Multimedia Streaming Technology in Broadband Networks
3 – Digital Rights Management System

Hideki Yamamoto

With the spread of broadband, services for distributing digital contents, such as software, games, video, and the like, (or "content distribution services"), have started to take off in a real way. However, the fact that digitalized contents can be copied very easily has prevented content rights holders from adopting a more positive attitude to content distribution. For content holders, the key functions required in a content delivery system are unified management of copyright information supplied to the distributor, control of delivery servers on the basis of this copyright information, and encoding of the information streams. This essay looks at these different functions, which are all installed in the OKI MediaServer.

Copyright management systems

In seeking to prevent unauthorized copying of contents over networks, the first priority is to make it possible to examine the copyright status of individual authors. The purpose of a copyright management system is to perform unified management of copyright information relating to digital contents. The copyright management system requires:

① a database for managing copyright information;
② means for linking database information and contents; and
③ a function for assigning universally identifiable IDs to contents.

The copyright management system we have developed at Oki is described below.

(1) Overview of copyright management system

We have developed a system based on the Content ID Forum (cIDf) specifications[1)] in order to satisfy these requirements. cIDf is a group set up with the objective of promoting distribution of digital contents, and it has established formats for copyright information and ID numbers used to identify copyright information, as well as methods for managing this information, and so on.

The copyright information is structured as illustrated in Table 1. The ID centre management number in the copyright information is a universal unique number which has the composition shown in Table 2. The regional code is assigned in country units, or the like.

In the cIDf specifications, the ID centre management number issues a separate ID, each time the distribution conditions of the contents change. Furthermore, in order to create an association between a content and an ID centre management number, the ID centre management number is embedded optionally in the content, as a digital watermark.

Table 1 Configuration of cIDf copyright information

Item name	Meaning / Description
ID centre management number	A universal unique number which identifies the content; set when a content ID application is made.
Content attribute	Information indicating the content details / category
Rights attribute	Rights information relating to the content
Rights use attribute	Information relating to delegation, approval, transfer of rights
Distribution attribute	Information referenced when distributing contents

Table 2 Composition of ID centre management number

Item name	Meaning / Description	Size (bit)
Version number	Designates version of ID centre management number	4
Regional code	Number identifying location of ID centre	4
Centre number	ID centre number	8
Centre content number	Number identifying contents managed by ID centre	Any

(2) Integration of VOD system and copyright management system

A system has been developed for registering copyright information and embedding digital watermarks in contents delivered by VOD systems. Fig. 1 shows the configuration of this system[2)].

A digital watermark must be embedded each time a new content distribution condition is added, but in this system, by closely integrating the copyright management system with the VOD system, the copyright management system obtains contents via VOD, and after assigning copyright information, in other words, after embedding a digital watermark, it returns the data automatically to the VOD server.

The data flow is simple to explain. In ①, the content is input to the VOD system without any digital watermark. The copyright information for that content is

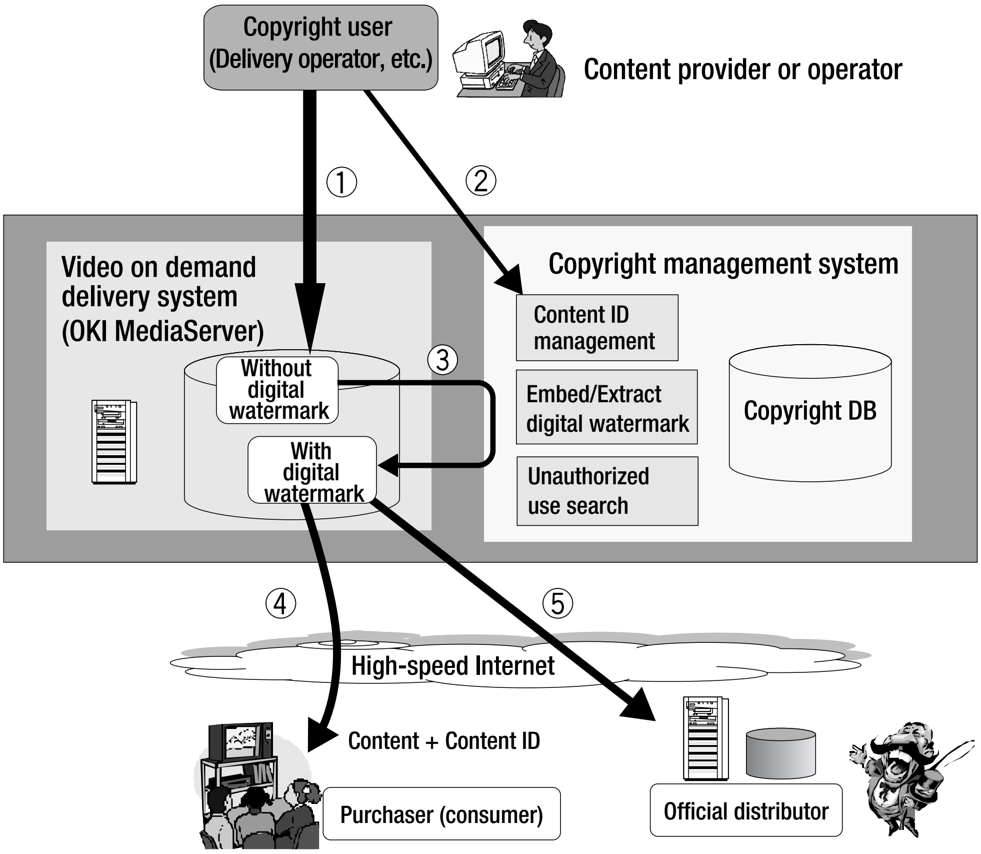
Copyright user
(Delivery operator, etc.)
Content provider or operator
①
②
Video on demand delivery system (OKI MediaServer)
Copyright management system
Content ID management
Embed/Extract digital watermark
Copyright DB
Unauthorized use search
③
Without digital watermark
With digital watermark
④
⑤
High-speed Internet
Content + Content ID
Purchaser (consumer)
Official distributor

Fig. 1 Copyright management system and video delivery system2)

registered in the database, and an ID number is issued ②. In ③, the digital watermark is embedded in the content. Delivery is only performed for contents which have been digitally watermarked ④. In the case of a distributed delivery system, the digitally watermarked contents are delivered to different distributors ∞. In this method, even in the case of different distribution conditions or a different bit rate relating to the same content, the copyright user simply needs to perform the operation of issuing a new ID for the content already stored in the VOD server.

(3) Application example

This system was used in a video streaming experiment carried out by the content distribution verification test promotion committee to perform the tasks of issuing copyright information for annual news video contents, and embedding digital watermarks. It was also used for movie previews over the Internet. In this way, the practical usability of the system was proven.

A corroborative experiment was also performed with the Digital Content Association of Japan to investigate integration with a system that determines which centre to obtain copyright information from, if there are a number of different ID management centres on the network, (“Resolution System”, hereinafter “RA”)[4] (Fig. 2).

Licence management

A fee-charging content delivery service using a video delivery system requires: a viewing licence definition function for selling contents, delivery server control functions based on sold licenses, and billing and authentication functions. These functions are described in more detail below.

(1) Viewing licence assignment units

Since content distribution does not involve logistical issues in the same way as rental videos, a number of different contents can easily be bundled together for sale or purchase. Therefore, in this system, viewing licences are assigned to groups of contents, rather than individual contents, as illustrated in Fig. 3. For example, content groups, such as detective story packs or cowboy story packs, can be created and a price established for each group. If a content group only contains one content, then a licence is defined just for that content. The following functions are provided for performing operations on the content groups.

① Function for adding contents to a group

Sometimes, extra contents may be added to a group at a later stage, for instance, in the case of a serial program, J-league soccer pack, or the like. Adding

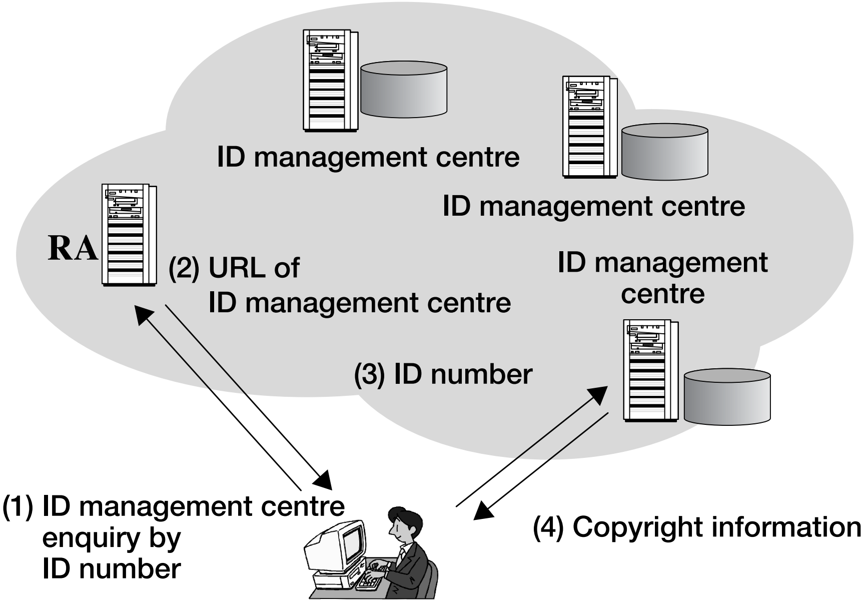
ID management centre
ID management centre
RA
(2) URL of ID management centre
ID management centre
(3) ID number
(1) ID management centre enquiry by ID number
(4) Copyright information

Fig. 2 Overview of RA experimental system

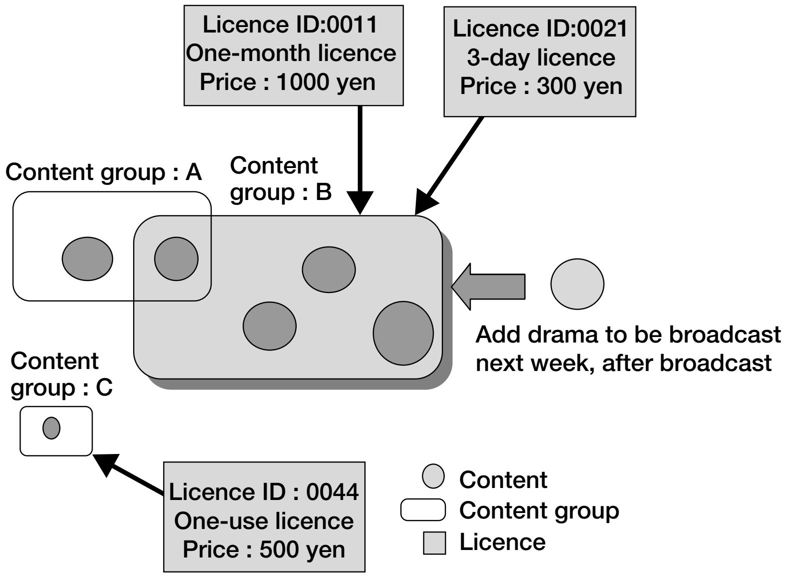

Fig. 3 Relationship between content groups and licences

contents to a group presents no disadvantages to service users, and hence there are no restrictions on this service.

② **Controlling changes to group members**

Removing items from a content group after a licence has been sold will be disadvantageous for existing customers (viewers) and therefore the operator is not allowed to perform this action. However, the operator is permitted to remove items from a content group before it is put on sale.

(2) Types of licence

The various types of licence are listed in Table 3.

A viewing licence can be defined for a content group as described in (1) above. It is also possible to define a number of licences for the same content group. Licence information and licence purchasing histories (called "contractual information") are managed in a database. Table 4 shows the approximate structure of this contractual information.

Table 3 Types of viewing licence

Name	Meaning / Description
Frequency limit	A licence which limits the number of times a content is viewed. Each time playback is started, this is counted as one viewing.
Time limit	A licence which allows a content to be viewed for a certain time period only, after purchase of the licence.
Regular subscription	A time limit licence which automatically renews the contract when the time period expires. Automatic renewal continues until the contract is expressly cancelled.

Table 4 Approximate structure of contractual information

Name	Meaning / Description
Contract ID	A universal unique ID which identifies the viewing contract
Licence ID	An ID which indicates the type of licence. This ID is used to search the database for more detailed information on the licence.
User ID	ID of the user who purchased the licence
Contract date/time	Date & time when licence was purchased
Initial viewing date	Date & time of first viewing after purchase of licence
Purchase price	Price of licence

(3) Control of delivery servers on the basis of licences

When a delivery request is made for a content that is subject to licensing, the delivery server first checks whether the user in question has a valid licence, and then starts delivery. If the licence period expires during delivery, then the delivery operation is terminated.

In an actual service, the operator's customer support line may receive a request from a user wishing to cancel a licence because they have accidentally bought the wrong one. Provided that the user has never viewed the relevant content, the ISP side will then accept the cancellation request. The "initial viewing date" field is provided in the contractual information in order to deal with situations of this kind.

(4) Billing and authentication interface function

Billing information for each user is obtained by collating contractual information stored in a relational database (RDB). This makes it very easy to create an interface with the service operator's billing system.

User authentication is required when a user purchases a licence, or wishes to view a content using a licence he or she has bought. The OKI MediaServer contains a built-in authentication database designed for small-scale services. When used by an ISP, or the like, the equipment can be set up to access an external authentication server. RADIUS and LDAP samples are provided for interfacing with the authentication server.

(5) Application examples of licence management

Fig. 4 shows the general structure of the OKI MediaServer operating as a distributed delivery server incorporating licence management functions, and the illustration also shows the flow of data from purchase of a licence by a user until viewing of the content. The boxed regions in the picture indicate OKI MediaServer modules. The content portal is a list of contents located on a Web server, and it is usually constructed by the service operator. In most cases, the authentication server is also provided in advance by the operator, and in this illustration, this server can be accessed by the authentication module of the OKI MediaServer. Since the authentication module uses CGI technology, it can also be executed from the content portal side. The operational procedure up until viewing of the content is described below.

① The viewing user selects items to purchase from the licence information indicated by the content portal, in other words, information relating to content groups, prices, time restrictions, etc. (viewing contract). The server performs user authentication, and provided that this authentication is successful, it creates contractual information corresponding to the selected licence and adds it to the database. A contract is established in the system, the moment that this contractual information is added to the database.

② When the user subsequently selects a content that he or she wishes to view after the contract has been set up, if time has passed since the licence was purchased, then the server performs authentication once again before executing view processing. In view processing, the server searches the database to check that the user has already bought the indicated licence, and that this licence is still within its validity period. If the licence is valid, then the server sends information required for content delivery to the player side, whilst simultaneously issuing a delivery instruction to a delivery server. In the case of a distributed configuration, the delivery instruction is output to the local server that is nearest to the viewer.

③ The local server starts to deliver content to the user's terminal, in accordance with the delivery instruction. This instruction contains delivery time limit information calculated from the licence information, for example, in the case of a 3-day licence bought at 18:00 on 10th September 2002, the delivery time limit will be 18:00 on 13th September 2002. When this time point is reached, the delivery module (video pump) of the local server will terminate delivery.

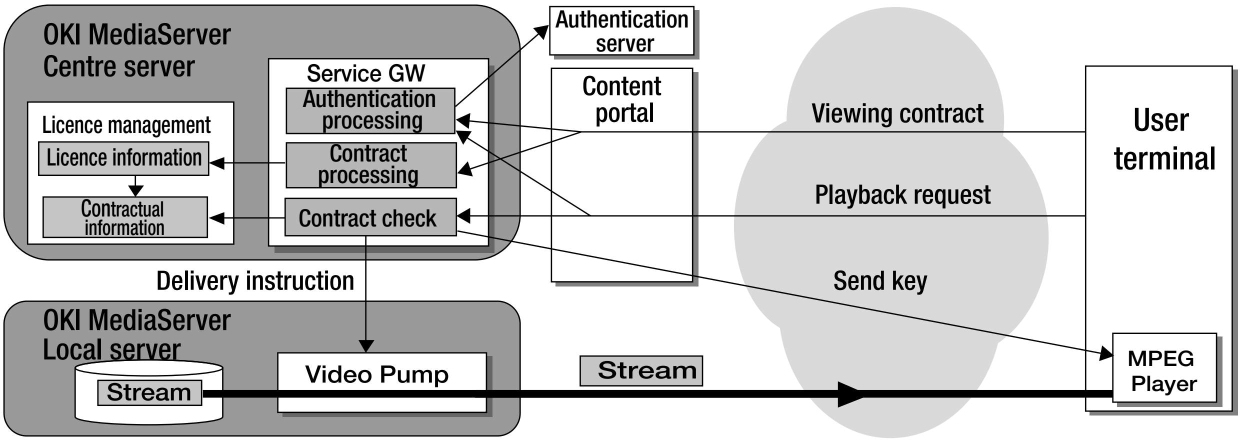

Fig. 4 Application example of licence management in OKI MediaServer

An almost identical configuration to this is used in practice by large-scale service providers for their paid content delivery services.

Encryption of the communication channel

In streaming delivery using the OKI MediaServer, received data is reproduced straight away without saving, rather than storing contents in the user terminal. This means that the set-up is superior to a download-type delivery server in terms of content protection, but functions have also been proposed for encrypting the communication channel in order to protect content from illegal viewing, or other kinds of unauthorized access.

In the example in Fig. 4, the communications are encrypted at the following points.

① Communication of authentication information from user terminal to content portal when establishing viewing contract or re-viewing contents.

② Communication of key information from Service Gateway to MPEG Player. Here, the key information contains the key required to decode the encrypted stream.

③ Streamed information delivered from the video pump to the MPEG player. This information is encrypted on the basis of a common key code.[5] Information stream encryption can also be applied to real-time video contents, in addition to stored contents.

What is more, in the copyright management system

TIPS Trends and Glossary of Terms

Trends

One of the technologies used for DRM is Microsoft's Windows Media Technology, but this uses library groups to manage licences, and requires considerable software development to build a practical commercial service. The licence management system and stream encryption technology used in the OKI MediaServer are constructed as packages at a level which allows the operator to set up services straight away. One feature of the Server OKI MediaServer is that it handles licence types which cover virtually all the sales formats used in actual content-related services (magazine, rental video, etc.) In addition, its authentication and billing interface supports standard protocols, permitting easy integration with existing systems.

Formats for copyright management systems are currently in the process of standardization, with initiatives such as cIDf, MPEG-21 and TV-Anytime Forum. This essay has used an example where cIDf specifications are installed, but the OKI MediaServer itself can readily handle any meta data written in XML, thus enabling a flexible response to future trends in format standardization.

Terminology

RADIUS : An acronym of Remote Authentication Dial In User Service. An established user authentication protocol for dial-up services, etc. An IETF standard. Examples include : RFC2058, 2865, 2866, 2869, etc.

LDAP : An acronym of Lightweight Directory Access Protocol. A protocol for Internet directory services. V3 is currently the predominant LDAP version.

illustrated in Fig. 1, ciphered communications are used when registering copyright information.

Conclusion

This article has looked at copyright management systems, licence management systems and communication channel encryption, which are all important digital rights management (DRM) technologies required in content distribution. By incorporating these technologies, the OKI MediaServer can be used to provide stable content distribution services. Although not mentioned in this essay, operational measures, such as management of original copies of contents (tapes, etc.) and management of server administrators, etc., are also vital in terms of content protection.

The standardization of DRM-related meta data is currently making positive strides, such as the TV-Anytime Forum[6)], MPEG-21[7)], cIDf, and the like. This article has used an example where cIDf is installed, but since the meta data management functions of the OKI MediaServer are capable of storing all kinds of XML documents, the equipment would be readily able to handle meta data based on another standard. In the future, we aim to make an active contribution to meta data standardization, as well as continuing to offer products installed with the very latest technologies. ◆◆

■ References

1) Content ID Forum : http://www.cidf.org/

2) Kondo, Sato, Yamamoto, Nagasaka: “Video delivery systems with integrated copyright management systems”, Proc. IEICE General Conf. 2001, B-16-2, 2001

3) Video Streaming Experiment Group : “Starting public experiments of distributed video content delivery using broadband Internet”, http://www.vsforum.org/home/whats/release-exp-20010423.html, 2001

4) Yamamoto, Uchida, et. al.: “Fundamental systems for promoting content distribution”, IPA 2001 Research Report, 2002

5) Sato, Yamamoto, Nagasaka : “Block encryption processing methods for MPEG streaming”, Proc. of 1st FIT Conf., Information Processing Society of Japan, 2002

6) TV-Anytime Forum : http://www.tv-anytime.org/, 2002

7) MPEG : “MPEG-21 Overview”, http://mpeg.cselt.it/, 2001

● Author

Hideki Yamamoto Broadband Media Company, Media Solutions Div.