IEICE Electronics Express, Vol.7, No.20, 1534–1538

An efficient access control method for composite multimedia content

Shoko Imaizumi[1,2a)], **Masaaki Fujiyoshi**[2], **and Hitoshi Kiya**[2]

[1] *Industrial Research Institute of Niigata Prefecture*
1–11–1 Abuminishi, Chuo-ku, Niigata-shi, Niigata 950–0915, Japan

[2] *Graduate School of System Design, Tokyo Metropolitan University*
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan

a) *shoko.imaizumi@m.ieice.org*

Abstract: This paper proposes an access control method for composite multimedia content in which only a single key is delivered to a user. The proposed method simultaneously controls access to each medium in one composite multimedia content in which a medium can be hierarchically encoded. This method introduces recursive hash chains for key generation so that the number of delivered key is reduced to one, whereas the conventional method having the above mentioned features has to deliver multiple keys to a user. The managed key in the proposed method is also reduced to one.

Keywords: scalable hierarchical access control, hash chain, media-aware encryption, key delivery, key management

Classification: Science and engineering for electronics

References

[1] J. C. Birget, X. Zou, G. Noubir, and B. Ramamurthy, "Hierarchy-based access control in distributed environment," *Proc. IEEE ICC*, Helsinki, Finland, vol. 1, pp. 229–233, June 2001.

[2] Y. Wu, D. Ma, and R. H. Deng, "Progressive protection of JPEG 2000 codestreams," *Proc. IEEE ICIP*, Singapore, pp. 3447–3450, Oct. 2004.

[3] M. Joye and S. M. Yen, "One-way cross-trees and their applications," *LNCS*, vol. 2274, pp. 346–356, 2002.

[4] M. Fujiyoshi, S. Imaizumi, and H. Kiya, "Encryption of composite multimedia contents for access control," *IEICE Trans. Fundamentals*, vol. E90-A, no. 3, pp. 590–596, March 2007.

[5] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.

1 Introduction

As a huge variety of communication channels and terminals exist, scalable transmission becomes popular in which a low quality content is decoded by decompressing a certain portion of the compressed codestream. For control-

DOI: 10.1587/elex.7.1534
Received August 16, 2010
Accepted September 16, 2010
Published October 25, 2010

ling access to scalable content, scalable access control methods have been studied [1, 2, 3, 4].

In a simple method for scalable access control, components of a content are individually encrypted with different keys [1]. This method, thus, manages keys as many as the components and it delivers the keys to a user in proportion to the number of components to be decoded. By using hash chains [5], the number of managed keys and that of delivered keys are reduced to the number of scalability types, such as spatial, temporal, or SNR scalability, in a content [2, 3]. Similarly, the access control method that manages and delivers keys as many as media are applied to composite multimedia content [4].

This paper proposes an efficient access control method for composite multimedia content; the proposed method reduces the number of delivered keys to one by introducing recursive hash chains, though this method controls access to content as well as the conventional method [4]. It is noted that the proposed method manages only a single key.

2 Preliminary

For composite multimedia content, a method controls access to a content based on not only medium type (audio, video, text, and so on) but also the depth of hierarchical structure in a medium (audio quality, frame rate, the resolution of image/video, etc). In this paper, it is assumed that a content represented by $\mathcal{U}$ consists of X media and a medium has a hierarchical structure which the depth is $N+1$, as

$$\mathcal{U} = \{\mathcal{A}^1, \mathcal{A}^2, \ldots, \mathcal{A}^X\}, \tag{1}$$

$$\mathcal{A}^1 \supset \mathcal{A}^1_1 \supset \mathcal{A}^1_2 \supset \cdots \supset \mathcal{A}^1_N, \tag{2}$$

where $\mathcal{A}^x$ $(x = 1, 2, \ldots, X)$ represents a medium and $\mathcal{A}^1$ has a hierarchical structure.

Hereafter, the content shown in Fig. 1 is used as an example. That is, content $\mathcal{U}$ consists of three media $\mathcal{A}^1$, $\mathcal{A}^2$, and $\mathcal{A}^3$ $(X = 3)$ and the hierarchy

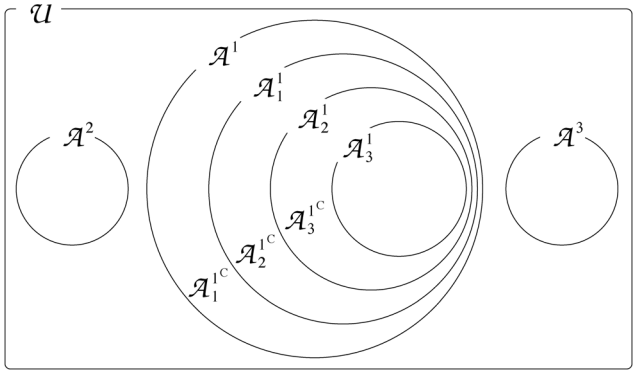

Fig. 1. An example composite multimedia content, $\mathcal{U}$. The number of media is three $(X = 3)$ and the hierarchy depth of medium $\mathcal{A}^1$ is four $(N+1 = 4)$.

DOI: 10.1587/elex.7.1534
Received August 16, 2010
Accepted September 16, 2010
Published October 25, 2010

depth of $\mathcal{A}^1$ is four $(N+1=4)$, i.e.,

$$\mathcal{A}^1 \supset \mathcal{A}^1_1 \supset \mathcal{A}^1_2 \supset \mathcal{A}^1_3. \tag{3}$$

The complementary sets $\mathcal{A}^{1^c}_1$, $\mathcal{A}^{1^c}_2$, and $\mathcal{A}^{1^c}_3$ in Fig. 1 are

$$\mathcal{A}^{1^c}_1 = \mathcal{A}_1 - \mathcal{A}^1_1, \tag{4}$$
$$\mathcal{A}^{1^c}_2 = \mathcal{A}^1_1 - \mathcal{A}^1_2, \tag{5}$$
$$\mathcal{A}^{1^c}_3 = \mathcal{A}^1_2 - \mathcal{A}^1_3, \tag{6}$$

respectively.

In the next section, an access control method which delivers only a single key to a user is proposed for composite multimedia content. The method also manages only a single key.

3 Proposed method

This section proposes an efficient access control method for composite multimedia content. Here, the key generating mechanism in the proposed method is focused. The proposed mechanism reduces the number of managed keys and that of delivered keys to one by introducing recursive hash chains.

Hereafter, a more practical example based on Fig. 1 is used, and the example is shown in Fig. 2 (a). In this example, $\mathcal{A}^1$ is digital video, and it is playable in several frame rates; 120, 60, 30, and 15 frames per second (fps). Frames decoded at each rate are represented by $\mathcal{A}^1$, $\mathcal{A}^1_1$, $\mathcal{A}^1_2$, and $\mathcal{A}^1_3$, respectively. Media $\mathcal{A}^2$ and $\mathcal{A}^3$ are audio and text, respectively.

Access control is provided based on not only media but also the frame rates of the video in this example. Keys are generated as shown in Fig. 2 (b), and each key is used for encryption and decryption of the corresponding component; For the video, key $K_{\mathcal{A}^{1^c}_1}$ is for $\mathcal{A}^{1^c}_1$ that is a complementary set

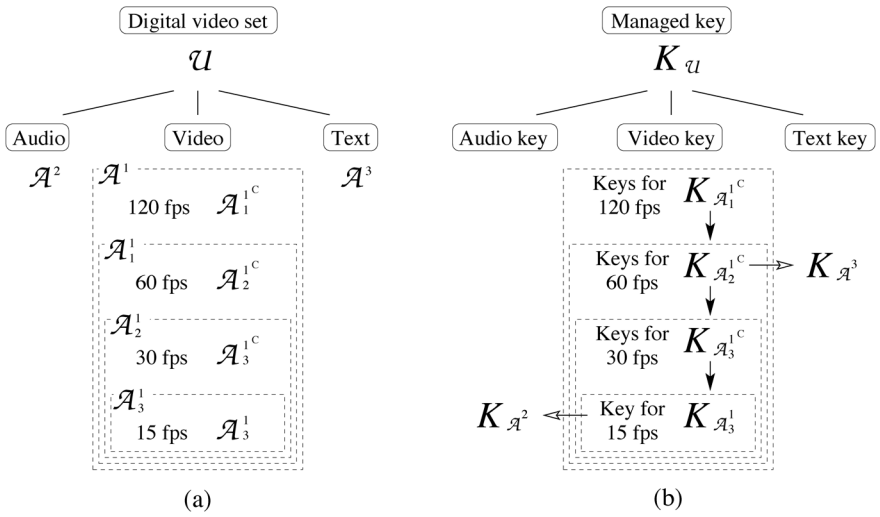

Fig. 2. The proposed method. (a) the content to be protected and (b) the key generating algorithm. A black arrow shows an ordinary hash function and a white arrow shows a recursive hash function.

DOI: 10.1587/elex.7.1534
Received August 16, 2010
Accepted September 16, 2010
Published October 25, 2010

for frames decoded at 120 fps only. Similarly, keys $K_{\mathcal{A}_2^{1c}}$ and $K_{\mathcal{A}_3^{1c}}$ are for $\mathcal{A}_2^{1c}$ and $\mathcal{A}_3^{1c}$, respectively. Keys $K_{\mathcal{A}^2}$ and $K_{\mathcal{A}^3}$ are for audio and text, respectively. It is noted that key $K_{\mathcal{U}}$ is the single managed key and it is used as $K_{\mathcal{A}_1^{1c}}$ for the video.

Firstly in the proposed key generation, keys $K_{\mathcal{A}_n^{1c}}$ $(n = 2, 3, \ldots, N)$ and $K_{\mathcal{A}_N^1}$ are generated from $K_{\mathcal{A}_1^{1c}}$ as

$$K_{\mathcal{A}_n^{1c}} = H^{n-1}\left(K_{\mathcal{A}_1^{1c}}\right) = H^{n-2}\left(H\left(K_{\mathcal{A}_1^{1c}}\right)\right), \quad n = 2, 3, \ldots, N, \tag{7}$$

$$K_{\mathcal{A}_N^1} = H\left(K_{\mathcal{A}_N^{1c}}\right), \tag{8}$$

where $H(\cdot)$ is a one-way hash function. Eqs. (7) and (8) represent an ordinary hash chain [5], and the chain is shown with black arrows in Fig. 2 (b).

On the other hand, keys $K_{\mathcal{A}^2}$ and $K_{\mathcal{A}^3}$ are generated by *recursive hash chains* in the proposed key generation. In this example, these keys are given as

$$K_{\mathcal{A}^2} = H\left(K_{\mathcal{A}_3^1} \oplus H\left(K_{\mathcal{A}_3^1}\right)\right), \tag{9}$$

$$K_{\mathcal{A}^3} = H\left(K_{\mathcal{A}_2^{1c}} \oplus H\left(K_{\mathcal{A}_2^{1c}}\right)\right), \tag{10}$$

where $\oplus$ represents a bitwise exclusive or operation. As shown in Eqs. (9) and (10) which represent recursive hash chains, keys given by Eqs. (7) and (8) are repeatedly used to generate other hash chains different from the ordinary hash chain. The recursive hash chains are shown with combination of black and white arrows in Fig. 2 (b).

It is clear from Eqs. (9) and (10), a user permitted to decode frames at 120 and/or 60 fps can obtain $K_{\mathcal{A}^2}$ and $K_{\mathcal{A}^3}$ in this example, and he/she can decode the audio and the text in addition to the video. Similarly, a user permitted to decode frames at 30 and/or 15 fps can access to the audio as well as the video. Meanwhile, a user permitted to decode only the audio or the text can obtain nothing but either $K_{\mathcal{A}^2}$ or $K_{\mathcal{A}^3}$. It is noted that any arbitrary key combination can be used to generate another hash chain, it affects the access permissions to the audio and the text in this example. Moreover, any operation can be employed instead of a bitwise exclusive or.

The proposed method just delivers only a single key to any user regardless of his/her access permission, though it serves an access control to composite multimedia content based on not only media but also the hierarchy structure in a medium. This feature is achieved by recursive hash chains in which keys generated by an ordinary hash chain are reused to generate other hash chains. The proposed method also reduces the number of managed keys to one.

4 Evaluation

The proposed method is evaluated by comparing with the conventional method [4] that uses ordinary hash chains [5] only. Evaluation is given in terms of the number of managed and delivered keys.

DOI: 10.1587/elex.7.1534
Received August 16, 2010
Accepted September 16, 2010
Published October 25, 2010

Table I. Comparisons in terms of the number of managed and delivered keys.

	Proposed	Conventional [4]
Managed keys	1	X
Delivered keys	1	X

Table I shows the results of comparisons. The proposed method manages and delivers only a single key regardless of the number of media and the depth of the hierarchical structure in a medium, whereas the conventional method [4] must manage and deliver keys as many as media. The table brings out the effectiveness of the proposed method.

5 Conclusions

An efficient access control method introducing recursive hash chains has been proposed for composite multimedia content in this paper. The proposed method reduces the number of both managed and delivered keys to one by the proposed key generation mechanism using recursive hash chains.

Applying the proposed method to other security technologies such as authentication and digital watermarking is a further work.

DOI: 10.1587/elex.7.1534
Received August 16, 2010
Accepted September 16, 2010
Published October 25, 2010