Pay-per-view | Encoding Technology | Expanded Distribution of Content

Technology Reports

Content Distribution Technology for Free Distribution of Content and Reliable Charging

We have devised a new charging method and conducted experiments with content distribution technology to further develop the content business. This technology allows flexibile redistribution and charging (including negative charging, i.e., cash-back) for the replay of content; content can be redistributed freely by users since they are charged in a block-by-block manner at the time they play it.

Takeru Ishihara, Hideaki Ito, Masayuki Terada and Sadayuki Hongo

1. Introduction

Presently, charging for content is generally conducted at distribution from the server, since it is easier to manage content fees at the server. However, even if a user feels that the downloaded content is uninteresting and halts the replay, he/she is charged for the full content, despite having viewed only a part of it. We have developed a content distribution technology that resolves this issue by charging fees not at downloading, but for only the part viewed during replay on a client's device such as a mobile terminal. Since charging is done on the client device, the content distribution technology is referred to as "client-side charging technology."

Client-side charging technology permits flexible charging, such as out-of-range charging, usage-based charging, and negative charging (cash-back) for content like a commercial message that the content provider wants the users to view. Moreover, acquisition of detailed viewing information and content distribution are freely performed. The use of client-side charging technology permits pay-per-view at any time and anywhere, thus improving user convenience. For instance, when only a part of downloaded content is viewed, a user is not charged for the full download, but only for the part viewed. Furthermore, even if the user is out of range, content data that were provided by a magazine or acquired from a friend can also be viewed.

With further development of the content market in mind, NTT DoCoMo has investigated the possibility of implementing the distribution of video content using client-side charging technology. Such a system can be implemented using one of two methods: replaying video content on a notebook PC and being charged via a mobile terminal, or only using the mobile terminal. We first investigated the former method and verified that the client-side charging technology is feasible by devising the encoding method of content.

This article provides an overview of client-side charging technology, describes a configuration of the system verified as feasible, and compares this technology with other competitive technologies.

2. Characteristics of Client-side Charging Technology

The five characteristics of client-side charging technology are described below.

1) Charging is also possible out of range

Since charging is done autonomous-

ly on the client side, content can be replayed and charged even if the user is out of range.

2) Content may be freely distributed

Since this method requires decoding and charging when replaying encoded content, there is no need to prevent copying, and content may be freely distributed among users.

3) Sequential charging (such as ¥10/min) is possible

Content may be divided into a number of blocks (such as by every minute), and fees are charged as each block is replayed. The fee for each block of content may also be changed.

4) Negative charging (cash-back) is possible

Negative charging is possible by applying a negative fee for every block. In other words, cash-back makes it possible for the content containing commercial messages to be charged for only the part viewed, with the normal charge for the remaining content.

5) Detailed viewing information is available to determine which parts of content have been viewed

Charged blocks may be considered viewed blocks. Since the charge log may be used, the parts of content replayed by each user can be determined, and detailed information on viewing history obtained.

Figure 1 shows an example of a charging method used with client-side charging technology for characteristics 3), 4) and 5) above.

3. Encoding Technology for Client Charging

3.1 Overview

An easily operated method of encoding and decoding is used with client-side charging technology. This method permits processing with minimal CPU load on the mobile terminal and audiovisual device despite continuous charging on the mobile terminal during frequent communication between the two devices, thus ensuring that video quality remains unaffected.

Figure 2 shows the overall configuration of client-side charging technology. A secure method is adopted to copy and store an IC card key generated by the server to the mobile terminal. The server encodes the content and generates dedicated content. The dedicated content consists of encrypted content, an encrypted content key (initial key), a charging table, and the Message Authentication Code (MAC)[*1]. This is designed to ensure that dedicated content may be freely copied, with payment for only the viewed content. It is therefore necessary to prevent illegal copying, and to ensure that content is divided into blocks of a few minutes or a few seconds. For the same reason, the content key necessary for decoding content is encrypted. Moreover, if the initial key is altered, content will not be replayed correctly, or if the charging

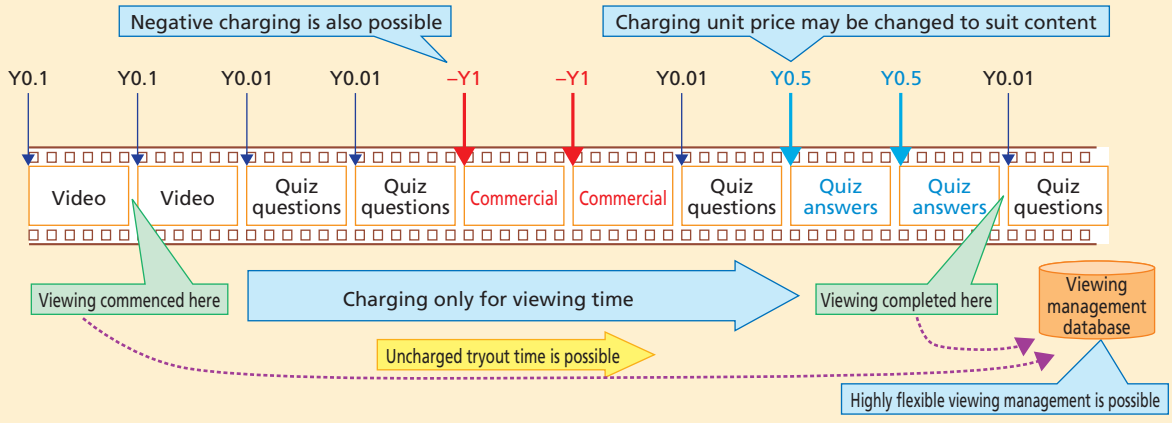

Figure 1 Charging method

*1 **MAC**: A code used to verify that the data has not been altered.

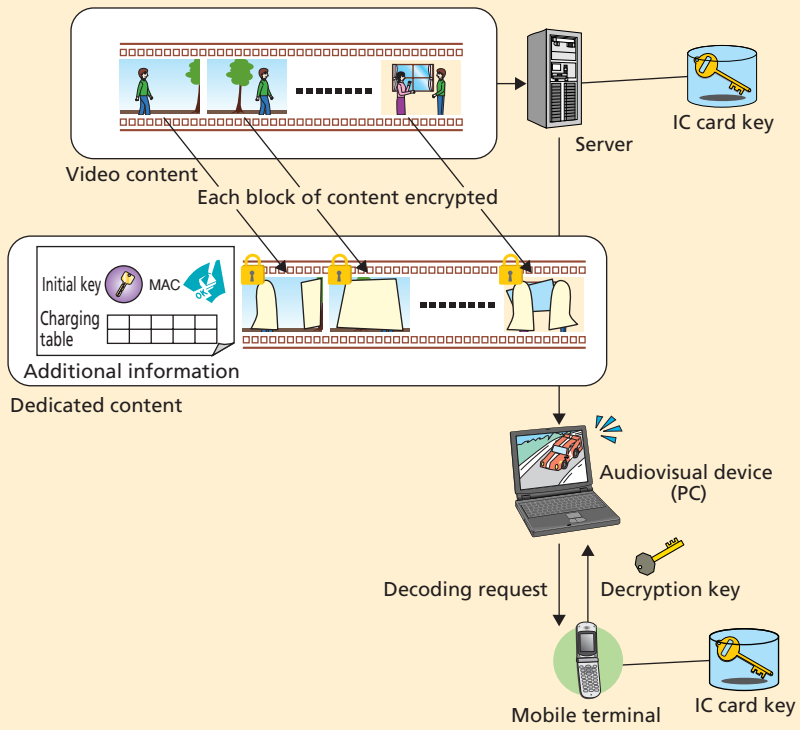

Figure 2 Overview of client-side charging technology

table is altered charging will be incorrect at replay. A value computed from the initial key and charging table is therefore assigned as the MAC to prevent alteration by verifying that it matches the value computed at dedicated content generation prior to replay, thus preventing charging errors.

The audiovisual device downloads the dedicated content from the server encoded by using client-side charging technology. A decoding request is sent to the mobile terminal when the audiovisual device (PC) replays the content. The mobile terminal then creates a decryption key to decode the encoded content, and conducts charging at the same time. The decryption key is received at the PC for decoding and replaying content.

3.2 Encoding

The content encoding procedure (**Figure 3**) is described as follows.

A content key is randomly determined for the content that will be encrypted (Fig. 3 (1)). The charging table, content key, and IC card key are used to compute the initial key that was the encrypted content key, and the MAC (Fig. 3 (2)). The decryption key is then computed based on the content key and block number (Fig. 3 (3)). Each content block is encrypted with common key cryptosystem[*2] using a decryption key for each block (Fig. 3 (4)), with the encrypted content block being generated (Fig. 3 (4)). All encrypted content blocks, the initial key, charging table, and MAC are then output together as dedicated content (Fig. 3 (5)).

3.3 Decoding

The dedicated content decoding and replay procedure (**Figure 4**) is described as follows.

The initial processing conducted by the mobile terminal involves deriving the content key using the IC card already stored in the mobile terminal based on the fixed initial key included in individual dedicated content (Fig. 4 (1)). The MAC is used to verify that the initial key, charging table, and content key have not been altered (with this processing terminated if any alteration is detected) (Fig. 4 (2)). Next, the mobile terminal derives the relevant decryption key using the content key and block number based on a send request for the decryption key associated with the block number from the audiovisual device, simultaneously verifies the corresponding amount for the relevant location from the charging table, and then conducts charging on the mobile terminal. The derived decryption key is sent to the audiovisual device (Fig. 4 (3)). The audiovisual device updates the decryption key, decrypts the encrypted content block using the decryption key in a common key cryptosystem, and then replays the

*2 **Common key cryptosystem**: An encoding method that uses the same keys for encrypting and decrypting. This method involves less computing than with methods using different keys for encoding and decoding, although the keys must be sent to the decrypting party in advance.

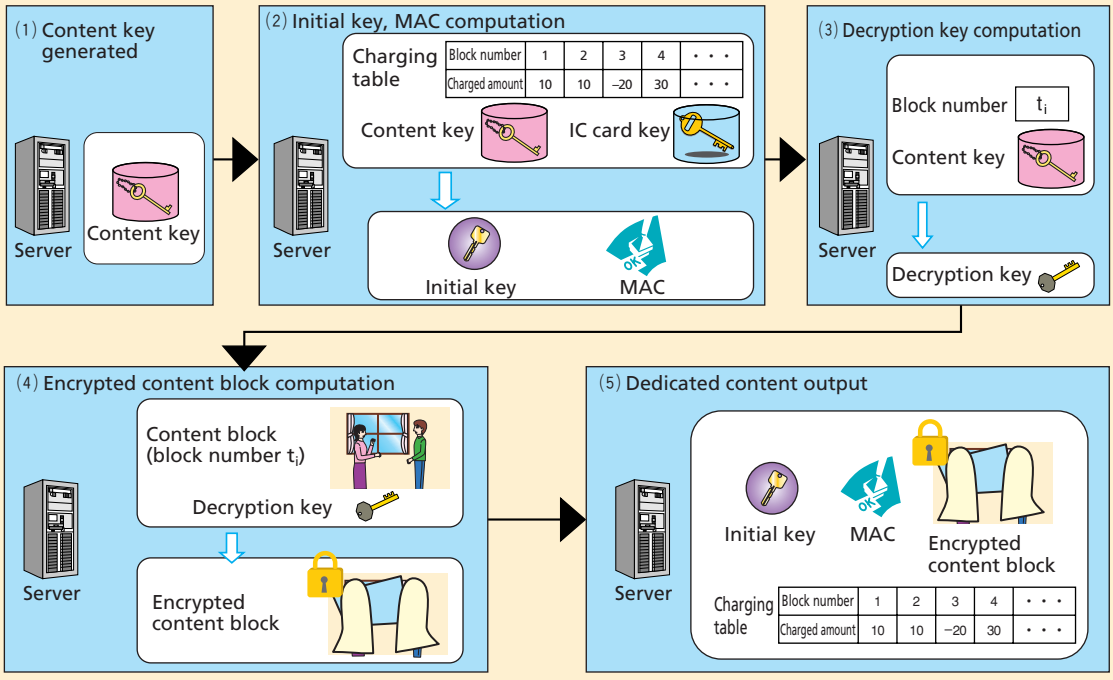

Figure 3 Encoding procedure

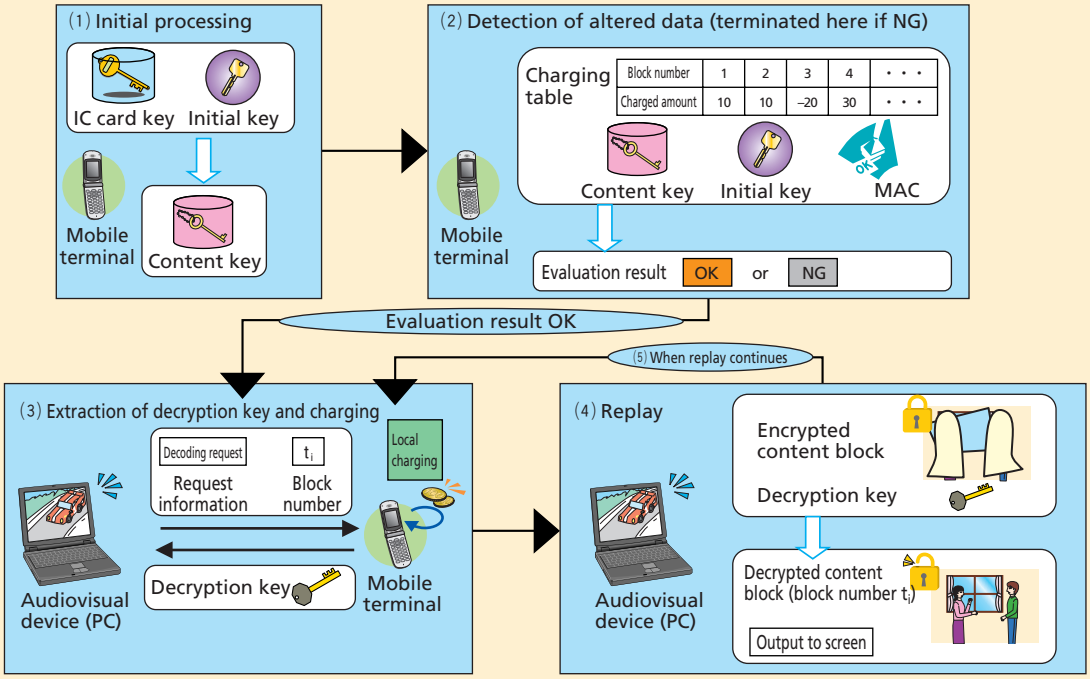

Figure 4 Decoding and replay procedure

decrypted content block (Fig. 4 (4)). When replay of the decoded data is complete or insufficient decoded data available for replay, the audiovisual device issues another send request for the decryption key to the mobile terminal and repeats the replay process until replay is complete (Fig. 4 (5)).

Since the procedure above permits reliable charging upon replaying content with this technology, dedicated content may be distributed via various means of distribution, and therefore downloaded from a server or obtained from such external storage media as microSDs and DVDs, or received from another user's audiovisual device.

4. System Configuration

Client-side charging technology requires ready encoding and decoding that does not affect video replay quality. **Figure 5** shows the configuration of a system devised to demonstrate that the method satisfies these requirements.

The system comprises content server supporting functions to encode content, and store and distribute converted dedicated content, an end-user mobile terminal, an audiovisual device (such as a PC), and a management server. A P903i mobile terminal is used, with a 1.66-GHz PC as the audiovisual device. Encoded and decoded blocks are approximately 1.2 MB in size.

Content is encoded on the content server. The encoded dedicated content is downloaded to the end user's audiovisual device. To replay the dedicated content, the audiovisual device sends the number of the block of dedicated content to be decoded to the mobile terminal. The mobile terminal sends the decryption key used in decrypting the block to the audiovisual device, and

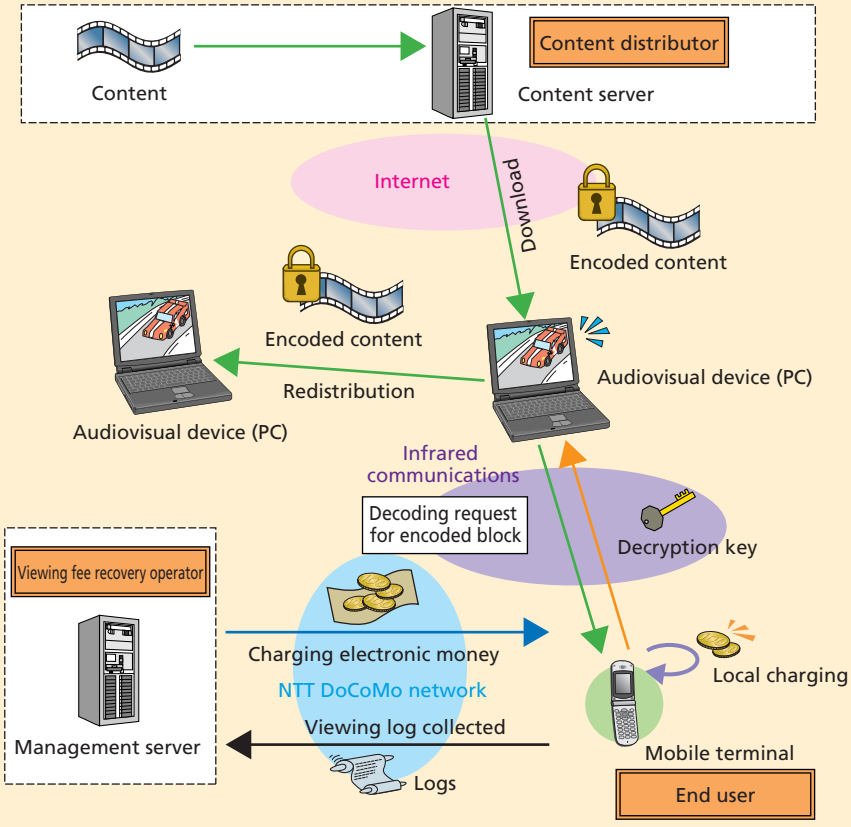

Figure 5 Configuration of feasibility demonstration system

then conducts charging. Charging can be done, for example, by deducting from prepayments. The audiovisual device and mobile terminal need not be linked on a network to connect to both the content server and the management server when viewing content. When the mobile terminal is linked on a network, information related to the viewing log and that related to charging conducted within the mobile terminal is sent to the server of the contractor responsible for recovering viewing fees.

Charging in the system used for verification adopted deduction from prepayments, and it was verified that the system was able to charge for and replay 720 × 480 pixel video content without any problem.

The system was verified using an infrared connection between the audiovisual device and mobile terminal, although both FeliCa®*3 and Bluetooth®*4 are also usable in principle.

5. Comparison with Other Technologies

Table 1 shows the differences with other competitive technologies. Comparisons are made with general Digital Rights Management (DRM)*5 technologies used with iTunes®*6 and LISMO®*7, online distribution technologies used with 4th MEDIA®*8, and client-side charging technologies.

1) Charging Possible while Viewing

Indicates whether charging is possible while replaying content. With general DRM technology, download starts after charging, and not while viewing. In contrast, with online distribution technology, viewing rights are downloaded during viewing, and simultaneous charging is therefore possible. With client-side charging technology, charging is done at the start of viewing each content block.

2) Flexibility of Charging

Indicates the degree of charging flexibility. With general DRM technology, content is sold in units, resulting in low flexibility. Conversely, some online distribution technologies permit charging in response to the amount of content viewed. With client-side charging technology, fees are charged for each content block, resulting in a very high level of flexibility.

3) Content Redistribution by End User (Word of Mouth Distribution)

Indicates whether a downloaded content file can be redistributed. Redistribution is possible with some types of DRM technology. Since charging starts at replay with client-side charging technology, redistribution is possible without any restriction.

4) Offline Viewing

Indicates whether content may be viewed offline. Although this is possible with both general DRM technology and client-side charging technology, content can only be viewed online with online distribution technology.

5) Communication while Viewing

Indicates whether communication is

Table 1 Comparison of similar and competitive technologies

	DRM technology	Online distribution technology	Client-side charging technology
Charging possible while viewing	×	○	○
Flexibility of charging	× Sold in units	○ Charging possible in response to amount viewed and part of replayed content	○ Charging possible in accordance with amount viewed and part of replayed content
Content redistribution by end user (word of mouth distribution)	△ Possible with some technology	×	○
Offline viewing	○	×	○
Communication while viewing	○ Communication not required	×	○ Communication not required
Obtainable viewing information (marketing information)	△ Marketing information only	○ Actual viewing status obtainable	○ Actual viewing status obtainable

○: Possible △: Possible depending on conditions ×: Impossible

*3 **FeliCa®**: A non-contact IC card technology developed by Sony Corp. A registered trademark of Sony Corp.

*4 **Bluetooth®**: A short-range communications standard between mobile terminals, such as cell phones, notebook PCs, PDAs, etc. A registered trademark of Bluetooth SIG Inc. in the United States.

*5 **DRM**: Functions for protecting copyrights of digital content by restricting redistribution, and preventing unauthorized copies, etc.

*6 **iTunes®**: A registered trademark of Apple Computer, Inc. in the United States.

*7 **LISMO®**: A registered trademark of KDDI Inc.

*8 **4th MEDIA®**: A registered trademark of Plala Networks Inc.

required while viewing. With general DRM technology, communication is not required after the download, though viewing is only possible while online with online distribution technology. In this case, content cannot be viewed unless viewing rights have been downloaded, which requires communication. The volume of communication is minimal when only viewing rights are to be downloaded, even though some communication is still required. On the other hand, communication is not required with client-side charging technology when viewing content, and only necessary when a communication path has been established after viewing.

6) Obtainable Viewing Information (Marketing Information)

Indicates the degree to which service providers are able to acquire viewing information about the users. With general DRM technology, marketing information is only available for each item of content. Detailed records of viewing are obtainable, however, with online distribution technology and client-side charging technology.

Issues associated with security may occur depending on how the general DRM technology is used, while client-side charging technology has an added feature of improved security through the use of anti-tampering devices[*9] such as the IC card.

6. Conclusion

This article has described the system configuration using the features of client-side charging technology. Future topics will include verifying ability to view only on the mobile terminal to increase user viewing opportunities, and verifying application to content other than video to increase the range of content able to be viewed by the user.

REFERENCES

[1] M. Inamura, T. Tanaka and K. Nakao: "Realizing Illegal Copy Protection for Digital Contents," SCIS2003, 2003 (In Japanese).

[2] M. Inamura and T. Tanaka: "Implementation and Evaluation of Illegal Copy Protection for Digital Contents," CSEC-22, 2003 (In Japanese).

[3] R. Mori, M. Kawahara and Y. Ohtaki: "Superdistribution: The Microelectronic Approach to Intellectual Property Right Processing," Journal of Information Processing Society of Japan, Vol. 37, No. 2, 1996 (In Japanese).

[4] K. Kanno: "Operational Management Systems and Methods," Japanese Patent 1998-83298, 1998 (In Japanese).

[5] H. Takada: "Information Management Equipment, Information Management Systems, and Media Storing Information Management Software," Japanese Patent 2001-249730, 2001 (In Japanese).

[6] R. Hoshino, H. Aono, S. Hongo, M. Suzuki, K. Akai and T. Matsumoto: "The Secure Charging Model on the Client, and It's Application," JIPS 65th National Convention, 2003 (In Japanese).

[7] H. Aono, R. Hoshino, S. Hongo, M. Suzuki, K. Akai and T. Matsumoto: "An Implementation of the Charging System on the Client by Inseparable Processing of Content Replay and Charging," CSEC-21, 2003 (In Japanese).

[8] H. Aono, R. Hoshino, S. Hongo, M. Suzuki, K. Akai and T. Matsumoto: "Evaluation of the Charging System on the Client by Inseparable Processing of Content replay and Charging," CSS2003, 2003 (In Japanese).

*9 **Anti-tampering device**: A device providing a means of preventing the internal analysis and changes of content. Security is generally compromised if the internal nature of the circuit, its operation, or processing procedures become known or changed.