Tamper-resistant Charging Technology for a Seamless Environment

Hiroshi Aono†, *Reiko Hoshino, and Sadayuki Hongo*

Abstract

Most music download services provided by mobile e-commerce place constraints on users to prevent illegal copying of the downloaded digital contents. To solve this problem, we have developed a system that enables music and other content to be freely redistributed while ensuring that it is paid for by subsequent users. Our system prevents overcharging and illegal playback by computing charges and providing digital contents simultaneously, whereas these are done independently in the current system.

1. Introduction

Although digital content was initially provided via broadband Internet access such as ADSL (asymmetric digital subscriber line) to desktop terminals, in recent years it has also come to be delivered to mobile terminals. This development is essentially the result of faster Internet connections on cellular handsets. At the same time, illegal copying of digital content obtained from download services has become a major problem. The main method of solving this problem is to implement systems that either prevent copying or limit it. However, this approach limits the terminals on which paid-for content can be used, which is an inconvenience for the user. On the other hand, allowing unrestrained distribution of usable digital content would make it difficult for a content provider (CP) to collect usage fees.

Previous proposals for preventing illegal copying include complete prohibition of copying [1] and permitting only primary copying (no copying of copies) [2], [3]. Methods such as these have been used as illegal-copying-prevention technologies that assign unique IDs to media or devices. They have been implemented in a variety of systems and media including SD memory cards, DVD-R/RW, CPRM (content protection for recordable media), MagicGate [4] memory sticks, and Blu-ray disks. These technologies make use of terminal-unique information to limit the use of content, so they have great potential for preventing the open distribution of digital content.

There is also the superdistribution model [5] and soft-denchi ("software battery") system [6], [7] that aim to achieve open distribution of digital content by charging for content at the client side. The superdistribution model allows for unrestrained distribution of encrypted digital content by delivering and transferring licensing information including a content decoding key through the use of a secret key stored in tamper-resistant hardware called a secure multimedia card. Keitaide-music ("music on your mobile") [8] is one example of a system based on the superdistribution model that enables unrestrained distribution of digital content. The soft-denchi system can charge for software at the client side when it is used. In this process, a soft-denchi manager decreases the amount of previously purchased (prepaid) value whenever the software is used. The user can use the software until that amount falls to zero and can always recharge the system with new value. Soft-denchi also features portability—it can be used at other terminals. However, this requires a soft-denchi management server connected via the Internet.

NTT DoCoMo is also collaborating with Professor Tsutomu Matsumoto of Yokohama National University in proposing a client-side charging system to enable the redistribution of digital content while collecting remuneration for its use [9]-[11]. It aims to accomplish this by performing charge processing in a manner inseparable from the playback of digital con-

† NTT DoCoMo Inc.
Yokosuka-shi, 239-8536 Japan
E-mail: aonoh@nttdocomo.co.jp

tent. This would enable content providers to collect usage fees even when content is distributed in an unrestrained manner. Furthermore, by using our proposed charging system with the content, we avoid the need for the end user having to change client software or hardware to handle different CP charging methods. This idea of charging for content usage on the client side is similar to the ideas of the superdistribution model and soft-denchi system. The main feature of the proposed system is that it performs the illegal playback prevention and usage charging functions independently by performing charge computation inseparably and simultaneously with the playback of digital content while maintaining the convenience of services for end users.

This article first explains the precondition and requirements of this service and then outlines the proposed model, data format, and associated player. Next, it describes an implementation of the proposed system based on an MP3* player.

2. Client-side charging system

2.1 Service requirements

If content playback and charge processing are performed independently of each other, there is a strong risk of content being viewed or listened to without usage fees being paid or of usage fees being collected when content has not been played back. Making content playback and charge processing inseparable on the client enables CPs to collect their usage fees and end users to use content while paying each CP accordingly in a trouble-free manner. It also enables content to be distributed freely. General requirements for setting up such a service can be broadly divided into those on the CP side and those on the end-user side.

1) CP-side requirements
   - Charge processing must be executed simultaneously with content playback.
   - Charge settings need to be modifiable on a content-by-content basis.
   - Usage fees must be collected in proportion to content usage.
2) End-user requirements
   - Content must be played back when charge processing is performed.
   - Content must be usable by any end user on any terminal by copying that content.
   - There should be no need to communicate with a CP or other entities at the time of playback.

2.2 Proposed model

The proposed system consists of a CP, fee-collecting agent, and end user. The CP first prepares content data (M) and encrypts it to encrypted content (M'). Then, using a data creation function that constructs charge logic (P), which defines the rules for collecting usage fees, the CP formats specialized content (data) that combines P and M'. The client terminal has a specialized player for playing the specialized content (data). It consists of a signature-verification module (Verifier), a data-splitting module (Splitter), a content-playback module (Decoder), a control module (Manager), and a smart card (**Fig. 1**). The Verifier checks to see whether data has been delivered from the correct server and whether it has been tampered with. This function is necessary to prevent the use of M' or P that might have been altered. The Splitter divides data into M' and P. The smart card, in turn, executes P, performs charge processing, and generates a key (k) for decrypting M'. Performing both charge processing and key generation on the smart card means that computational results obtained on the smart card are needed for content playback. It also prevents mischarging resulting from executing only charge processing and illegal use of content by executing key generation without charging. The Decoder consists of the Decrypting part that decrypts M' using k and the Decoding part that plays back M. The Manager sends P to the smart card, passes k obtained from the smart card to the Decoder, monitors whether P is being correctly executed on the smart card, and terminates playback if it is not correct. Furthermore, if the decryption of M' is not proceeding correctly, the Manger prevents charging from taking place (see 2.4).

2.3 Format of specialized content data

The data format used for our scheme is shown in **Fig. 2**. Data is divided into n blocks (data = {$block_1$, $block_2$, ..., $block_n$}) per charge unit. Each $block_i$ (i = 1, ..., n) corresponds to the smallest unit for charging and consists of charge logic (P_i) describing the charging for that unit and content M_i' for that charge unit ($block_i$ = {P_i, M_i'}). For example, charge logic (P_i) might instruct the system to charge 5 yen for ten seconds of listening to or viewing of that content, to give a 50% discount if the amount charged for that content exceeds 300 yen, and to charge nothing after the

* MP3: Data format defined by MPEG-1 (Motion Picture Experts Group 1) audio layer 3.

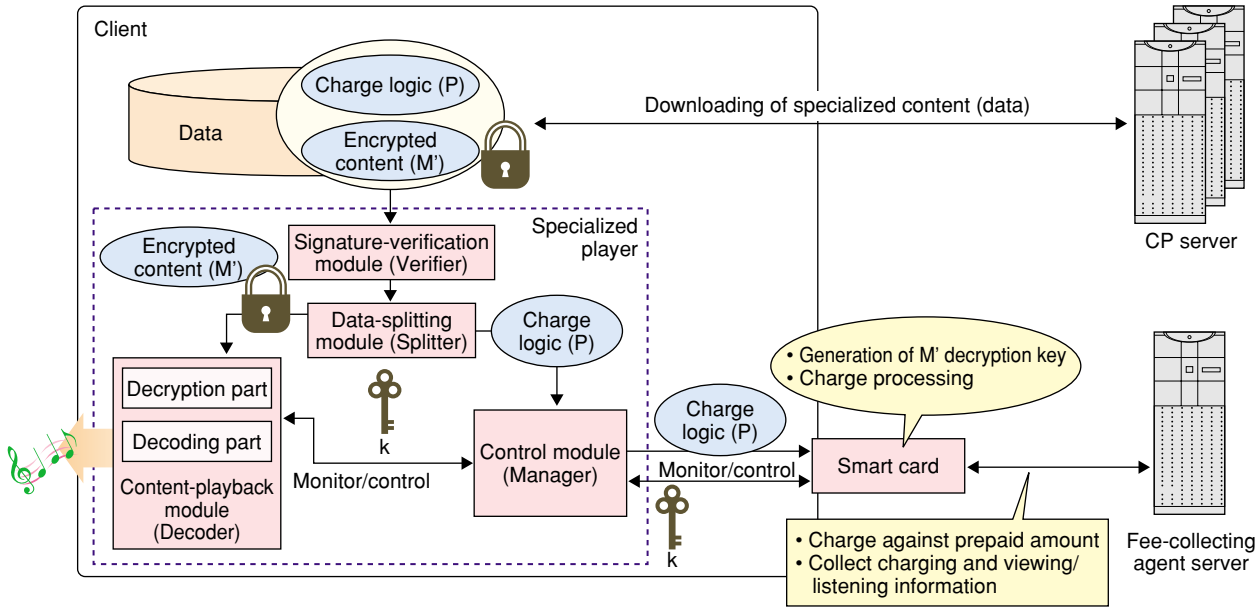

Fig. 1. Configuration of specialized player.

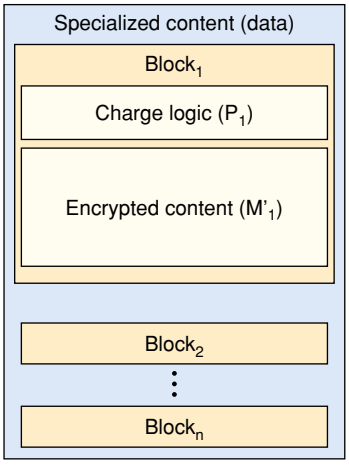

Fig. 2. Format of specialized content data.

amount exceeds 700 yen. This information is written in a special format.

We created data according to the following procedure.

1) Encrypt a charge-unit's worth of MP3 data using key k_i to obtain encrypted data (M_i'). Combine this data with charge logic (P_i) for that data plus the message authentication code (MAC_i) of data (M_i). This combined data is treated as one block of data ($block_i$).
2) Include in data $block_i$ i) secret information to be shared by the CP and smart card and ii) the digital signature for $block_i$ and the secret information.

2.4 Playback procedure at the specialized player

The playback procedure between the specialized player and smart card is shown in **Fig. 3**.

1) The smart card performs user authentication based on a personal identification number (PIN), and the specialized player and smart card exchange the session key (k).
2) The specialized player sends the smart card a charge request (E_k) that contains the key for encrypting P_i, the decryption key (k_{i-1}) of the previous charge unit, and the hash value ($hash_{i-1}$) of content data after decryption.
3) The smart card performs charge processing and generates decryption key k_i, encrypts this decryption key using k, and sends the result to the specialized player. Here, the generation of decryption key k_i is performed using k_{i-1} and $hash_{i-1}$.
4) The specialized player decrypts the content data and verifies MAC_i included in $block_i$ of the data. If the verification succeeds, the player sends a charge-commit request to the smart card and plays back the music. If the verification fails, it sends a charge-rollback request to the smart card and terminates playback.
5) When it receives a charge-commit request, the smart card subtracts a usage fee corresponding to the amount of playback from the prepaid balance. If it receives a charge-rollback request, it performs no fee subtraction and terminates processing.

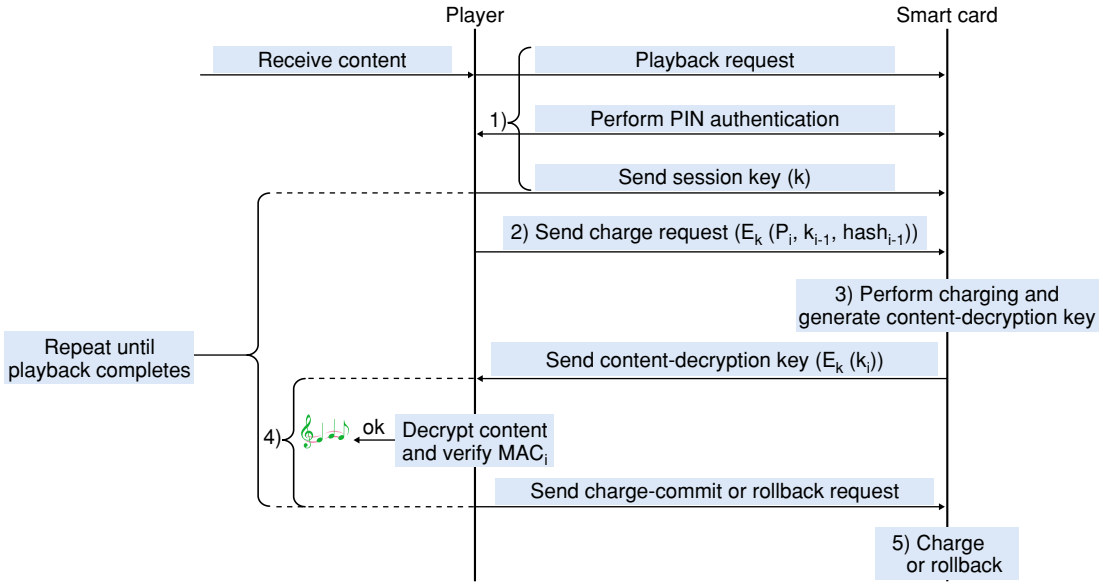

Fig. 3. Playback procedure between specialized player and smart card.

3. Implementation and evaluation

This section describes a prototype that we implemented to verify the feasibility of the charging system. The target content used in this implementation was music data in MP3 format. The implementation was achieved by modifying an existing MP3 player (Zinf [12]). The playback procedure and data configuration are described below.

The specialized content downloaded via the network was played back on the client terminal and the playback performance was measured and evaluated. Compared with ordinary playback, the communication with the smart card and the processing within the smart card constitute overheads. Furthermore, to prevent skipping, the charge-unit time must be set with these overheads in mind. The communication with the smart card and charge processing and key generation within it take 2 s. Therefore, a charge-unit time of 2 s or more should enable playback without skipping, leading to correct playback with charging in 2-s periods.

The size of specialized content (data) increases as the charge-unit time becomes shorter because the numbers of charge logic (P) and MAC entries increase with the number of additional charge units. For a five-minute piece of music, for example, this increase could come to 150 entries of P and MAC (corresponding to an increase in data size of about 64 bytes $\times$ 150). In the proposed model, content does not necessarily have to be downloaded from the network, which means that an increase in data size may not be a serious problem. Nevertheless, if the data size causes it to fill up the terminal's memory or recording media (such as an SD card or memory stick), users may demand smaller data sizes. Thus, the charge-unit time must be decided taking into account both this need and security.

4. Conclusion

In this article, we described a content charging system that performs charge computation in a manner inseparable from content playback. This system aims to enable unrestrained distribution of content by providing client-side charge processing as opposed to the current style of paying each content provider according to its charging scheme for each item of content. We also reported on a prototype implementation for testing this system. We found that charge computation could be executed inseparably from content playback and that playback and charging could be performed appropriately. Here, we assumed that the specialized player was achieved with tamper-resistant software. In future research, we plan to investigate a system that presumes tamper resistance not just for the specialized player but for the entire system through cooperative interaction between smart cards, specialized players, servers, and so on.

References

[1] Microsoft Product Activation: http://www.Microsoft.com/japan/windowsxp/pro/techinfo/productactivation/asp/
[2] M. Inamura, T. Tanaka, and K. Nakao, “Realizing Illegal Copy Protection for Digital Contents,” Symposium on Cryptography and Information Security (SCIS), 2003 (in Japanese).
[3] K. Inamura and T. Tanaka, “Implementation and Evaluation of Illegal Copy Protection for Digital Contents,” CSEC-22, Jul. 7, 2003 (in Japanese).
[4] MagicGate: http://www.sony.co.jp/Products/mssupport/media/ms_mg.html
[5] R. Mori, M. Kawahara, and Y. Ohtaki, “Superdistribution: The Microelectronic Approach to Intellectual Property Right Processing,” Information Processing, Vol. 37, No. 2, 1996 (in Japanese).
[6] K. Kanno, “Operation Management System and Operation Management Method,” Patent 1998-83298 (Japan), 1998 (in Japanese).
[7] H. Takata, “Information Management Equipment, Information Management System, and Media for Storing Information Management Software,” Patent 2001-249730 (Japan), 2001 (in Japanese).
[8] Keitaide-Music Consortium: http://www.keitaide-music.org/index_e.html
[9] R. Hoshino, H. Aono, R. Hoshino, S. Hongo, M. Suzuki, K. Akai, and T. Matsumoto, “The secure charging model on the client, and its application,” JIPS 65th National Convention, 2003 (in Japanese).
[10] 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,” 21st CSEC Group Meeting, 2003 (in Japanese).
[11] 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).
[12] Zinf: http://www.zinf.org/

Hiroshi Aono
Manager, Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. and M.S. degrees in information science from Kyushu Institute of Technology, Fukuoka in 1987 and 1989, respectively. He joined NTT in 1989. He is engaged in research of object-oriented design methods, R&D of network management systems using those methods, and R&D of security technologies. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the Information Processing Society of Japan (IPSJ).

Reiko Hoshino
Network Management Development Department, NTT DoCoMo Inc.
She received the B.E. and M.S. degrees in information science from Ochanomizu University, Tokyo in 2000 and 2002, respectively. She joined NTT DoCoMo in 2002. She is engaged in research on security technologies, especially in the area of tamper-resistant mobile environments. She is a member of IPSJ.

Sadayuki Hongo
Director, Network Management Development Department, NTT DoCoMo Inc.
He received the B.E. and M.E. degrees in electronic engineering from Iwate University, Iwate in 1982 and 1984, respectively. He joined NTT in 1984. He is engaged in research on intelligent telephone terminals, telephone-terminal operation behavior, icon recognition, computational theory of visual information processing, multimedia education, and information security. He is a member of IEICE and IPSJ.