View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by IntechOpen

We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

154
Countries delivered to

Our authors are among the
TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

A Novel Access Control Scheme for Multimedia Content with Modified Hash Chain

Shoko Imaizumi[1], Masaaki Fujiyoshi[2] and Hitoshi Kiya[2]
[1]*Chiba University*
[2]*Tokyo Metropolitan University*
Japan

IntechOpen

1. Introduction

With the continuing growth in network technology, the exchange of digital images and audio as well as text has 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. For the protection of digital content, *access control* based on naïve encryption (encrypting the whole content) (1) or media-aware encryption (2–6) has been studied widely.

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

Scalable access control schemes have been proposed (2–6) for JPEG 2000 (7) coded images and/ or MPEG-4 fine granularity scalability (8) coded videos. These schemes control access to entities corresponding to hierarchical scalability assigned by coding technologies, so that the user can obtain an image or a video at the permitted quality from one common codestream. *Hash chain* (9; 10) has also been introduced to several schemes for reduction of managed keys and the keys delivered to each user (3–6).

Although a hash chain-based access control scheme has been proposed for multimedia content (11), the number of managed keys and that of delivered keys increase, depending on the kinds of media in the content.

In this chapter, we introduce an efficient access control scheme for multimedia content. The scheme assumes that multimedia content consists of several media and there is a scalable hierarchy on the quality in each or one medium. By introducing *modified* hash chains (MHCs), the number of managed keys is reduced to one and the number of delivered keys is also less than the conventional scheme (11). When a scalable hierarchy is in only one medium, the delivered key is particularly reduced to one. The managed key is not delivered to any user, providing security against key leakage. This scheme is also resilient to collusion attacks, in which malicious users illegally access the multimedia content at higher quality than that allowed by their access rights.

IntechOpen

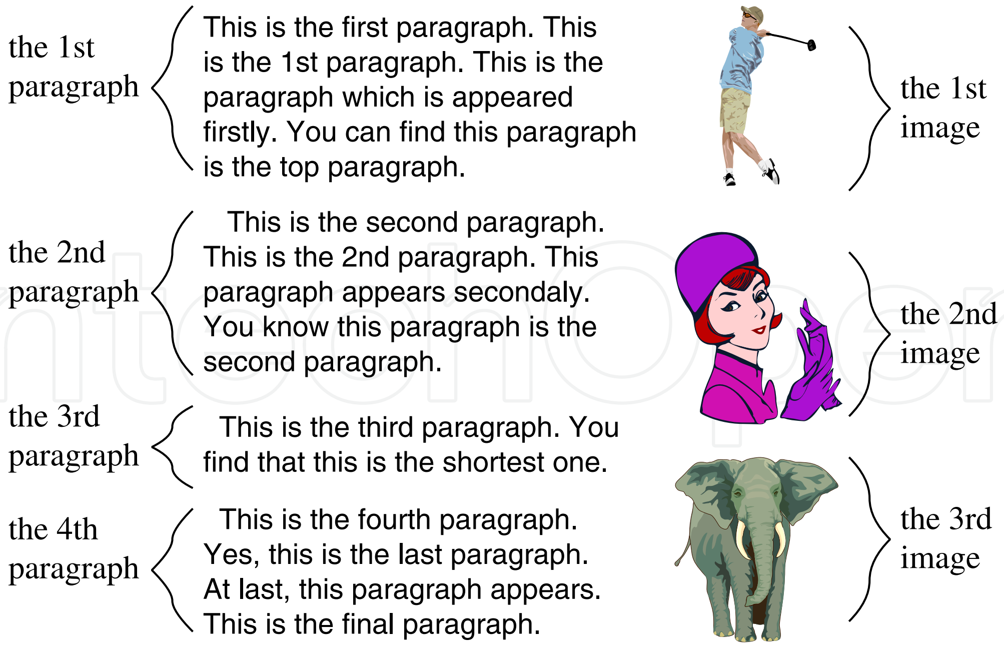

the 1st paragraph
This is the first paragraph. This is the 1st paragraph. This is the paragraph which is appeared firstly. You can find this paragraph is the top paragraph.
the 2nd paragraph
This is the second paragraph. This is the 2nd paragraph. This paragraph appears secondaly. You know this paragraph is the second paragraph.
the 3rd paragraph
This is the third paragraph. You find that this is the shortest one.
the 4th paragraph
This is the fourth paragraph. Yes, this is the last paragraph. At last, this paragraph appears. This is the final paragraph.
the 1st image
the 2nd image
the 3rd image

Fig. 1. An example of multimedia content (the number of media $M = 2$, the number of entities in the first medium $D_1 = 4$, and the number of entities in the second medium $D_2 = 3$).

This chapter is organized as follows. Section 2 mentions the conventional access control scheme for multimedia content and summarizes the requirements for access control. The new scheme is described in Section 3 and Section 4, and is analyzed in Section 5. Finally, conclusions are drawn in Section 6.

2. Access control for multimedia content

This section briefly describes the conventional access control scheme for multimedia content (11), and summarizes the requirements for access control to clarify the aim of this work.

2.1 Conventional scheme (11)

The conventional scheme (11) assumes that multimedia content consists of M different media (image, video, audio, text, and so on), in each of which a scalable hierarchy (image/video resolution, frame rate, audio quality, etc) exists; 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 a particular multimedia content consisting of M different media, this scheme manages M keys. Figure 1 shows an example of multimedia content where $M = 2$. For the m-th medium where $m = 1, 2, \ldots, M$, all encryption keys are derived from managed key K_m^1. Encryption keys $K_m^{d_m}$'s are derived through an ordinary hash chain (OHC) (9) as

$$K_m^{d_m} = H^{d_m - 1}\left(K_m^1\right), \; d_m = 2, 3, \ldots, D_m + 1, \tag{1}$$

where $H^{\alpha}(\beta)$ represents a cryptographic one-way hash function $H(\cdot)$ applied to β recursively α times, and D_m represents the number of entities in the medium, i.e., the depth of the scalable hierarchy. The d_m-th entity in the m-th medium is encrypted with its corresponding encryption key, $K_m^{d_m}$.

Each user receives different set of M decryption keys due to which media/entities the user is allowed to access to, and also receives the common encrypted multimedia content. From the delivered keys, the user derives decryption keys $K_m^{\delta_m}$'s for accessible entities in accessible media through the same OHC as used in the encryption key derivation. That is,

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

where $K_m^{\Delta_m}$ is the delivered key for the m-th medium. It is noted that decryption keys $K_m^{\delta_m}$'s are the same as encryption keys $K_m^{d_m}$'s. By using Δ_m decryption keys, the user decrypts Δ_m entities from the first entity to the Δ_m-th entity.

A user who receives $K_m^{D_m+1}$ cannot access any entities in the m-th medium, because one-way property of $H(\cdot)$ prevents the user to derive any other valid keys for the m-th medium of the multimedia content. The conventional scheme introduced this *unusable key* concept in order to cope with medium-based access control.

2.2 Requirements

We describe three requirements for access control of multimedia content, i.e.,

- reduction of managed keys and delivered keys,
- protection of managed key,
- collusion attack resilience.

As mentioned in the previous section, the conventional scheme (11) encrypts entities in a medium independently of those in other media. This feature of the conventional scheme requires to manage and deliver the same number of keys as media in the multimedia content, i.e., M keys are managed and M keys are delivered to a user for the multimedia content consisting of M different media. This conventional scheme employs a simple OHC (9) rather than cross-way hash trees (10).

The conventional scheme (11) delivers the managed keys to users who are allowed to access at least one medium at the highest quality. The managed keys should not be delivered to any users and should be protected against key leakage.

A collusion attack is made by multiple users to obtain multimedia content with higher quality than that allowed by their access rights. For example, when a user who is allowed to display images and another user who is allowed to read text paragraphs share their keys, they can also obtain audio coupled with images and text paragraphs. Access control schemes must be resilient to collusion attacks.

In the next section, we introduce a new access control scheme for multimedia content. This scheme manages only one key for a particular multimedia content and delivers less key to each user than the conventional method (11), regardless of which media/entities in the content the user can access. The single managed key is not delivered to any user. It is also resistant to collusion attack.

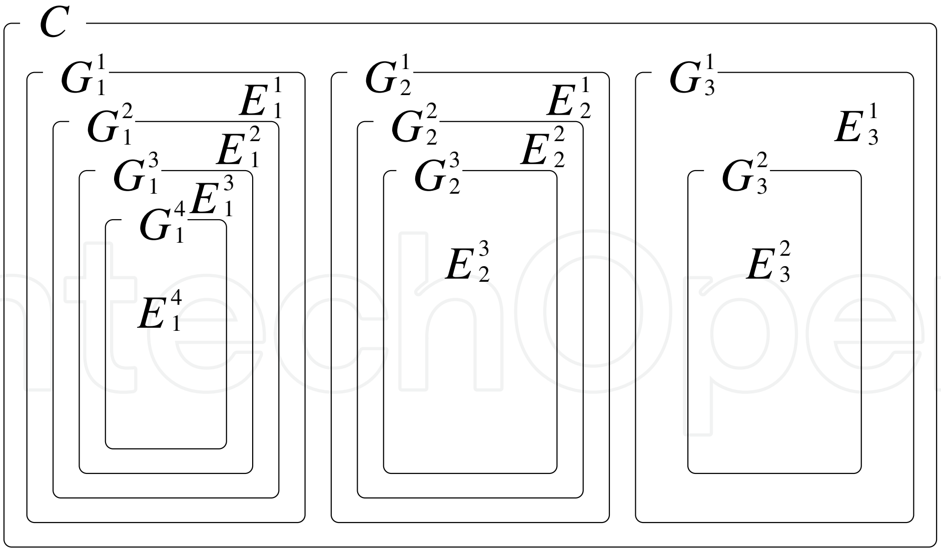


Fig. 2. An example of multimedia content conceptual diagram with a scalable hierarchy in each medium (the number of media $M = 3$ and the depths of each scalable hierarchy $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

3. Access control for multimedia content with multiple hierarchies (12)

First, we assume that multimedia content C consists of M media and each medium has a hierarchical structure;

$$C = \left\{ G_1^1, G_2^1, \ldots, G_m^1, \ldots, G_M^1 \right\}, \tag{3}$$

$$G_m^1 \supset G_m^2 \supset G_m^3 \supset \cdots \supset G_m^{D_m}, \quad m = 1, 2, \ldots, M, \tag{4}$$

where G_m^1 represents the m-th medium itself, and D_m is the depth of the scalable hierarchy in the m-th medium. The complementary sets represent entities in medium G_m^1 as

$$E_m^{d_m} = G_m^{d_m} - G_m^{d_m+1}, \quad d_m = 1, 2, \ldots, D_m - 1, \tag{5}$$

and

$$E_m^{D_m} = G_m^{D_m}. \tag{6}$$

This scheme derives keys from single managed key K_C and encrypts multimedia content C by encrypting $E_m^{d_m}$'s using those corresponding keys.

Fig. 2 shows an example conceptual diagram of the assumed multimedia content, where multimedia content C consists of three media, G_1^1, G_2^1, and G_3^1, i.e., $M = 3$, and the depths of each scalable hierarchy in medium G_m^1 are four, three, and two ($D_1 = 4$, $D_2 = 3$, and $D_3 = 2$), respectively, i.e.,

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset G_1^4, \tag{7}$$

$$G_2^1 \supset G_2^2 \supset G_2^3, \tag{8}$$

$$G_3^1 \supset G_3^2. \tag{9}$$

$E_m^{d_m}$'s are entities in medium G_m^1.

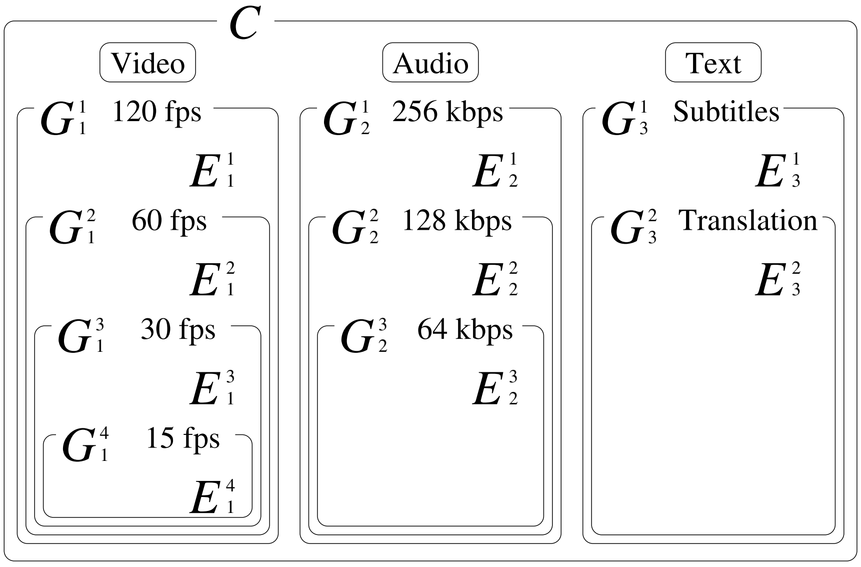


Fig. 3. A practical example of multimedia content with a scalable hierarchy in each medium (the number of media $M = 3$ and the depths of each scalable hierarchy $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

For easy understanding, more practical example of Fig. 2 is given in Fig. 3. Multimedia content C in Fig. 3 consists of video G_1^1, audio G_2^1, and text G_3^1, i.e., $M = 3$, and each medium has a scalable hierarchy, whose depths are four, three, and two, i.e., $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$, respectively.

3.1 Key derivation using a MHC

In the example based on Fig. 3, access control is provided based not only on media, but also on each scalable hierarchy in each medium. Keys for encryption are derived as shown in Fig. 4, and each key is used to encrypt and decrypt the corresponding entity. For example, $K_{E_1^1}$ is a key for entity E_1^1 which represents video frames decoded only at 120 frames per second (fps). $K_{E_1^2}$, $K_{E_1^3}$, and $K_{E_1^4}$ are similarly keys for E_1^2, E_1^3, and E_1^4, respectively. $K_{E_2^{d_2}}$ and $K_{E_3^{d_3}}$ are also keys for audio $E_2^{d_2}$ and text $E_3^{d_3}$ ($d_2 = 1, 2, 3$, $d_3 = 1, 2$), respectively. It is noted that key K_C is the single managed key.

Firstly, key $K_{E_1^0}$ is derived from K_C as

$$K_{E_1^0} = H\left(K_C\right), \tag{10}$$

where $H(\cdot)$ is a cryptographic one-way hash function. Similarly, keys $K_{E_m^{d_m}}$'s are derived by

$$\begin{aligned} K_{E_m^{d_m}} &= H^{d_m}\left(K_{E_m^0}\right), \\ d_m &= 1, 2, \ldots, D_m, \quad m = 1, 2, 3, \end{aligned} \tag{11}$$

where keys $K_{E_2^0}$ and $K_{E_3^0}$ are given in the next paragraph. Eq. (11) represents OHCs (9), and the OHCs are shown with solid arrows in Fig. 4.

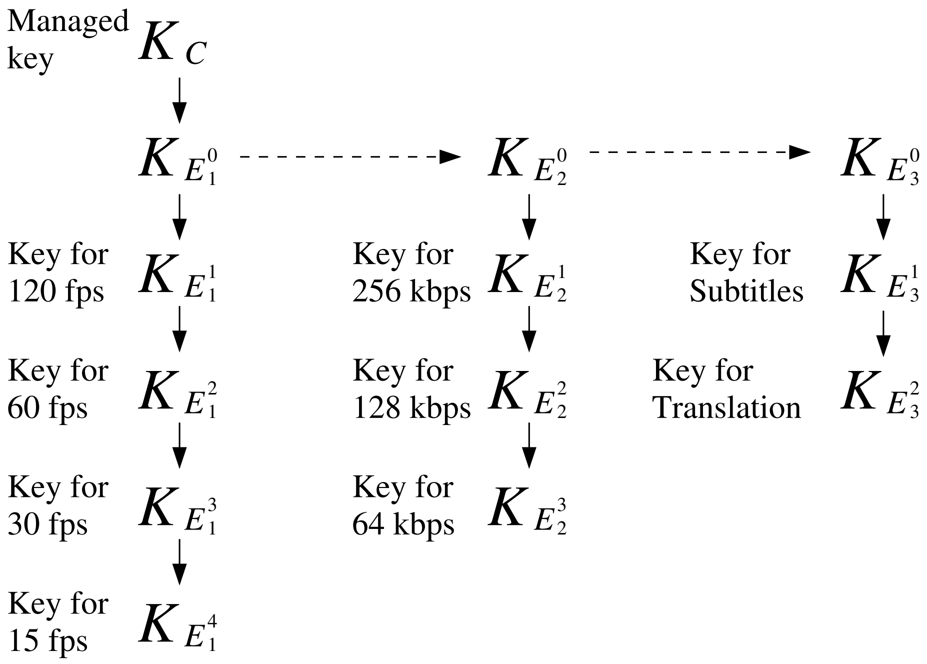


Fig. 4. Key derivation to control access to the multimedia content shown in Fig. 3. Solid arrows represent OHCs and dashed arrows represent a MHC.

Meanwhile, keys $K_{E_2^0}$ and $K_{E_3^0}$ are derived by a MHC. In this example, these keys are given as

$$\begin{aligned} K_{E_m^0} &= H\left(f\left(K_{E_{m-1}^0}, H\left(K_{E_{m-1}^0}\right)\right)\right) \\ &= H\left(f\left(K_{E_{m-1}^0}, K_{E_{m-1}^1}\right)\right), \\ m &= 2, 3, \end{aligned} \tag{12}$$

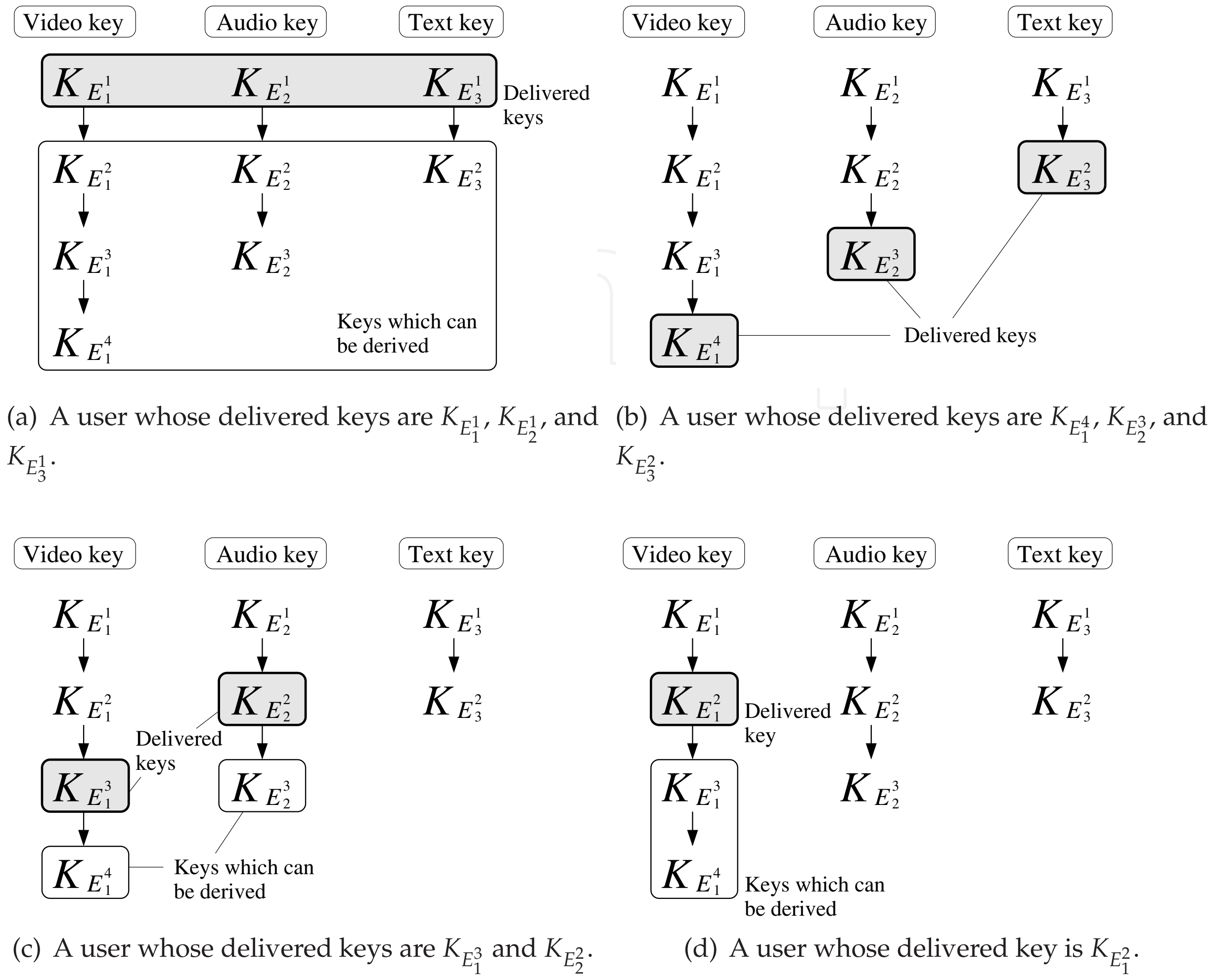
respectively, where $f(\cdot)$ is a function with two inputs and one output in which the length of inputs and output are identical. A bitwise exclusive or (XOR) operation is a simple example of function $f(\cdot)$. As shown in Eq. (12) which represents a MHC introduced in this scheme, keys given previously are repeatedly used to derive another hash chain that is different from the OHC. The MHC is shown with dashed arrows in Fig. 4.

3.2 Encryption and decryption

Each entity $E_m^{d_m}$ is encrypted using each corresponding key $K_{E_m^{d_m}}$, and then, multimedia content C is opened to public.

3.2.1 User allowed to access three media

A user allowed to access the whole multimedia content receives three keys $K_{E_1^1}$, $K_{E_2^1}$, and $K_{E_3^1}$ as shown in Fig. 5 (a). The user derives all keys needed to decrypt all entities, through OHCs. Each user allowed to access three media at arbitrary quality also receives three keys $K_{E_1^{d_1}}$, $K_{E_2^{d_2}}$, and $K_{E_3^{d_3}}$. A user allowed to access each medium at the lowest quality, i.e., video at 15 fps, audio at 64 kbps, and translation data, receives three keys $K_{E_1^4}$, $K_{E_2^3}$, and $K_{E_3^2}$ as shown in Fig. 5 (b). The user cannot, however, derive any keys from his/her delivered keys.



(a) A user whose delivered keys are $K_{E_1^1}$, $K_{E_2^1}$, and $K_{E_3^1}$.

(b) A user whose delivered keys are $K_{E_1^4}$, $K_{E_2^3}$, and $K_{E_3^2}$.

(c) A user whose delivered keys are $K_{E_1^3}$ and $K_{E_2^2}$.

(d) A user whose delivered key is $K_{E_1^2}$.

Fig. 5. Delivered keys and derived keys for each user.

3.2.2 User allowed to access two media

Fig. 5 (c) shows an example user allowed to access two of the three media. In this example, the user can access video at 30 fps and audio at 128 kbps. The user receives two keys $K_{E_1^3}$ and $K_{E_2^2}$, and derives keys $K_{E_1^4}$ for video and $K_{E_2^3}$ for audio, respectively.

3.2.3 User allowed to access a single medium

If a user can access only movie at 60 fps, the user receives single key $K_{E_1^2}$ and derives keys $K_{E_1^3}$ and $K_{E_1^4}$ dependently as shown in Fig. 5 (d). Each user who can access a single medium receives single key $K_{E_1^{d_1}}$, $K_{E_2^{d_2}}$, or $K_{E_3^{d_3}}$.

In this scheme, the number of keys which a user receives is equal to the number of media which he/she can decode. Each user uses only OHCs to derive keys from the delivered keys. Keys K_C, $K_{E_1^0}$, $K_{E_2^0}$, and $K_{E_3^0}$ are not delivered to any user.

3.3 Features

Three main features of the access control scheme are briefly summarized here. They have satisfied with the requirements described in Section 2.2.

This scheme, introducing a MHC, has reduced the number of managed keys to one. The number of delivered keys is less than the conventional scheme (11) which manages and delivers the same number of keys as media in the multimedia content.

Each key for each entity is derived from the single managed key. The managed key is not delivered to any user.

The scheme using a MHC can prevent malicious users to collude to decode multimedia content at higher quality than that allowed by their access rights. As shown in Fig. 5, although keys are derived from delivered keys through OHCs, the OHCs are isolated from each other. This structure provides collusion attack resilience.

It is noted that any arbitrary function and key combination can be used for a MHC. In addition, it is noted that any arbitrary key assignment can be used to properly control access to the multimedia content.

4. Access control for multimedia content with a single hierarchy (13)

In this section, we assume that multimedia content C consists of M media and only medium G_1^1 has a hierarchical structure which the depth is D_1, as

$$C = \left\{G_1^1, G_2^1, \ldots, G_m^1, \ldots, G_M^1\right\}, \tag{13}$$

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset \cdots \supset G_1^{D_1}. \tag{14}$$

This scheme derives keys from single managed key K_C and encrypts multimedia content C by encrypting entities $E_m^{d_m}$'s using those corresponding keys $K_{E_m^{d_m}}$'s. In addition, each user receives only a single key regardless of his/her access right.

Fig. 6 shows an example conceptual diagram of the assumed multimedia content, where multimedia content C consists of three media, G_1^1, G_2^1, and G_3^1, i.e., $M = 3$, and the depth of the scalable hierarchy in medium G_1^1 is four ($D_1 = 4$), i.e.,

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset G_1^4. \tag{15}$$

E_1^1, E_1^2, E_1^3, and E_1^4 are entities in medium G_1^1. More practical example is given in Fig. 7. Multimedia content C in Fig. 7 consists of video, audio, and text, i.e., $M = 3$, and video is four-tiered, i.e., $D_1 = 4$, in terms of frame rates. In this example, G_1^1 is video, and it is playable in several frame rates; 120, 60, 30, and 15 fps.

4.1 Key derivation using MHCs

For multimedia content C shown in Fig. 7, keys for encryption are derived as shown in Fig. 8, and each key is used to encrypt and decrypt the corresponding medium/entity. $K_{E_1^1}$ is a key for entity E_1^1 which represents video frames decoded only at 120 fps. $K_{E_1^2}$, $K_{E_1^3}$, and $K_{E_1^4}$ are

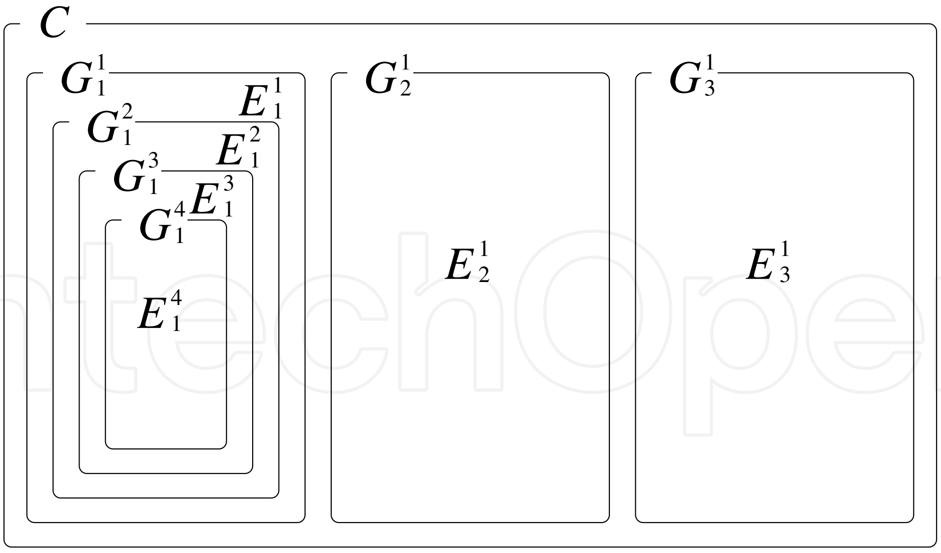


Fig. 6. An example of multimedia content conceptual diagram with a scalable hierarchy in the first medium (the number of media $M = 3$ and the depth of the scalable hierarchy $D_1 = 4$).

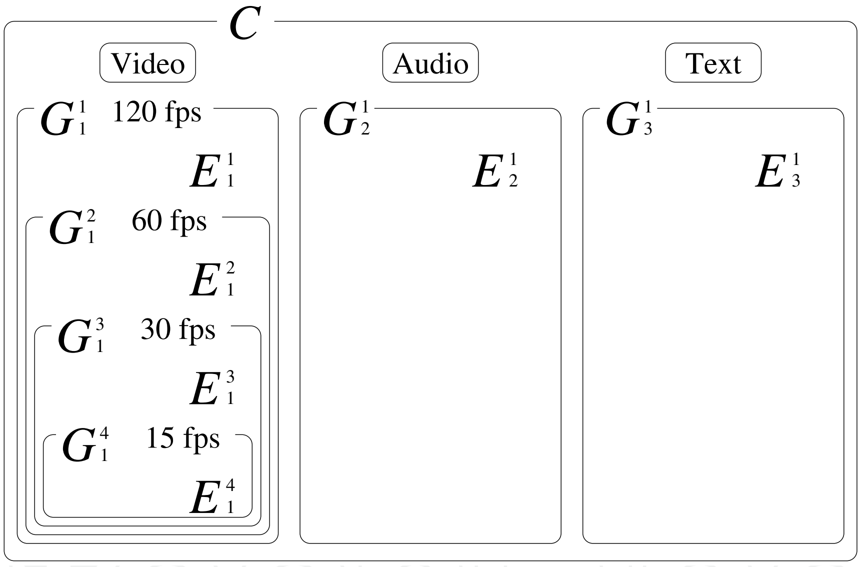


Fig. 7. A practical example of multimedia content with a scalable hierarchy in the first medium (the number of media $M = 3$ and the depth of the scalable hierarchy $D_1 = 4$).

similarly keys for E_1^2, E_1^3, and E_1^4, respectively. $K_{E_2^1}$ and $K_{E_3^1}$ are also keys for audio E_2^1 and text E_3^1, respectively. It is noted that key K_C is the single managed key.

Firstly, keys $K_{E_1^{d_1}}$ are derived from the managed key K_C as

$$K_{E_1^{d_1}} = H^{d_1}(K_C), \quad d_1 = 1, 2, \ldots, D_1, \tag{16}$$

where $H(\cdot)$ is a cryptographic one-way hash function. Eq. (16) represents an OHC (9), and the OHC is shown with solid arrows in Fig. 8.

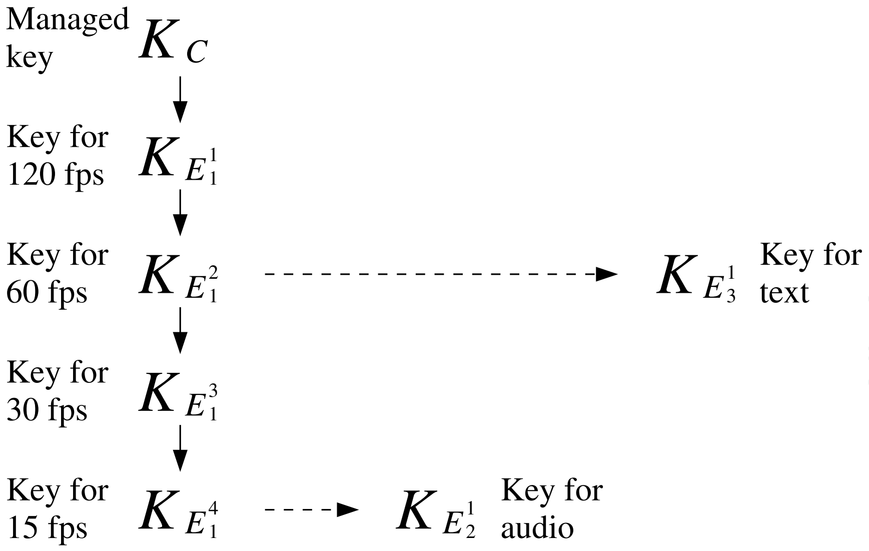

Managed key K_C
Key for 120 fps $K_{E_1^1}$
Key for 60 fps $K_{E_1^2}$
Key for 30 fps $K_{E_1^3}$
Key for 15 fps $K_{E_1^4}$
$K_{E_3^1}$ Key for text
$K_{E_2^1}$ Key for audio

Fig. 8. Key derivation to control access to the multimedia content shown in Fig. 7. All users who are allowed to access video with any frame rates can access audio medium. Users who are allowed to access video with 120 or 60 fps can also view text paragraphs. Solid arrows represent an OHC and dashed arrows represent MHCs.

Meanwhile, keys $K_{E_2^1}$ and $K_{E_3^1}$ are derived by MHCs. In this example, these keys are given as

$$K_{E_2^1} = H\left(f\left(K_{E_1^4}, H\left(K_{E_1^4}\right)\right)\right), \tag{17}$$

$$\begin{aligned} K_{E_3^1} &= H\left(f\left(K_{E_1^2}, H\left(K_{E_1^2}\right)\right)\right) \\ &= H\left(f\left(K_{E_1^2}, K_{E_1^3}\right)\right), \end{aligned} \tag{18}$$

respectively, where $f(\cdot)$ is a function with two inputs and one output in which the inputs are the same length of the output. A simple example of function $f(\cdot)$ is a bitwise exclusive or (XOR) operation. As shown in Eqs. (17) and (18), keys given by Eq. (16) are repeatedly used to derive other hash chains that are different from the OHCs. The MHCs are shown with dashed arrows in Fig. 8.

4.2 Encryption and decryption

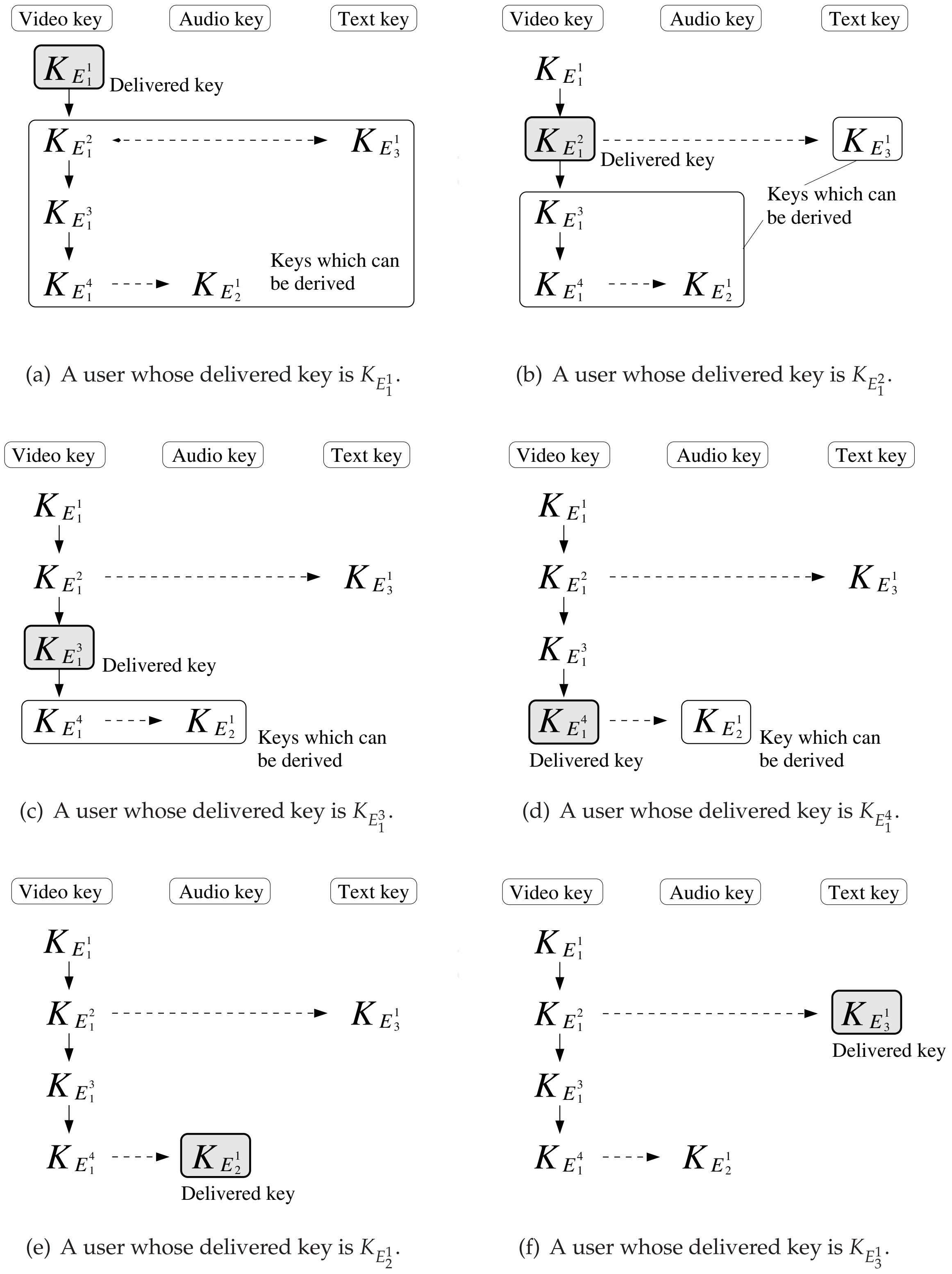
Each medium/entity $E_m^{d_m}$ is encrypted using corresponding key $K_{E_m^{d_m}}$, and multimedia content C is opened to public.

4.2.1 User allowed to access video, audio, and text

A user permitted to decode video frames at 120 or 60 fps receives $K_{E_1^1}$ or $K_{E_1^2}$ shown in Figs. 9 (a) and (b). Eq. (16) is the same as

$$K_{E_1^{d_1}} = H\left(K_{E_1^{d_1-1}}\right), \quad d_1 = 2, 3, \ldots, D_1. \tag{19}$$

The user can obtain $K_{E_1^{d_1}}$ $(d_1 = 2, 3, 4)$ using an OHC in Eq. (19).



(a) A user whose delivered key is $K_{E_1^1}$.

(b) A user whose delivered key is $K_{E_1^2}$.

(c) A user whose delivered key is $K_{E_1^3}$.

(d) A user whose delivered key is $K_{E_1^4}$.

(e) A user whose delivered key is $K_{E_2^1}$.

(f) A user whose delivered key is $K_{E_3^1}$.

Fig. 9. A single delivered key and derived keys for each user.

As shown in Fig. 8, keys $K_{E_2^1}$ and $K_{E_3^1}$ for audio E_2^1 and text E_3^1 are derived from $K_{E_1^4}$ and $K_{E_1^2}$, respectively, using MHCs in Eqs. (17) and (18). Thus the user can also obtain $K_{E_2^1}$ and $K_{E_3^1}$ and play audio and read text in addition to watch the video.

4.2.2 User allowed to access video and audio

A user can access video frames decoded at 30 or 15 fps receives $K_{E_1^3}$ or $K_{E_1^4}$ as shown in Figs. 9 (c) and (d). The user obtains $K_{E_1^4}$, but cannot derive $K_{E_1^2}$. Thus the user cannot derive $K_{E_3^1}$ for text E_3^1, and can derive only $K_{E_2^1}$ for audio E_2^1 by Eq. (17) and play audio as well as the video.

4.2.3 User allowed to access audio

A user allowed to access only audio E_2^1 receives $K_{E_2^1}$ as shown in Fig. 9 (e). $K_{E_2^1}$ is a key derived by Eq. (17). Any keys cannot be derived from $K_{E_2^1}$.

4.2.4 User allowed to access text

A user allowed to access only text E_3^1 receives $K_{E_3^1}$ as shown in Fig. 9 (f). $K_{E_3^1}$ is a key derived by Eq. (18). $K_{E_3^1}$ can derive no other key.

4.3 Features

The following three features of the access control scheme have satisfied the requirements described in Section 2.2.

By introducing MHCs, the number of managed keys and that of delivered keys are reduces to one, respectively. In contrast, the conventional scheme (11) manages and delivers the same number of keys as media.

The single managed key is the basis of each key for each entity/medium. Any user do not receive the managed key.

This scheme also prevents collusion attacks. Even if any of the users shown in Fig. 9 collude to access multimedia content at higher quality than that allowed by their access rights, they cannot access the content beyond their rights.

It is noted that any arbitrary function and key combination can be used for a MHC. In addition, it is noted that any arbitrary key assignment can be used to properly control access to the multimedia content.

5. Evaluation

The MHC-based scheme is evaluated by comparing with the conventional scheme (11) which uses only OHCs. Evaluation is given in terms of the number of managed keys and that of delivered keys, protection of managed keys, and collusion attack resilience.

Table 1 shows the results of comparisons. The MHC-based scheme manages only a single key regardless of both the number of media and the depths of each scalable hierarchy in each medium, whilst the conventional scheme must manage M keys, which is the same number

	MHC-based	Conventional (11) (OHC-based)
The number of managed keys	1	M
The number of delivered keys	between 1 and M	M
Protection of managed keys	Yes	No
Collusion attack resilience	Yes	Yes

Table 1. Comparisons in terms of the number of managed keys and that of delivered keys, protection of managed keys, and collusion attack resilience.

of media in the multimedia content. The MHC-based scheme delivers the same number of keys as accessible media, while the conventional scheme should deliver M keys in any case. Particularly, when only a single medium has a hierarchical structure, the MHC-based scheme constantly delivers a single key to each user.

The single managed key is not delivered to any user in the MHC-based scheme, whereas the managed keys are delivered to users allowed to access at least one medium at the highest quality in the conventional scheme. The MHC-based scheme is also resilient to collusion attacks as the conventional scheme. The table brings out the effectiveness of the MHC-based scheme.

6. Conclusion

This chapter has introduced a new access control scheme for multimedia content, in which MHCs are employed. The scheme manages only a single key regardless of both the number of media and the depths of each scalable hierarchy in each medium. Each user also receives less keys than the conventional method. Particularly, when a hierarchical structure exists in only one medium, any user receives a single key. The single managed key is not delivered to any user, providing security against key leakage. This scheme also prevents collusion attacks, in which malicious users illegally access the multimedia content at higher quality than that allowed by their access rights.

7. References

[1] B. B. Zhu, M. D. Swanson, and S. Li, "Encryption and authentication for scalable multimedia: current state of the art and challenges," in *Proc. SPIE*, vol.5601, pp.157–170, 2004.

[2] Z. Shahid, M. Chaumont, and W. Puech, "Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns," in *Proc. IEEE ICIP*, pp.1273–1276, 2009.

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

[4] Y. G. Won, T. M. Bae. and Y. M. Ro, "Scalable protection and access control in full scalable video coding," in *Proc. IEEE IWDW*, vol.4283 of *LNCS*, pp.407–421, 2006.

[5] S. Imaizumi, M. Fujiyoshi, Y. Abe, and H. Kiya, "Collusion attack-resilient hierarchical encryption of JPEG 2000 codestreams with scalable access control," in *Proc. IEEE ICIP*, pp.II–137–II–140, 2007.

[6] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "Efficient collusion attack-free access control for multidimensionally hierarchical scalability content," in *Proc. IEEE ISCAS*, pp.505–508, 2009.

[7] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system.* ISO/IEC 15444–1, 2004.

[8] *Information technology — Coding of audio – Visual objects – Part 2: Visual.* ISO/IEC 14496–2, 2004.

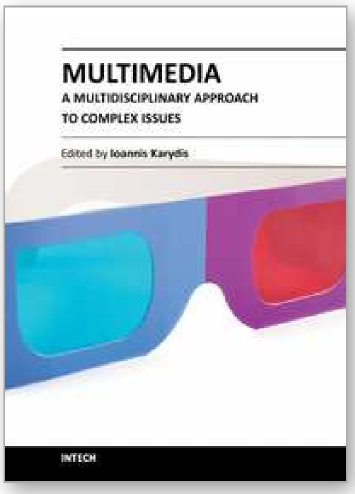
[9] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol.24, no.11, pp.770–772, 1981.

[10] M. Joye and S. M. Yen, "One-way cross-trees and their applications," in *Proc. IACR PKC*, vol.2274 of *LNCS*, pp.355–358, 2002.

[11] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE ICIP*, pp.1977–1980, 2006.

[12] S. Imaizumi, M. Fujiyoshi, H. Kiya, N. Aoki, H. Kobayashi, "Derivation Scheme for Hierarchical Access Control to Multimedia Content," in *Proc. International Workshop on Advanced Image Technology*, 2012, to be published.

[13] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "An efficient access control method for composite multimedia content," *IEICE Electronics Express*, vol.7, no.20, pp.1534–1538, 2010.



Multimedia - A Multidisciplinary Approach to Complex Issues

Edited by Dr. Ioannis Karydis

ISBN 978-953-51-0216-8
Hard cover, 276 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

The nowadays ubiquitous and effortless digital data capture and processing capabilities offered by the majority of devices, lead to an unprecedented penetration of multimedia content in our everyday life. To make the most of this phenomenon, the rapidly increasing volume and usage of digitised content requires constant re-evaluation and adaptation of multimedia methodologies, in order to meet the relentless change of requirements from both the user and system perspectives. Advances in Multimedia provides readers with an overview of the ever-growing field of multimedia by bringing together various research studies and surveys from different subfields that point out such important aspects. Some of the main topics that this book deals with include: multimedia management in peer-to-peer structures & wireless networks, security characteristics in multimedia, semantic gap bridging for multimedia content and novel multimedia applications.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Shoko Imaizumi, Masaaki Fujiyoshi and Hitoshi Kiya (2012). A Novel Access Control Scheme for Multimedia Content with Modified Hash Chain, Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis (Ed.), ISBN: 978-953-51-0216-8, InTech, Available from: http://www.intechopen.com/books/multimedia-a-multidisciplinary-approach-to-complex-issues/a-novel-access-control-scheme-for-multimedia-content-with-modified-hash-chain

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen