Content Copyright Protection Technology Needed for Cooperative Broadcasting/Communication Services

Shinji Ishii[†]*, Sadakatsu Muto, Masahito Kawamori, and Katsuhiko Kawazoe*

Abstract

Content distribution involving cooperation between broadcasting and communication services requires permission for the use of copyrighted digital content for both services. Moreover, these permissions must be handled securely by the receiving terminals. This article introduces copyright protection technology that can be applied to server-type broadcasting services for which operating standards are currently being formulated.

1. Copyright protection technology for digital content

The digital content distribution in current use is broadly divided between viewing digital broadcasting using a set-top box (STB) or TV set with a built-in digital tuner and viewing digital content on the Internet using a personal computer. From the perspective of the content user, there is no need to distinguish between digital broadcasting services and digital content distribution over the Internet. However, there are differences in the establishment of services based on TV broadcasting, which began under the guidance of a national policy, and the Internet, which arose through free thinking. Consequentially, there are also technological differences.

2. Copyright protection technology

One of the main differences between digital and analog recording is that digital recording does not degrade the quality and further copies can easily be made from any copy. While these features are major advantages for the user, they make it possible for people to freely copy copyright-protected content for purposes other than personal use, which is not desirable from the viewpoint of a healthy content distribution market. Copyright protection technology is a technological solution for mediating between these two conflicting aspects.

Our aim is to utilize the advantages of both broadcasting and communication to develop an optimal hybrid system.

Examples of broadcasting and communication services are listed in **Table 1**, along with comparisons of encryption and copyright protection technology. The copyright protection technologies for digital broadcasting and Internet streaming that are currently the subject of standardization activities are compared in **Fig. 1**.

The copyright protection technology for current digital broadcasting can be broadly classified into conditional access systems (CASs), which restrict reception, and rights management and protection (RMP) technology, for which operation specifications are now being formulated. Reception restriction technology is the standard [1] used since the beginning of CS (communication satellite) digital broadcasting (subscription-based services) in 1996, but the scrambling of free-of-charge broadcasting services began in April of this year, with additional standards for BS (broadcast satellite) digital broadcasting [2]. The same kinds of systems are used for digital broadcasting, including terrestrial broadcasting, satellite broadcasting, and cable broadcasting (simultaneous retransmission of CATV (cable TV)), both in Japan

[†] NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: ishii.shinji@lab.ntt.co.jp

Table 1. Examples of broadcasting and communication services and comparison of encoding processing and copyright protection technology.

Type	Storage*1	Transmission system	Service examples	Encoding processing technology		Copyright protection technology	
				CAS	DRM	RMP	DRM
Broadcasting	No	Streaming	Terrestrial, BS, and CS are in service	Fixed reception technology (with scrambling) performed by CAS	—	CCI function (part of the CAS function) can be used	—
	Yes	Downloaded file	Server-type broadcasting operation use being decided	Limited playback technology (encryption) using ACI		Using RMPI (capable of more detailed description than is CCI)	
Communication	No	Streaming	VOD	Implemented by same method as limited playback	DRM	Using RMPI (capable of more detailed description than is CCI)	DRM
	Yes	Downloaded file	Download from server and store				

*1 Indicates whether or not the service providers assume local storage (excluding recording for private use)
BS: broadcast satellite
ACI: accounting control information
CCI: copy control information

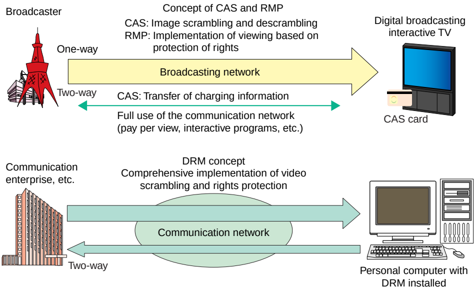

Broadcaster
Concept of CAS and RMP
CAS: Image scrambling and descrambling
RMP: Implementation of viewing based on protection of rights
Digital broadcasting interactive TV
One-way
Broadcasting network
Two-way
CAS: Transfer of charging information
Full use of the communication network (pay per view, interactive programs, etc.)
CAS card
Communication enterprise, etc.
DRM concept
Comprehensive implementation of video scrambling and rights protection
Communication network
Two-way
Personal computer with DRM installed

Fig. 1. Comparison of rights protection system concepts for content distribution.

and worldwide. On the other hand, digital rights management (DRM) has come to be widely used as copyright protection technology for streaming content on the Internet. Both of those approaches ensure secure viewing of copyrighted content within the range of authorized use, so they both have the same functions.

For subscription-based TV broadcasting, it is necessary to enable anyone installing a TV receiver to immediately receive the programs of any of the broadcast channels, as long as the viewing contract or other such preparation has been completed in the case of pay channels. For that purpose, TV receivers, including those for digital broadcasting, must be based on specifications for broadcasting systems that are standard, even among different broadcasters [3], [4].

For Internet distribution of content using personal computers, on the other hand, the user terminals (i.e., personal computers) vary in their performance, memory and storage capacities and operating system types and versions, and the user must install the application software required for each Internet service provider. Considering this situation, we believe that using standard specifications that extend communication functions to current digital broadcasting is a realistic approach to cooperative broadcasting and communication services during the market establishment phase. From these viewpoints, server-type broadcasting, for which operation specifications are currently being formulated, is being studied on the basis of digital broadcasting standards [5].

3. Rights management and protection information

An overview of viewing licensing based on rights management and protection information (RMPI) is shown in **Fig. 2**. The order of operations is indicated by the numbers in the figure.

Preparation for registration of content in the distribution center

(1) RMPI is obtained from the broadcasting company or other content owner.

(2) If it is necessary to append RMPI that provides details within the range permitted by the RMPI of (1) according to the specific environment of the distribution network management function, then supplementary RMPI is defined and reserved. Of course, this supplementary RMPI may not contradict the permissions received in the RMPI of (1).

Operational steps for when the user wants to playing the content

(3) The user makes a request to play the content. The playing request management function first confirms that the receiver is of the proper type for the content on the basis of the RMPI. Then, to protect the user, public key encryption is used for mutual authentication to ensure that the receiver is connected to a reliable distribution center.

(4) On the basis of the user's request, the pay request management function makes a request for license issuing processing.

(5) The user's contract is retrieved by the database management system to check for permission to view the content before proceeding to the actual licensing procedure.

(6) The RMPI for the content that is relevant to the user's request is obtained from the RMPI management function, and a license that reflects the conditions set in that information is generated.

(7) The license is generated. At the same time, if the content has an associated charge, charging processing is executed. The receiver can then operate within the bounds of the issued license. For example, if the number of times the content may be played is specified, the TV set will present the content that many times, but no more unless the license is renewed. To increase the security level, the TV set can report the number of remaining plays to the content distribution center for checking just before each replay when a multi-play license has been issued, as a measure against unauthorized modification of the receiver.

Steps such as those described above ensure honest operation of the receiver according to the RMPI specified by the broadcaster. Typical RMPI items that are specifically needed for server-type broadcasting ser-

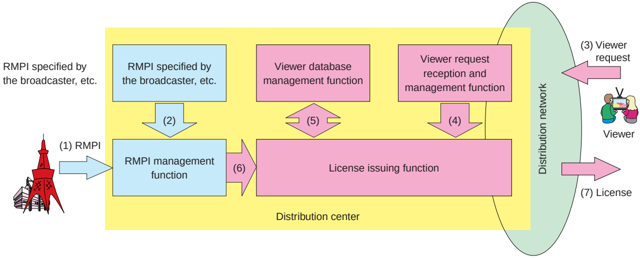

RMPI specified by the broadcaster, etc.
RMPI specified by the broadcaster, etc.
Viewer database management function
Viewer request reception and management function
(3) Viewer request
(2)
(5)
(4)
Distribution network
Viewer
(1) RMPI
RMPI management function
(6)
License issuing function
(7) License
Distribution center

Fig. 2. Issuing of a license that permits viewing on the basis of rights management and protection information (RMPI).

vices or are assumed are shown in **Table 2** and an example of the XML (extensible markup language) description for those items is shown in **Fig. 3**.

4. Future copyright protection systems

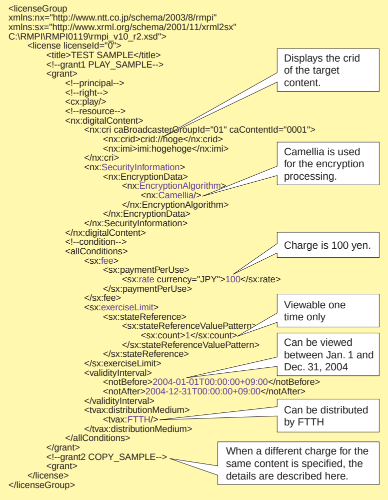
We have developed a rights protection system that meets the needs of a content distribution system based on cooperation between broadcasting and communication services. With recent technical advances—optical fiber, which can deliver the high-quality digital content of an HDTV (high-definition TV) program library via both broadcasting and broadband networks, large hard disk drives that can record and replay digital HDTV programs, and Blu-ray[*1] discs for high-density digital recording—it has become technically feasible to draw up a true business model for broadcasting/telecommunication cooperative services.

In this article, we focused on how copyright protection information for digital content can be used in a business-to-consumer (B2C) environment, where digital content moves from the communication company to the user's receiver. However, since the business-to-business (B2B) distribution of digital content among broadcasters and telecommunications companies must also be accompanied by copyright management information, the distribution of copyright permission management and digital content should be integrated. We believe that, in the future, mobile services involving AV (audio/visual) equipment, personal computers, and hand-held recording devices (cellular phones, PDAs, etc.) centered around a home server within the household will further enrich our lives. It goes without saying that copyright management of digital content use within the permitted range is necessary in this case too. We will continue research and development of the copyright protection technology and copyright management methods needed to support such a digital content distribution market.

Table 2. Examples of rights manegement and protection information.

Content charge control	Charges are presented for each form of content purchase.
Control of copy generations	The number of permitted copy generations (i.e., a copy made from a copy) is controlled. In current digital broadcasting, three types of control are being used: unlimited copying, one generation of copying, and no copying.
Control of number of copies	The number of copies that can be made in one generation from the purchased content is controlled.
Control of the copying destination	This specifies authorized devices when the content is to be written to an external storage device.
Control of the number of playbacks	Playback is permitted only a certain number of times.
Time control of the playback function	Content stored in the receiver can be played back only during a limited period.
Control of whether local storage is permitted.	Specifies the conditions for storage in the receiver (for server-type broadcasting)
Regional control	Specifying viewing permissions region by region
Gender-based control	Used to provide services specific for males or females
Control over special playback features	Controls playback features other than simple playback, such as skipping certain parts (e.g., commercials), pausing, fast forward, rewind, etc.
Viewer age control function	Controls viewing by comparing the age classification of the content with the age setting on the receiver
Control of use by viewer attributes	When viewer attributes are used in two-way services, etc., viewer authentication is performed to protect the viewer.
Encryption processing specification control	Specifies the encryption algorithm and use mode
Authentication processing specification control	Specifies the authentication method
Distribution media control	Applied when matching the content to the transmission capacity of the distribution network, etc.
Control of number of distribution times	Limits the number of times the content can be distributed

[*1] Blu-ray: A next-generation optical disc format jointly developed by thirteen leading consumer electronics and PC companies in Japan and other countries. It uses a blue-violet (wavelength: 405 nm) laser and can store 27 GB of data on one side of a 12-cm disc, which is sufficient for recording HDTV broadcasting directly in digital form. http://www.blu-ray.com/info/



```
<licenseGroup
xmlns:nx="http://www.ntt.co.jp/schema/2003/8/rmpi"
xmlns:sx="http://www.xrml.org/schema/2001/11/xrml2sx"
C:\RMPI\RMPI0119\rmpi_v10_r2.xsd">
    <license licenseId="0">
        <title>TEST SAMPLE</title>
        <!--grant1 PLAY_SAMPLE-->
        <grant>
            <!--principal-->
            <!--right-->
            <cx:play/>
            <!--resource-->
            <nx:digitalContent>
                <nx:cri caBroadcasterGroupId="01" caContentId="0001">
                    <nx:crid>crid://hoge</nx:crid>
                    <nx:imi>imi:hogehoge</nx:imi>
                </nx:cri>
                <nx:SecurityInformation>
                    <nx:EncryptionData>
                        <nx:EncryptionAlgorithm>
                            <nx:Camellia/>
                        </nx:EncryptionAlgorithm>
                    </nx:EncryptionData>
                </nx:SecurityInformation>
            </nx:digitalContent>
            <!--condition-->
            <allConditions>
                <sx:fee>
                    <sx:paymentPerUse>
                        <sx:rate currency="JPY">100</sx:rate>
                    </sx:paymentPerUse>
                </sx:fee>
                <sx:exerciseLimit>
                    <sx:stateReference>
                        <sx:stateReferenceValuePattern>
                            <sx:count>1</sx:count>
                        </sx:stateReferenceValuePattern>
                    </sx:stateReference>
                </sx:exerciseLimit>
                <validityInterval>
                    <notBefore>2004-01-01T00:00:00+09:00</notBefore>
                    <notAfter>2004-12-31T00:00:00+09:00</notAfter>
                </validityInterval>
                <tvax:distributionMedium>
                    <tvax:FTTH/>
                </tvax:distributionMedium>
            </allConditions>
        </grant>
        <!--grant2 COPY_SAMPLE-->
        <grant>
    </license>
</licenseGroup>
```

Displays the crid of the target content.

Camellia is used for the encryption processing.

Charge is 100 yen.

Viewable one time only

Can be viewed between Jan. 1 and Dec. 31, 2004

Can be distributed by FTTH

When a different charge for the same content is specified, the details are described here.

Fig. 3. Example of XML description of RMPI.

References

[1] "CS digital broadcasting receivers," Association of Radio Industries and Businesses, Standard ARIB STD-B1, May 2001.

[2] "Access restriction standards for digital broadcasting," Association of Radio Industries and Businesses, Standard ARIB STD-B25, Jun. 2003.

[3] http://www.arib.or.jp/

[4] http://www.catv.or.jp/jctea/

[5] "Coding, transmission and recording restriction methods for server-type broadcasting," Association of Radio Industries and Businesses, Standard ARIB STD-B38, Feb. 2003.

Shinji Ishii
Senior Research Engineer, Promotion Project 1, NTT Cyber Solutions Laboratories.

He joined NTT in 1989. He is interested in developmental research on security systems for multimedia communications. Recently, he has been engaged in the development of copy protection systems for digital broadcasting and broadband communications.

Sadakatsu Muto
Promotion Project 1, NTT Cyber Solutions Laboratories.

He joined NTT in 1989 and engaged in the developmental research on the database system supporting web services. Recently, he has been engaged in the development of copy protection systems for digital broadcasting and broadband communications.

Masahito Kawamori
Senior Research Engineer, NTT Cyber Solutions Laboratories.

He joined NTT Laboratories in 1989. He has worked in research areas such as artificial intelligence, language processing, and interactive agents using speech recognition. His current research area is metadata and media delivery systems for broadcasting and broadband communications.

Katsuhiko Kawazoe
Senior Research Engineer, NTT Cyber Solutions Laboratories.

He received the B.E. and M.E. degrees in engineerring from Waseda University, Tokyo in 1985 and 1987, respectively. Since joining NTT in 1987, he has mainly been engaged in R&D of radio communication systems, satellite communication systems, and the personal handy-phone system (PHS). His specialty is forward error correction systems. He is currently a co-chairman of the Association of Radio Industries and Businesses Working Group for Broadcasting Systems based on a Home Server. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and received the Young Engineer Award from IEICE in 1995.