An Efficient Access Control Scheme for Multimedia Content
Using Modified Hash Chain

Shoko Imaizumi
Division of Information Sciences
Graduate School of Advanced Integration Science
Chiba University
Chiba, Japan
Email: imaizumi@chiba-u.jp

Masaaki Fujiyoshi, Hitoshi Kiya
Dept. of Information and Communication Systems
Tokyo Metropolitan University
Tokyo, Japan
Email: fujiyoshi-masaaki@tmu.ac.jp,
kiya@sd.tmu.ac.jp

Abstract—This paper proposes an access control scheme for multimedia content consisting of several media such as text, images, sound, and so on. The proposed scheme simultaneously controls access to each medium of multimedia content in which a hierarchy based on the quality (resolution, frame rate, bit rate, and so on) is allowed to be in one medium. The proposed scheme derives keys through hash chains, and each medium/entity is encrypted with each individual key. By introducing modified hash chains, the proposed scheme manages only a single key for multimedia content, and it delivers only a single key to a user for the content regardless of which parts in the content the user can access; whereas the conventional access control schemes having the above mentioned features manage and/or deliver multiple keys. The single managed key is not delivered to any user. Furthermore the proposed scheme is resilient to collusion attacks. Performance analysis shows the effectiveness of the proposed scheme. The proposed scheme is more secure and simpler than the conventional scheme in terms of key management and delivery.

Keywords—multimedia communication; access control; key derivation; hash chain; cryptography.

I. INTRODUCTION

With the growth in network technology, the exchange of digital images and sound as well as text become very common regardless of whether the digital content is used for commercial purpose or not. Since such digital content is easily duplicated and re-distributed, protecting copyrights and privacy is an important issue. Access control based on naïve encryption (encrypting the whole content) [1] or media-aware encryption [2]–[6] has been studied widely to protect digital content.

A simple and straightforward way for realizing versatile access control to multimedia content consisting of several media to which several entities belong is encrypting each entity individually. This approach, however, has to manage a large number of keys, according to the number of entities in multimedia content. Moreover, a user has to receive a number of keys, according to the number of accessible entities.

On the other hand, for JPEG 2000 [7] coded images and/or MPEG-4 fine granularity scalability [8] coded videos, scalable access control schemes have been proposed [2]–[6]. These schemes utilize one- or multi-dimensionally hierarchical scalability provided by coding technologies so that a user can obtain an image or a video in the permitted quality from one common codestream. In addition, hash chain [9], [10] is introduced to several schemes for reducing the managed and managed keys [3]–[6].

Though a hash chain-based access control scheme has been proposed for multimedia content [11], the number of managed keys increases dependently on not only the number of media but also the dimensions of hierarchies in the media. The number of delivered keys is increased as many as the number of managed keys. Moreover, malicious users can share their keys to increase accessible media/entities in this scheme.

This paper proposes an access control scheme for multimedia content which the scheme manages and delivers only a single key. The proposed scheme assumes that content consists of several media and there is a scalable hierarchy on the quality in one of media. By introducing modified hash chains, the managed key is one as many as the delivered key regardless of which media/entities the user is allowed to access. The managed key is not delivered to any user in terms of security against key leakage. Moreover, the proposed scheme is resilient to collusion attacks which malicious users can share their keys to access much more portions beyond their rights illegally.

This paper consists of five sections. Section II mentions the conventional access control scheme for multimedia and describes the problems of the conventional scheme. The new scheme is proposed in Section III and is analyzed in Section IV. Finally, conclusions are drawn in Section V.

II. CONVENTIONAL ACCESS CONTROL SCHEME FOR MULTIMEDIA CONTENT

This section briefly describes the conventional access control scheme for multimedia content [11], and summarizes problems of the conventional scheme to clarify the aim of this work.
A. Conventional Scheme

The conventional scheme [11] assumes that content consists of $M$ different media (image, video, sound, text, and so on) which a hierarchy (image/video resolution, frame rate, bit rate, etc.) exists in each medium. In the text medium, the appearing order of paragraphs has its own meaning, and it is referred to as a semantic hierarchy. The scheme uses a symmetric encryption technique.

For multimedia content consisting of $M$ different media, this scheme manages $M$ keys. Fig. 1 shows an example of multimedia content where $M = 2$. For the $m$-th medium where $m = 1, 2, \ldots, M$, encryption keys are derived from managed key $K_{D_m}$ that corresponds to the $m$-th medium, where $D_m$ represents the number of entities in the medium, i.e., the depth of the hierarchy. Encryption keys $K_{d_m}$’s are derived through a hash chain as

$$K_m = H^{D_m-d_m} \left(K_m^{D_m}\right), \quad d_m = 0, 1, \ldots, D_m - 1,$$  

where $H^\alpha(\beta)$ represents that cryptographic one-way hash function $H(\cdot)$ is applied to $\beta$ recursively $\alpha$ times. The $d_m$-th entity in the $m$-th medium is encrypted with its corresponding encryption key, $K_m^{d_m}$.

A user receives $M$ decryption keys. Each user receives different set of decryption keys, which are delivered keys, due to which media/entities the user is allowed to access, but all users receive the common encrypted multimedia content. From the delivered keys, the user derives keys for accessible entities in accessible media through the same hash chain as used in the encryption key derivation. That is,

$$K_m = H^{D_m-d_m} \left(K_m^{\Delta_m}\right), \quad \delta_m = 1, 2, \ldots, \Delta_m - 1,$$  

where $K_m^{\Delta_m}$ is the delivered key for the $m$-th medium. By using $\Delta_m$ decryption keys, the user decrypts $\Delta_m$ entities from the first entity to the $\Delta_m$-th entity.

A user who receives $K_m^{d_m}$ cannot access any entities in the $m$-th medium, because one-way property of $H(\cdot)$ prevents the user to generate any other valid keys for the $m$-th medium of the content. The conventional scheme introduced this unusable key concept in order to cope with medium-based access control.

B. Problems of the Conventional Scheme


- the number of managed and delivered keys
- collusion attack-vulnerable

As mentioned in the previous section, the conventional scheme encrypts entities in a medium independently of other media. This feature of the conventional scheme requires managed and delivered keys as many as media in the multimedia content, i.e., $M$ keys are managed and $M$ keys are delivered to a user for content consisting of $M$ different media. This conventional scheme employs ordinary hash chains [9] rather than cross-hash trees [10] in essentials.

The latter problem is also attributed to the feature just described in the above paragraph. Though introducing unusable key concept in order to serve medium-based access control, the conventional scheme allows malicious users to collude to access inaccessible media. A user who can display images and another user who is allowed to read texts share their keys and obtain both images and text paragraphs.

In the next section, a new access control scheme for multimedia content is proposed. The proposed scheme manages only a single key and delivers also only a single key to a user regardless of which media/entities in the content the user can access. In addition, the proposed scheme is resistant to collusion attack.

III. PROPOSED SCHEME

This section proposes a new access control scheme for multimedia content. The proposed scheme assumes that multimedia content $C$ consists of $M$ media and the first medium has a hierarchical structure:

$$C = \{G_1^1, G_1^2, \ldots, G_1^m, \ldots, G_1^M\},$$  

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset \cdots \supset G_1^D_m,$$

where $G_1^m$ ($m = 1, 2, \ldots, M$) represents the $m$-th medium content itself, and $D_1$ is the depth of the hierarchy in the first medium. The complementary sets represent entities in medium $G_1^1$ as

$$E_1^{d_m} = G_1^{d_m} - G_1^{d_m+1}, \quad d_m = 1, 2, \ldots, D_m - 1,$$  

and

$$E_1^{D_m} = G_1^{D_m}.$$

The proposed scheme derives keys from single managed key $K_C$ and encrypts content $C$ by encrypting $E_1^{d_m}$’s using those corresponding keys. In addition, this scheme delivers only a single key to each user.

Fig. 2 shows an example conceptual diagram of the assumed multimedia content, where content $C$ consists of
Figure 2. An example of multimedia content conceptual diagram in the proposed scheme (the number of media \(M = 3\) and the depth of the hierarchical structure in the first medium \(D_1 = 4\)).

Figure 3. A practical example of multimedia content (the number of media \(M = 3\) and the depth of video \(D_1 = 4\)).

three media, \(G_1^1, G_2^1, \) and \(G_3^1\), i.e., \(M = 3\), and the hierarchy depth of medium \(G_1^1\) is four \((D_1 = 4)\), i.e.,

\[ G_1^1 \subset G_2^1 \subset G_3^1 \subset G_4^1. \]  

\(E_1^1, E_2^1, E_3^1,\) and \(E_4^1\) are entities in medium \(G_1^1\).

A. Key Derivation and Encryption

This section provides the key derivation mechanism in the proposed scheme under the condition content \(C\) is abstracted as Fig. 2. For easy understanding, more practical example is given in Fig. 3. Content \(C\) in Fig. 3 consists of video, sound, and text, i.e., \(M = 3\), and video has a hierarchy with four in depth in terms of the frame rate, i.e., \(D_1 = 4\). In this example, \(G_1^1\) is digital video, and it is playable in several frame rates; 120, 60, 30, and 15 frames per second (fps). Shown in Fig. 4, frames decoded at each rate are represented by \(G_1^1, G_2^1, G_3^1,\) and \(G_4^1\), respectively. Media \(G_2^1\) and \(G_3^1\) are sound and text, respectively.

In the example here, access control is provided based on not only media but also the frame rates of video. For content \(C\) shown in Fig. 3, keys for encryption are derived as shown in Fig. 5, and each key is used to encrypt and decrypt the corresponding medium/entity. For the video, \(K_{E_1^1}\) is managed key \(K_C\)

\begin{align*}
\text{Key for} & \quad 120 \text{ fps} \quad K_{E_1^1} \\
\text{Key for} & \quad 60 \text{ fps} \quad K_{E_1^2} \cdots \quad K_{E_1^3} \\
\text{Key for} & \quad 30 \text{ fps} \quad K_{E_1^2} \quad K_{E_1^3} \\
\text{Key for} & \quad 15 \text{ fps} \quad K_{E_1^4} \\
\end{align*}

\(K_{E_1^4}\) which represents frames decoded at 120 fps only. Similarly, keys \(K_{E_2^1}, K_{E_3^1}\), and \(K_{E_4^1}\) are for \(E_2^1, E_3^1,\) and \(E_4^1\), respectively. Keys \(K_{E_2^1}\) and \(K_{E_3^1}\) are for sound and text, respectively. It is noted that key \(K_C\) is the single managed key.
Firstly in the proposed scheme, keys $K_{E_1^{d_1}}$ are derived from $K_C$ as

$$K_{E_1^{d_1}} = H^{d_1}(K_C), \quad d_1 = 1, 2, \ldots, D_1,$$  
(8)

where $H(\cdot)$ is a cryptographic one-way hash function. Eq. (8) represents an ordinary hash chain [9], and the chain is shown with solid arrows in Fig. 5.

Meanwhile, keys $K_{E_2}^{d_1}$ and $K_{E_3}^{d_1}$ are derived by modified hash chains in the proposed scheme. In this example, these keys are given as

$$K_{E_2}^{d_1} = H\left(f\left(K_{E_1^{d_1}}, H\left(K_{E_2}^{d_1}\right)\right)\right),$$  
(9)

$$K_{E_3}^{d_1} = H\left(f\left(K_{E_2}^{d_1}, H\left(K_{E_3}^{d_1}\right)\right)\right),$$  
(10)

respectively, where $f(\cdot)$ is an function with two input and one output in which the length of inputs and output are identical. A bitwise exclusive or operation is a simple example of function $f(\cdot)$. As shown in Eqs. (9) and (10) which represent modified hash chains introduced in this paper, keys given by Eq. (8) are repeatedly used to derive other hash chains that are different from the ordinary hash chains. The modified hash chains are shown with combination of solid and dashed arrows in Fig. 5.

Each entity $E_{dm}^{d_1}$ is encrypted using each corresponding key $K_{E_{dm}^{d_1}}$ and encrypted content $C$ is opened to public.

**B. Delivered Key for Each User and Decryption**

1) User allowed to access video, sound, and text: A user permitted to decode frames at 120 or 60 fps receives $K_{E_1^{d_1}}$ or $K_{E_2}^{d_1}$ shown in Figs. 6 (a) and (b). Eq. (8) is same as,

$$K_{E_1^{d_1}} = H\left(K_{E_1^{d_1}}\right), \quad d_1 = 1, 2, \ldots, D_1.$$  
(11)

The user can obtain $K_{E_1^{d_1}}$ ($d_1 = 1, 2, 3, 4$) using an ordinary hash chain in Eq. (11).

As shown in Fig. 5, keys $K_{E_1^{d_1}}$ and $K_{E_2}^{d_1}$ for sound $E_2^{d_1}$ and text $E_3^{d_1}$ are generated from $K_{E_1^{d_1}}$ and $K_{E_2}^{d_1}$, respectively, using modified hash chains in Eqs. (9) and (10). Thus the user can also obtain $K_{E_2}^{d_1}$ and $K_{E_3}^{d_1}$ and play sound and read text in addition to watch the video.

2) User allowed to access video and sound: A user can access frames decoded at 30 or 15 fps receives $K_{E_1^{d_1}}$ or $K_{E_2}^{d_1}$ as shown in Figs. 6 (c) and (d). The user has $K_{E_2}^{d_1}$ but does not have $K_{E_2}^{d_1}$. Thus the user can obtain only $K_{E_2}^{d_1}$ for sound $E_2^{d_1}$ by Eq. (9) and play sound as well as the video.

3) User allowed to access sound: A user allowed to access only sound $E_2^{d_1}$ receives $K_{E_2}^{d_1}$ as shown in Fig. 6 (e). $K_{E_2}^{d_1}$ is a key generated by Eq. (9). Any keys cannot be generated from $K_{E_2}^{d_1}$.

4) User allowed to access text: A user allowed to access only text $E_3^{d_1}$ receives $K_{E_3}^{d_1}$ as shown in Fig. 6 (f). $K_{E_3}^{d_1}$ is a key generated by Eq. (10). $K_{E_3}^{d_1}$ can generate no other key.

### Table I

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of managed keys</td>
<td>1</td>
<td>$M$</td>
</tr>
<tr>
<td>The number of delivered keys</td>
<td>1</td>
<td>$M$</td>
</tr>
<tr>
<td>Delivery of managed keys</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Collision attack resilience</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**C. Features**

Two main features of the proposed scheme are briefly summarized here.

By introducing modified hash chains, the proposed scheme reduces both the managed and delivered keys to one. In contrast, the conventional scheme [11] manages and delivers keys as many as media.

By using modified hash chains, multiple media are related to prevent malicious users to collude. The conventional scheme is collusion attack-vulnerable, because the conventional scheme encrypts each medium separately.

In addition to the above features, the single managed key is not delivered to any users in the proposed scheme while the conventional scheme delivered the managed keys to some users.

It is noted that any arbitrary function and key combination can be used for a modified hash chain and that any arbitrary key assign can be used to properly control access to the content.

**IV. EVALUATION**

The proposed scheme is evaluated by comparing with the conventional scheme [11] which uses ordinary hash chains [9] only. Evaluation is given in terms of the number of managed and delivered keys, delivery of managed keys, and collusion attack resilience.

Table I shows the results of comparisons. The proposed scheme manages and delivers only a single key regardless of the number of media and the depth of the hierarchical structure in a medium, whilst the conventional scheme [11] must manage and deliver keys as many as media. The single managed key is not delivered to any user in the proposed scheme, whereas the managed keys are delivered to some users in the conventional scheme [11]. In addition, the proposed scheme is resilient to collusion attacks while the conventional scheme [11] is naive for collusion attacks. The table brings out the effectiveness of the proposed scheme.

**V. CONCLUSION**

This paper has proposed a new access control scheme for multimedia content in which modified hash chains are employed. The proposed scheme manages only a single key. This scheme also delivers only a single key to a user regardless of which portions of the content to which the user can access. In the proposed scheme, the single managed
key is not delivered to any user. Furthermore, the proposed scheme prevents malicious users to collude for accessing much more portions. Comparison result summarizes the effectiveness of the proposed scheme. The proposed scheme thus controls access to multimedia content securely and simply in comparison to the conventional scheme.
Applying the proposed scheme to content in which each medium has its own hierarchical structure is a further work. Moreover, we would like to apply the proposed scheme to other security technologies such as digital watermarking and secret sharing.

REFERENCES


