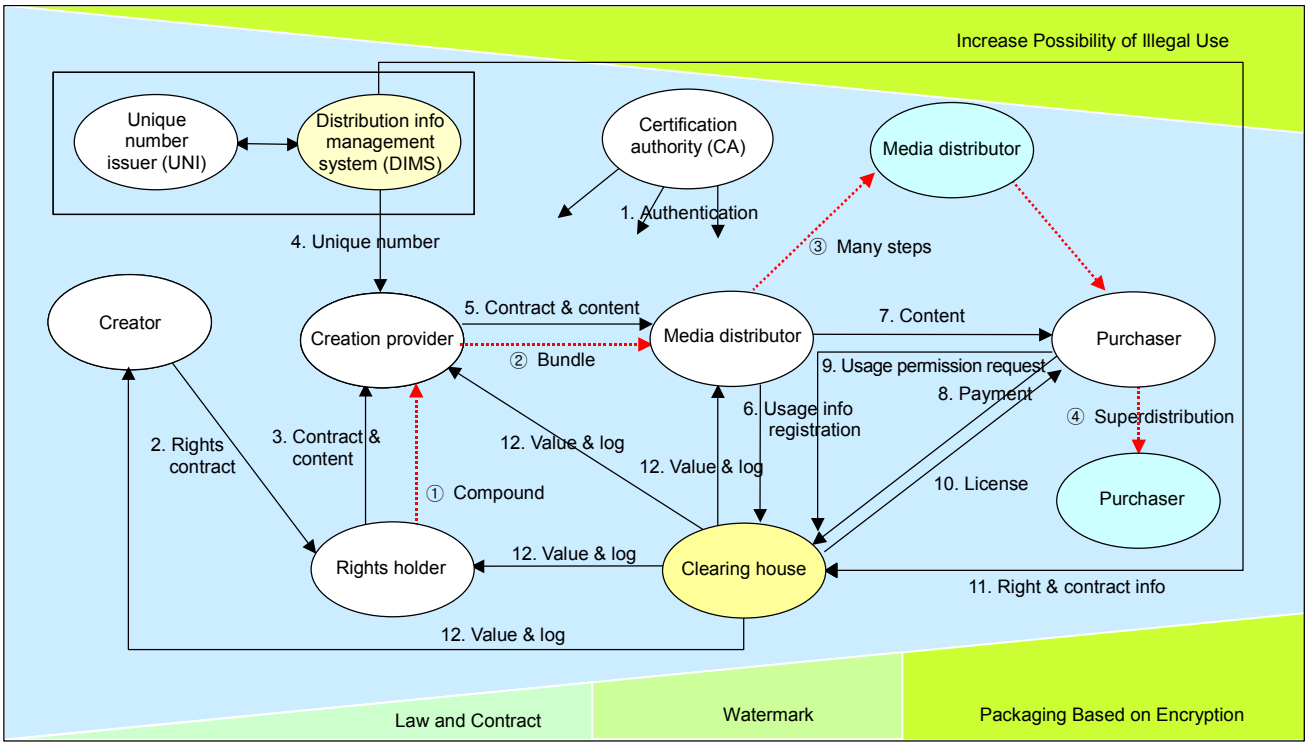

Fig. 2. Proposed distribution model.

watermark in the distribution contents using a watermarking tool provided by the DIMS. Based on the unique number, the DIMS can figure out which contents are distributed under which contract conditions.

Step 5. The creation provider then contracts with the media distributor. If the creation provider gives packaged contents to the media distributor [36], the business model for bundle content distribution is restricted and the secure container cannot include information that the media distributor needs to decide such things as sale policy and location of the secure container for superdistribution.

For compound content, the DIMS checks whether previous contracts have been violated and whether the creation provider can contract with the rights holders again if needed (① in Fig. 2).

Step 6. The media distributor packages the distribution content with metadata using an encrypted key and provides the clearing house with usage rules and the unique ID, as well as part of the key.

Step 7. Media distributors sell their contents to purchasers.

For selling bundle content, the media distributor defines each price and each usage rule for contents in the bundle content so that the clearing house issues a license for all the bundle content as well as licenses for each item of contents in the bundle content (② in Fig. 2). The media distributor can contract with other media distributors if the new contract does not violate a previous contract (③ in Fig. 2).

Step 8. The purchasers pay the bill through a web page that is made by a toolkit program that a payment company supports.

Step 9. The client DRM program sends a usage permission request to the clearing house through the media distributor.

Step 10. The clearing house provides the purchaser with a license that includes the decrypted key and usage rules determined according to a fee policy.

When one purchaser gets contents from another purchaser rather than a media distributor, the purchaser has to get a new license (④ in Fig. 2).

Steps 11 and 12. The clearing house distributes the royalties according to the royalty distribution information from the DIMS.

IV. DRM Framework

1. Metadata

Metadata includes the digital object identifier, content information according to each content type, rights information, distributor information, contract information, usage rules, digital signatures, watermarks, etc. However, the metadata does not include information about the original content [37], [38]. Recently, standardization for integrated metadata containing all the above information has not sufficiently progressed but has

progressed only partly as XrML for standardization of usage rules. This means that XrML does not include all the above information, such as contract and distributor information.

The above metadata has to be made out according to the roles of each entity in the distribution chain and managed systematically in every step of the distribution. For example, a creator writes metadata about content information, but other entities in the distribution chain can modify the metadata. In addition, metadata on distribution information can be made out by each entity.

Metadata has to be designed with a hierarchical structure as well as a nested structure, such as in MPEG-21's digital item declaration, to support compound content. The metadata also supports sequential structure for bundle content. Because bundle content is a selling content made by bundling independent contents that are made by the creation provider, the framework must support a structure that bundles the metadata and the contents.

Metadata is closely connected with secure containers and licenses, that is, a portion of the content and distribution information contained in the metadata is included in the secure container, which the purchaser can see in the client environment. The license also comprises a part of all the usage rules, which the purchaser selects based on a fee policy.

2. DIMS Server

The DIMS server consists of two subsystems.

The program service subsystem provides interoperability among different participants of the distribution by authenticating and providing basic DRM programs, such as watermarker, metadata editor, and packager.

Second, for protecting rights of distribution participants, the contract subsystem provides a contract environment to make a contact when a distribution participant gives a license to others. Based on the contracts, the subsystem provides the clearing house with the information necessary to fairly distribute royalties.

A. Contract Technology

The proposed contract subsystem protects the rights of distribution parties from the creator to the creation provider in a value chain. The contract document generated by the subsystem prescribes what kinds of rights to be permitted and how to share revenue. The subsystem provides the clearing house with information that is used to check if the permissions and obligations prescribed in the contract document are fully observed. The subsystem also has to contain detailed information that can serve as evidence in court in case of rights disputes.

The scenario for the contract process in No. 3 of Fig. 2 is described as follows.

Step 1. Authentication of contract parties

The DIMS can authenticate the rights holder and creation provider using their certificates.

Step 2. Make a contract

The rights holder and creation provider open a chat room to negotiate.

The rights holder draws up an actual contract using the contract templates and the contract data dictionary (CDD) offered by the DIMS.

If the creation provider agrees on the actual contract written by the rights holder, both parties provide their digital signatures.

Step 3. Delivery of contents and metadata

The DIMS gets the contract and the contents from the rights holder.

The DIMS gives the contents and results of signing the metadata, including the contract ID, to the creation provider. At this time, a watermark is not inserted into the contents because the creation provider can modify the contents. However, the

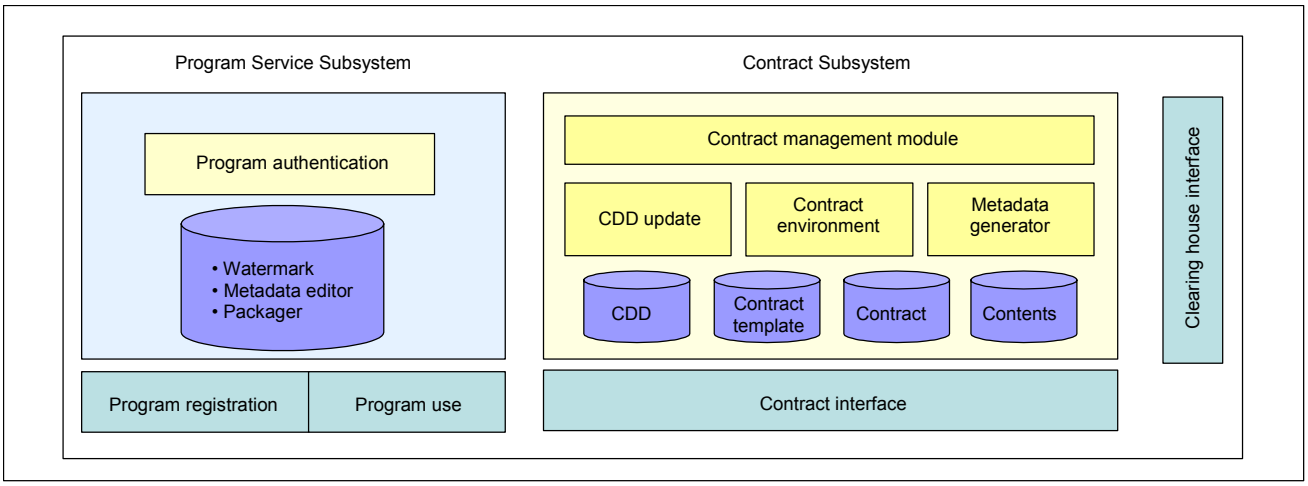

Fig. 3. DIMS structure.

data of the watermark corresponding to the content ID is inserted when the contract between the creation provider and the media distributor is made.

Here we explain the function of the structure elements of the contract subsystem in Fig. 3.

1) CDD Update Module

Using the concept of the rights data dictionary proposed by MPEG-21, a CDD database is made for the elements in relation to the contract.

Table 1 shows an example of a CDD database.

The variable attribute expresses variables that exist in the definition attribute and defines their type.

The faithfulness relation attribute describes the variables for the relations to the next contract if the variables have an effect upon the next contract in the distribution chain. The faithfulness relation is defined as follows. (The prime symbol marks the variable to denote the next contract.)

If the faithfulness relation about the period of contract is $Y' \leq Y$ as in Table 1, the period of contract Y' of the next contract is less than or equal to Y.

If the faithfulness relation about the percentage of royalty is $A' > A$, the royalty percentage A' of the next contract is bigger that A.

If the faithfulness relation about the requirement condition of security hardware is $L' \geq L$, the requirement condition L' of the next contract is satisfied with L.

The attribute value of the packaging metadata is described with XML tags, which have to be inserted into a secure container when the definition of the contract affects the action of the purchaser and must be enforced on the purchaser. For example, if the definition is "prohibit print of contents," the value of packaging metadata attribute is "<\print> NO."

2) Contents Environment

The contents environment provides an environment to make contract templates using the CDD database and to make actual contracts including the following functions.

- Contractor authentication function
- Function to create online format of contract
- Realtime contract function
  - · A multiparty contract is needed to distribute compound contents and bundle contents.
  - · A multisignature protocol solves the problem of simultaneous contract signatures of the distribution parties. It also provides a time-stamp that confirms the point of signature time.

3) Contract Management Module and Metadata Generator

The contract management module performs a validation check about previous contracts using the faithfulness relation in the CDD database and provides the result of signing metadata, including the contract ID to parties of the distribution [39].

Metadata and content is loosely coupled from the creator to the creation provider as C_1 and C_2 in Fig. 4. This means that no binding is done between the metadata and the content. This is because when the creation provider modifies the content, it causes the information of the watermark to be broken legally.

When the creation provider and media distributor make a contract, metadata and content are tightly coupled as information of the content ID or contract ID that is inserted into the content with watermarking as C_3 in Fig. 4. Even though information on the ID (in the form of binary digits) is embedded using a watermarking technique, it can be retrieved safely and is protected against external attacks to remove it. Error correction code techniques, such as Reed-Solomon, Bose-Chaudhuri-Hocquenghem [40], Turbo, and Low-Density Parity-Check [41], are often combined in this application so that the extraction does not allow any bit loss of the full code [42]. Even though there has been research on watermarking technology that applies to digital documents, the technology is not yet reliable [43].

A metadata generator creates metadata that is inserted into a secure container using the packaging metadata attribute in the CDD database when the creation provider and media distributor make a contract. The metadata is enforced by the

Table 1. Example of CDD database structure.

Classification	Headword	Definition	Variable	Faithfulness relation	Packaging metadata
Period of contract	Period	The period of contract is from X to Y.	X, Y	Y´≤Y	
	Extension	If contractor B does not request to extend the term of contract before X months on paper, the term of contract will extend 2 years.	X	X´>X	
Usage rule	Print	Contractor B cannot provide the contents with condition that purchasers can print the contents.			<print> NO <\print>

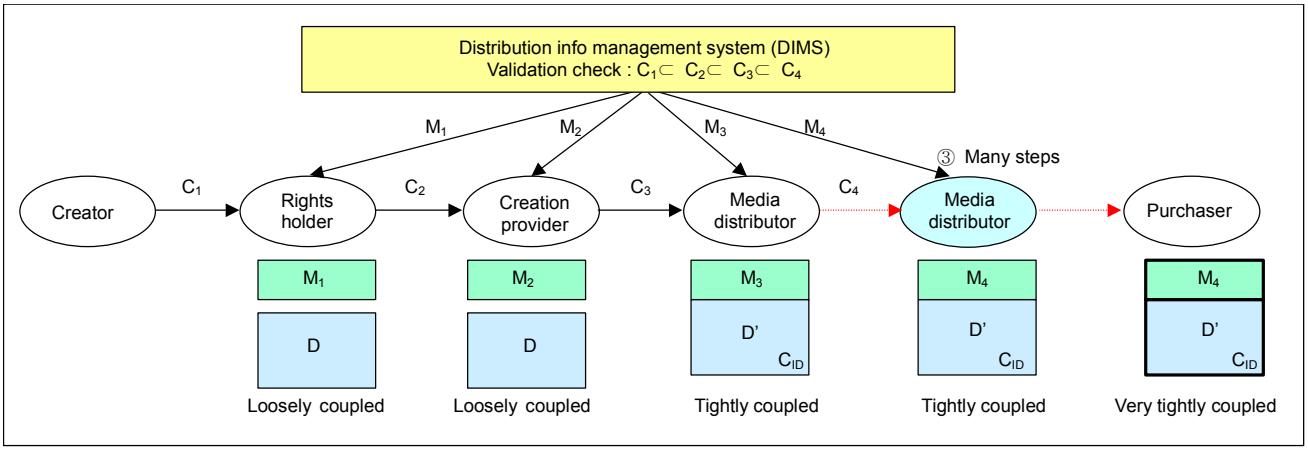

Fig. 4. Contact process.

DRM client program in the purchaser's environment.

When the media distributor sells contents to purchasers, metadata and content are tightly coupled as packaging based on a cipher mechanism.

4) Clearing House Interface

In arrow 11 of Fig. 2, the clearing house can fairly distribute royalties for sold contents as the clearing house obtains information about contracts through the clearing house interface.

3. Packaging & License

This section explains the distribution mechanism among the media distributor, clearing house, and purchaser. At this time, because the media distributor and clearing house are independent of each other, the clearing house cannot see the original contents even if the clearing house publishes a license for the contents.

First of all, this section explains how the media distributor packages contents in view of encryption and then describes what kind of data the media distributor exchanges with the clearing house to issue a license.

The packaging process by the distributors is as follows (Fig. 5):

Step ① The media distributor generates random numbers, such as R_C, R_{CH}, R_D. Using hashing *functions* $f()$, $g()$, $h()$, the media distributor generates keys K_C, K_{CH}, K_D.

Step ② The packaging program gets both raw contents and keys K_C, K_{CH}, K_D as input and puts the encrypted results into a secure container through the following process of encryption.

E_{Kc}[Content]: encryption of content under key K_C

$E_{Kd}[E_{KcH}[K_C]]$: double encryption of K_C under key K_{CH} first, then K_D

Step ③ When the packaging program in the media distributor registers sales contents at the clearing house (arrow 6 in Fig. 2), the program gives an encryption key such as $E_{Ku\text{-}CH}[C_{ID} \mid R_{CH}]$ to the clearing house, so that the clearing

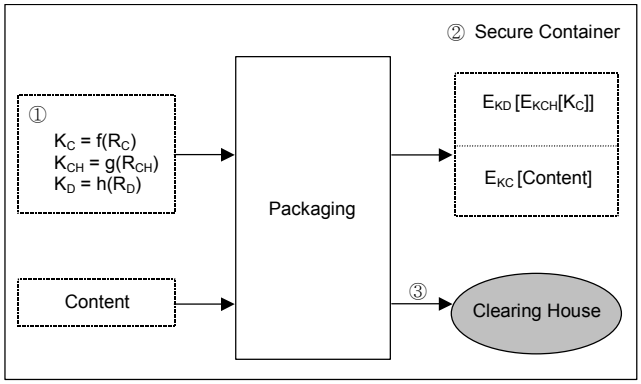

Fig. 5. Key generation and packaging process.

house can make a license in the following way.

$E_{Ku\text{-}CH}[C_{ID} \mid R_{CH}]$: encryption of C_{ID} (that is, Content ID) and R_{CH} under the public key of the clearing house.

Figure 6 shows the process for purchasing contents and for issuing licenses. Arrows 9 and 10 in Fig. 2 correspond to arrows ④, ⑤, ⑥ in Fig. 6.

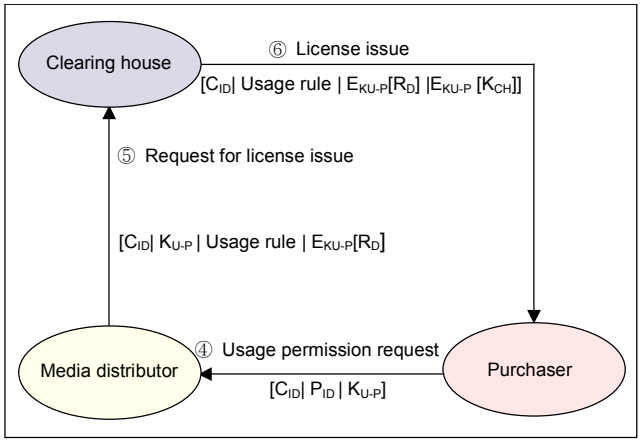

Fig. 6. License issuing process.

Step ④ Request usage permission: [C_{ID} | P_{ID} | K_{U-P}].

After payment, a program of the DRM client, which is installed in the PC of the purchaser, provides information, such as the content ID, the purchaser ID, and his or her public key K_{U-P}, for the media distributor.

Step ⑤ Request issuance of license: [C_{ID} | K_{U-P} | Usage Rule | $E_{Ku-P}[R_D]$].

The media distributor provides the clearing house with information, such as the content ID, the purchaser's public key K_{U-P}, chosen usage rules, and the encryption of R_D, generated as in Fig. 5 under the purchaser's public key.

Step ⑥ Issue the license: [C_{ID} | Usage Rule | $E_{Ku-P}[R_D]$‖ $E_{Ku-P}[K_{CH}]$].

The clearing house issues a license that includes the content ID, the chosen usage rules, the $E_{Ku-P}[R_D]$ that was supplied by the media distributor in step ⑤, and the encryption of K_{CH} under the purchaser's public key.

When the purchaser receives a license, the program of the DRM client can decrypt $E_{KD}[E_{KcH}[K_C]]$ in a secure container (② in Fig. 5) as follows: Both K_D and K_{CH} can be retrieved by decrypting $E_{Ku-cL}[R_D]$‖ $E_{Ku-cL}[K_{CH}]$ within the license using the purchaser's private key. By double decryption of $E_{KD}[E_{KcD}[K_C]]$ under key K_D, K_{CH} in the order, key K_C can be returned. In conclusion, the packaged contents can be decrypted using key K_C.

There are two important points in designing the license mechanism.

First, we designed the license so that the media distributor and the clearing house may be operated independently. This means that clearing houses are not able to decrypt the packaged contents. Clearing houses must be aware of K_C or [K_D, K_{CH}] to be able to decrypt the packaged contents. However, the media distributor provides the clearing house with the encryption of K_D under the client's public key. Note that the clearing house cannot decrypt the encrypted K_D, so it cannot decrypt the packaged contents.

Second, to decrypt packaged contents, intruders such as hackers, must attack the clearing house as well as the media distributor's system. The intruders have to get K_D and K_{CH} in order to decrypt the packaged contents. However, the media distributor does not give all the key information to the clearing house, but gives only K_{CH}. The media distributor then deletes K_{CH} from the database.

4. The DRM Client

The DRM client must protect the contents, audit trail, contents usage counts, decryption key, etc., from hackers. If the information is managed by the clearing house, there are two drawbacks: there is a performance penalty for connecting to the server each time contents are consumed, and offline contents consumption is not supported [44].

Technology, such as secure memory and tamper resistance, is needed for the DRM client system. However, this paper focuses on rendering existing contents using existing viewers, enabling them to be used under predetermined usage rules, and preventing any possible illegal reproduction or copyrights infringement.

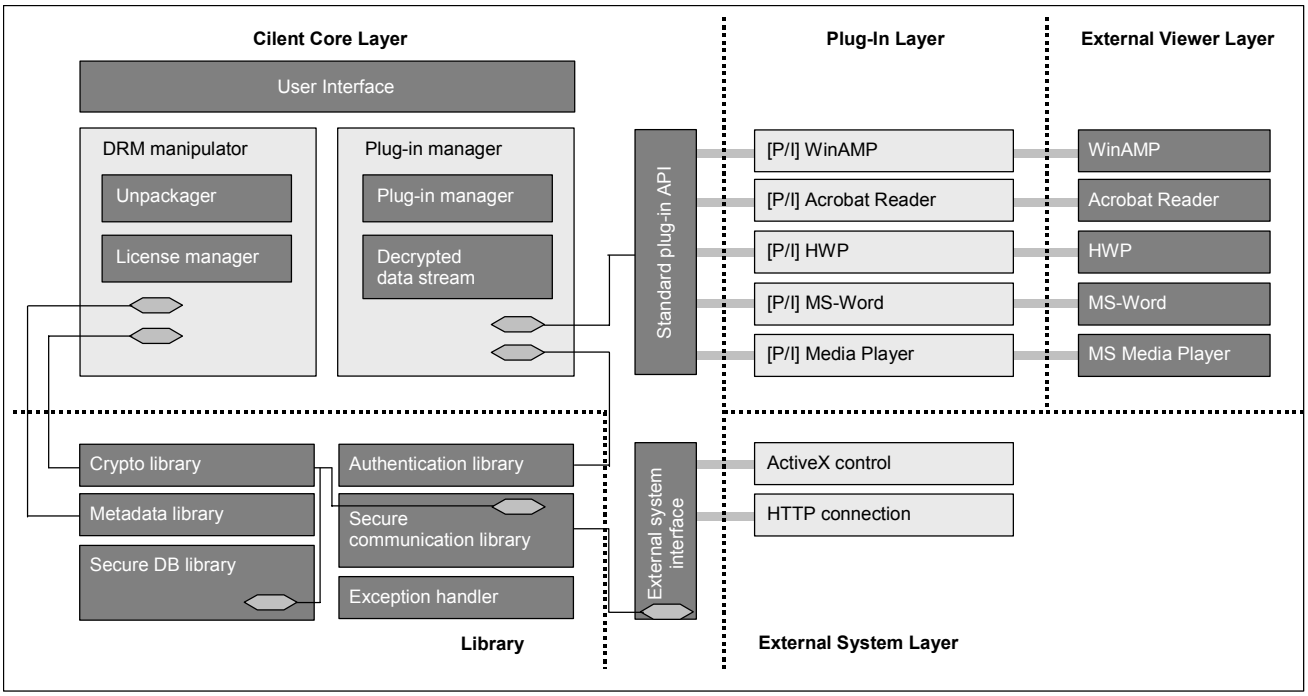

Fig. 7. DRM client structure.

Figure 7 shows the structure of the DRM client system that is installed in the purchaser.

• DRM Core Layer

As a program for controlling all the DRM client modules, the DRM core layer performs metadata parsing, control of renderers, decryption of package contents, permission for using contents, etc.

• Plug-In Layer

The plug-in layer enforces the policy of contents usage to renderers. The policy of contents usage is decided as the DRM core layer parses the license or uses information in a secure database. Plug-in is the easiest and safest method for controlling existing renderers, like not-copy, not-print, and control of usage count. However, the plug-in approach may have a limit. If the existing renderer does not support a plug-in mechanism, it can be implemented with a system programming approach.

• External System Interface

The external system interface provides links between the DRM client software and external systems, such as the DIMS and the clearing house.

When implementing the plug-in mechanism, special regard must be paid to the two following factors.

The first is how to deliver decrypted contents to external renderers. It is here that original content is most susceptible to hackers. The first method to overcome this liability is memory streaming, which directly gives decrypted data blocks to redererers through memory. The second method is filter driving. When a plug-in program intercepts an I/O request from renderers, the DRM client program decrypts the data block that the I/O request instruction requests in realtime, and the data is passed to the renderers through an I/O file system at the kernel level.

The second method is monitoring actions in relation to usage rules in the renderer. This is crucial for defining usage rules for the purchaser. The first method uses tools (for example, SDK/API) for the renderer itself to provide, such as Acrobat Reader and WinAMP. In the second method the rendering module is made with ActiveX supported by the renderer, such as the DOC and HWP, and the OLE container wraps the rendering module, and the OLE container catches events from the ActiveX program. The third method uses a hooking mechanism that intercepts events between renderers and an operation system like the MS Media Player.

Of the above methods, the mechanism of memory streaming and tools like SDK are the safest. However, the mechanism has to be supported by the renderer.

V. Analysis

This section explains whether the function of the DRM framework, which we defined in section II, is performed. We describe a fact and a hypothesis and redefine the detailed functions of the DRM framework based on our predefinition in section II. We will also explain how the distribution parties can perform the detailed functions using the proposed DRM framework.

The role of creation provider in the business model allows for fact 1.

Fact 1. The creation provider can create new contents by modifying the contents that the rights holder gives.

There is a reliable institution that protects the copyrights of analog contents in the real world. The creators or the right holders register their analog contents to the institution off-line. Therefore, hypothesis 1 is reasonable. Also, the clearing house must be operated by a reliable institution because the clearing house manages the payment process that purchasers take part in.

Hypothesis 1. The DIMS and the clearing house are operated by reliable institutions.

The goal of the proposed DRM framework is to protect the copyrights of distribution parties. Requirement 1 defines what kinds of functions the DRM framework has to meet in order for that goal to be satisfied.

Requirement 1 for the functions of a DRM framework.

$Security_1$: Prevent distribution parties from intentional illegal draining of contents.
$Security_2$: Prevent hackers or administrators from illegal draining of contents.
$Security_3$: Prevent purchasers from illegal draining of contents and compel purchasers to observe usage rules.
$Security_4$: Verify a copyright when illegal distribution of contents occurs.
$Security_5$: Detect illegal distributors.
$Security_6$: Create a chain of contracts in which later contracts observe the previous contracts.
$Transparent_1$: Provide sales reports to related distribution parties.
$Transparent_2$: Distribute royalties to related distribution parties.
$Type_1$: Support existing types of contents.

Section II defined the DRM framework as "enables secure and transparent distribution of digital contents …."

"Secure" means "not to make illegal use of contents" and "to abide by a contract." Regarding when the illegal use is prevented, the methods of preventing illegal use are classified as before and after arising. The methods for before-arising

prevention are classified according to performers of illegal use, such as the distribution participant, hacker, administrator, and purchaser (*Security*$_{1,2,3}$ in requirement 1). The methods for after-arising prevention can be divided according to detecting which subjects, such as a copyrighter or an illegal distributor (*Security*$_{4,5}$ in requirement 1). However, we do not consider fingerprint technology for *Security*$_5$ in this paper. Security6 is required to support the value-chain of distribution that allows making a new contract without violating the previous contract.

The meaning of "transparent" is "all the distribution participants related to the selling contents can see the sales report" and "all the distribution participants can receive the royalties due to them" (*Transparent*$_{1,2}$ in requirement 1).

It is very important for the DRM framework to support existing types of contents so that the DRM framework gains popularity in the real world. Thus, we added *Type*$_1$ to requirement 1 of the DRM framework.

Definition 1 defines at which parts of the distribution chain illegal acts can occur; this is related to *Security*$_{1,2,3,6}$. For using the proposed DRM framework, we will explain how illegal acts cannot be committed, except for *Security*$_1$, related to the rights holder and the creation provider.

Definition 1. Distribution subjects (or participants in the contents distribution) in which illegal acts occur.

Rights Holder: *Security*$_1$, *Security*$_6$
Creation Provider: *Security*$_1$, *Security*$_6$
Media Distributor: *Security*$_1$, *Security*$_2$, *Security*$_6$
Purchaser: *Security*$_3$
Clearing House: *Security*$_2$

Metadata and contents have to be tightly coupled to satisfy *Security*$_1$, which is related to the rights holder and the creation provider using strong security mechanisms, such as watermarks, digital signatures, and encryption technologies. However, these technologies cannot be applied because of fact 1: The digital signature on content by a rights holder becomes meaningless if the content can be modified by the creation provider later. Additionally, the above security mechanisms are not needed because of the trust relationship among the creator, the rights holder, and the creation provider in the real world. Nevertheless, if the rights holder and the creation provider distribute contents illegally, a victim can take lawful measures using the contract document in the proposed DRM framework.

However, if the media distributor sells the contents illegally, the DRM client program can detect the illegal contents because the creation provider provides the contents and metadata coupled tightly.

For *Security*$_6$, the proposed DRM framework can enforce previous contracts because the rights holder, the creation provider, and the media distributor use a reliable DIMS to make a new contract according to hypothesis 1.

For *Security*$_2$ related to hackers, the hacker knows that the target content of attacks exists in the system of the media distributor because the system is open on the Internet. For this reason, the system usually saves the original contents in an off-line device. The important issue in designing a DRM framework is how to manage the encryption key of the contents (K_C in Fig. 5). The proposed DRM framework does not save the key in the system, and the system has only one key (K_D in Fig. 5) of the two keys being used to encrypt the encryption key of the contents. Therefore, even though the hacker attacks the system, the hacker cannot decrypt the contents because he/she only can get part of the keys.

For *Security*$_2$ related to the administrator, the media distributor can distribute the contents illegally. However, the proposed DRM framework can detect the illegal contents (*Security*$_1$ in requirement 1). The administrator of the clearing house cannot get the original contents because he/she has only part of the decryption keys (K_{CH} in Fig. 5).

Security$_3$ has three detailed functions as follows.

1. Valid purchasers can see or play the original contents.
2. Purchasers can execute the usage rule corresponding to payment.
3. Purchasers cannot get the original contents illegally.

As the DRM framework encrypts the encryption keys (K_D and K_{CH} in Fig. 5) with the public key of the purchaser ($K_{U\text{-}P}$ in Fig. 6), suitable purchasers can see or play the contents.

The media distributor registers usage rules and prices to the clearing house (arrow 6 of Fig. 2). The clearing house checks whether the usage rule (arrow ⑤ in Fig. 6) is suitable for payment and issues a license. The plug-in layer of Fig. 7 enforces the policy of the content usage. Therefore, the purchasers perform the usage rule corresponding to the payment.

Regarding function 3 above, the contents are saved at devices in a packaged status, and important information is saved in a secure database. Therefore, the purchaser cannot get the original contents.

Definition 2 defines which participants of the distribution chain perform the functions in *Transparent*$_{1,2}$ and *Type*$_1$. In the following, we explain how the proposed DRM framework performs the functions.

Definition 2: Subjects of performing the functions.

Clearing House: *Transparent*$_{1,2}$
Purchaser: *Type*$_1$

The clearing house collects the fee of the contents usage, verifies the related distribution participants through the DIMS, reports the sales information, and distributes fees to the participants.

Table 2. Comparison of DRM systems.

	Microsoft	Intertrust	Adobe	Paper
Independence of participants in distribution chain	No	Partially support	No	Support
Value-chain (Sub-business model)	From media distributor to purchaser (superdistribution)	From media distributor to purchaser (superdistribution)	From distributor to purchaser	From creator to purchaser (bundle content, etc)
Encryption mechanism (key exposure)	License (unprotected)	License (unprotected)	Provide encryption to document	License (protected)
DRM client (contents type)	Windows Media Player (video/audio)	Inside viewer (all)	Acrobat Reader (PD)	Support external viewers through standard plug-in architecture (all)

The DRM client structure can support the existing types of contents.

VI. Comparison of the DRM Framework

Table 2 shows a comparison of existing DRM systems and the proposed DRM framework.

The item "independence between participants in the distribution chain" means that mutual trust among participants is supported systematically even though the participants do not know and trust each other.

The item "value-chain" means that the system provides coverage from any participant to any participant in the distribution chain of the MPEG-21 business model. This means that the Microsoft DRM system provides coverage from the media distributor to the purchaser, and the proposed framework provides coverage from the creator to the purchaser. Our proposed framework supports superdistribution, bundle content distribution, compound content distribution, and multistep distribution as a subbusiness model.

The item "encryption mechanism" represents the mechanism used when the media distributor distributes contents to purchasers. At this time, key exposure indicates whether the clearing house can obtain the original contents by decrypting encrypted contents using the key registered by the media distributor.

The item "DRM client" represents what kinds of viewer are used to play contents and what types of contents are supported by the DRM systems.

VII. Conclusion

We proposed four different popular submodels of contents distribution in the real world. We also pointed out the weak points of the MPEG-21 distribution business model from the point of view of protecting the rights of distribution participants and supporting the four submodels. We proposed a new distribution model to overcome the weaknesses of existing models. For our proposed model, we designed critical elements or systems for the DRM framework, such as metadata, contracting, licensing, packaging, and clients, to protect the rights of distribution participants.

However, two important issues of the proposed DRM framework remain unsolved. First, we should consider how to store important information, such as usage history and license information, when designing the DRM client. Second, for the framework to be successful, complete standardization should be established.

Our future research will include the following. First, we will investigate the extent to which the proposed framework should be incorporated in the MPEG-21 standardization activities. Second, we will work on seamlessly integrating the existing research in areas such as distribution chain security without any changes in the framework. Finally, in this work, we limited the framework to the download mechanism for distribution, but we intend to research the streaming and live mechanism because it requires a different packaging method.

References

[1] Bill Rosenblatt, Bill Trippe, and Stephen Mooney, *Digital Rights Management, Business and Technology*, M&T Books, 2002, pp. 79-102.

[2] U. Kohl, "Secure Container Technology as a Basis for Cryptographically Secured Multimedia Communication," *Proc. Multimedia and Security Workshop at ACM Multimedia*'98, Sept. 1998.

[3] Marc A. Kaplan, IBM Cryptolopes™, *SuperDistribution and Digital Rights Management*, http://www.research.ibm.com/people/k/kaplan/, Dec. 1996.
[4] Olin Sibert, "The DigiBox: A Self Protecting Container for Electronic Commerce," *Proc. USENIX'95 Electronic Commerce Workshop*, 1995.
[5] H. Sakamoto, M. Yamada, T. Nakamura, T. Nakanishi, and "Additional Content-Related Service/Product Offering System Based on New Standards: MPEG-21 and Content ID/DOI," *Proc. IEEE Multimedia and Expo'02, Int'l Conf.*, 2002.
[6] World Intellectual Property Organization, *WIPO Copyright Treaty,* 1996.
[7] World Intellectual Property Organization, *Berne Convention,* 1971.
[8] United States copyright law, *The Digital Millennium Copyright Act*, 1998.
[9] European Council, *European Copyright Directive,* 2001.
[10] http://www.odrl.net, ODRL.
[11] http://www.XrML.org, *XrML*.
[12] ISO/IEC TR 21000-1, *Vision, technologies and strategy*, 2001.
[13] ISO/IEC FDIS 21000-2, *Digital Item Declaration*, 2002.
[14] ISO/IEC FDIS 21000-3, *Digital Item Identification*, 2002.
[15] Draft Requirements for MPEG-21, *Intellectual Property Management and Protection*, N5235, 2002.
[16] Text of ISO/IEC CD 21000-5, *Part 5: Rights Expression Language*, N4942, 2002.
[17] Text of ISO/IEC CD 21000, *Part 6: Rights Data Dictionary*, N4943, 2002.
[18] Text of ISO/IEC CD 21000-7, *Digital Item Adaptation*, N5353, Jan. 2003.
[19] ISO/IEC JTC1/SC29/WG11, *Proposal for a new Part: MPEG-21 File Format - Part 9*, N4990, July 2002.
[20] ISO/IEC JTC1/SC29/WG11, *Final Call for Proposals on Digital Item Processing: Digital Item Base Operations and Digital Item Method Language*, N5329, Dec. 2002.
[21] ISO/IEC/JTC1/SC29/WG11, *Requirements for the Persistent Association of Identification and Description of Digital Items*, N5229, 2002.
[22] ISO/IEC JTC1/SC29/WG11, *Draft Requirements for Event Reporting*, N5230, Oct. 2002.
[23] http://www.editeur.org/onix.html, *Online Information Exchange.*
[24] http://www.dublincore.org/, *Dublin Core Metadata Initiatives.*
[25] http://www.w3.org/TR/1999/REC-rdf-syntax-19990222/, *Resource Description Framework Model and Syntax Specification*, 1999.
[26] http://www.cIDf.org, *Content ID Forum.*
[27] ANSI/NISO Z39.84 2000, *The Syntax for Digital Object Identifier*, 2000.
[28] SMPTE Standard 330M-2000, *Unique Material Identifier*, 2000.
[29] http://xml.coverpages.org/DPRLmanual-XML2.html, *Digital Property Rights Language.*
[30] http://www.imprimatur.net, *IMPRIMATUR Business Model,* Version 2.1, June 1999.
[31] R. Mori and M. Kawahara, "Superdistribution: The Concept and Architecture," *Trans. IEICE*, vols.E 73, no.7, July 1990.
[32] J. Jeon and S. Park, "DRM Security Framework:ID-Based Approach for Content Super-Distribution," *SCI*, 2001.
[33] A.O.Waller, G. Jones, T. Whitley, J. Edwards, D. Kaleshi, A. Munro, B. MacFarlane, and A. Wood, "Securing the Delivery of Digital Content over the Internet," *Electronics & Comm. Eng. J.*, vol. 14, Oct. 2002, pp. 239-248.
[34] Sarah Jung, Jongwon Seok, and Jinwoo Hong, "An Improved Detection Technique for Spread Spectrum Audio Watermarking with a Spectral Envelope Filter," *ETRI J.*, vol. 25, no. 1, Feb. 2003, pp. 52-54.
[35] Jongwon Seok, Jinwoo Hong, and Jinwoong Kim, "A Novel Audio Watermarking Algorithm for Copyright Protection of Digital Audio," *ETRI J.*, vol. 24, no. 3, Feb. 2002, pp. 181-189.
[36] E. V. Faber, R. Hammelrath, and F. P. Heider, "The Secure Distribution of Digital Contents," *Proc. Computer Security Applications Conf., 13th Ann.*, Dec. 1997, pp. 16-22.
[37] Young Man Ro, Munchurl Kim, Ho Kyung Kang, B.S. Manjunath, and Jinwoong Kim, "MPEG-7 Homogeneous Texture Descriptor," *ETRI J.*, vol. 23, no. 2, June 2001, pp.41-51.
[38] Chee Sun Won, Dong Kwon Park, and Soo-Jun Park, "Efficient Use of MPEG-7 Edge Histogram Descriptor," *ETRI J.*, vol. 24, no. 1, Feb. 2002, pp. 23-30.
[39] GennDurfree and Matt Franklin, "Distribution Chain Security," *ACM CCS*, 2002, pp. 63-70.
[40] Peterson, W. Wesley, and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed., MIT Press, Cambridge, Mass., 1972.
[41] D.J.C. MacKay, R.M. Neal, "Near Shannon Limit Performance of Low Density Parity Check Codes," *Electronics Lett.*, vol. 32, 1996, pp. 1645-1646.
[42] S. Joo, Y. Suh, J. Shin, and H. Kikuchi, "A New Robust Watermark Embedding into Wavelet DC Components," *ETRI J.*, vol. 24, no. 5, Oct. 2002, pp. 401-404.
[43] Mikhail J. Atallah, V. Raskin, and Christian F. Hempelmann, "Natural Language Watermarking and Tamperproofing," *Information hiding 5th Int'l Workshop*, Oct. 2002, pp. 195-210.
[44] W. Shapiro and R. Vingralek, "How to Manage Persistent State in DRM Systems," *LNCS 2320*, p. 176.

Junseok Lee received the BS degree in computer science from Ajou University in Korea in 1986 the MS degree in computer science from DongGuk University in 1989, and has been studying at Chungnam National University for the PhD degree since 2001. Since 1991, he has been with the Computer Software Research Laboratory of ETRI, where he has been engaged in government-funded projects, such as the EXPO system, distributed open mail system, hybrid messaging system, and so on. He is currently researching DRM-based contents distribution system.

Seong Oun Hwang received the BS degree in mathematics in 1993 from Seoul National University in Seoul, Korea, and the MS degree in computer and communications engineering in 1998 from Pohang University of Science and Technology (POSTECH), Pohang, Korea. He worked as a Software Engineer at LG-CNS Systems, Inc. from 1994 to 1996. Since 1998, he has worked as a Member of Engineering Staff at the Computer Software Technology Laboratory of ETRI (Electronics and Telecommunications Research Institute), where he was previously engaged in the research and development of information security technologies, such as cryptographic algorithms, protocols, and applications. He is now involved in the development project of DRM (Digital Rights Management)-based contents distribution systems where he designs and implements the security architecture of licensing mechanisms.

Sang-Won Jeong received the BA and MS degrees in library & information science from Chung-Ang University in Seoul, Korea in 1995. He worked for the Korea Database Promotion Center as a Researcher from 1998-2002, where he was engaged in standardization of data interchange and sharing and in design and implementation of the National Identification System. Since 2002, he has been working as a Member of Engineering Staff at the Computer Software Technology Laboratory of ETRI. He is now involved in a project on DRM standardization where he designed and implemented the multilingual Rights Data Dictionary system. He is also a member of Data Engineering Committee of TTA (Telecommunications Technology Association).

Ki Song Yoon received the BS degree in shipbuilding engineering in 1984 from Pusan National University in Pusan, Korea. He received the MS and the PhD degrees in computer engineering from City University of New York in New York, USA, in 1988 and in 1993. Since 1993, he has been with the Computer Software Research Laboratory of ETRI, where he has been engaged in government-funded projects, such as the distributed open mail system, hybrid messaging system, and so on. He is now a Principal Member of Engineering Staff at ETRI and is in charge of a project on DRM-based contents distribution systems.

Chang Soon Park received the BS degree in applied mathematics in 1975 from Seoul National University, Seoul, Korea, and the MS degree in computer engineering in 1992 from Yonsei University, Seoul, Korea. He received the PhD degree in computer engineering in 2000 from Chungnam National University, Daejeon, Korea. His doctoral dissertation work involved clustered file systems for multimedia service. Since 1977, he has worked at ETRI, where he has been engaged in government-funded projects, such as the development of a high-speed parallel computer, distributed open mail system, workstation clustering software, realtime OS, and so on. He is now a Principal Member of Engineering Staff at ETRI and is in charge of a project on software component methodology.

Jae-Cheol Ryou received the BS degree in industrial engineering from Hanyang University in 1985, the MS degree in computer science from Iowa State University in 1988, and the PhD degree in electrical engineering and computer science from Northwestern University in 1990. He joined the faculty of the Department of Computer Science at Chungnam National University, Korea, in 1991. He is currently with the Internet Intrusion Response Technology Research Center (IIRTRC), Chungnam National University, Korea. His research interests are Internet security and electronic payment systems.