IEICE TRANS. FUNDAMENTALS, VOL.E90–A, NO.3 MARCH 2007

PAPER Special Section on Multimedia and Mobile Signal Processing

Encryption of Composite Multimedia Contents for Access Control

Masaaki FUJIYOSHI[†a)], ***Member***, **Shoko IMAIZUMI**[††], ***Student Member***, ***and*** **Hitoshi KIYA**[†], ***Member***

SUMMARY An encryption scheme is proposed that considers hierarchies in media, such as text, images, sound, and so on, in a composite multimedia content to enable versatile access control. In the proposed scheme, a content provider has only one managed key (the master key) for a particular composite multimedia content, and an user who is permitted to access a reserved content entities in the composite content receives only one key that is subordinately generated from the master key. Another key generated from the identical master key is delivered to another user, and this permits the user to access different entities. This scheme introduces a new key concept, namely "unusable key," to keep all entities encrypted in a particular medium and to simultaneously decrypt several entities in other media. The other new key, "numbering key," is also used in this scheme to support simultaneous partial decryption of multiple images that are coded with a scalable coding technology. Simulation results show the effectiveness of the proposed scheme; in particular, the length of the managed master key and that of keys to be delivered to users are small.

key words: *multimedia communication, access control, cryptography, image coding, Internet*

1. Introduction

The growth in network technology has seen that the exchange of digital images and sound as well as texts become very common regardless of whether these contents are commercial or non-commercial. Since such digital contents are easily duplicated and re-distributed, protecting copyrights and the privacy of contents is an important issue. Three main approaches exist for protecting, namely, naïve encryption (encrypting the whole content) [1], digital watermarking [2], and partial encryption [3]–[8]. A scheme for partial encryption is proposed in this paper for controlling access to composite multimedia contents.

Composite multimedia contents are made up of several media which several entities belong to each medium. A simple and straightforward way to realize versatile access control to composite multimedia contents encrypts each entities individually, similar to a partial encryption scheme [3] for JPEG 2000 (JP2) [9], [10] coded images. This approach, however, has to manage a large number of keys, according to the number of entities in a content. Moreover, an user also has to receive a number of keys, according to the number of accessible entities.

Manuscript received July 5, 2006.
Manuscript revised October 2, 2006.
Final manuscript received November 16, 2006.

[†]The authors are with the Faculty of System Design, Tokyo Metropolitan University, Hino-shi, 192–0397 Japan.
[††]The author is with the Industrial Research Institute of Niigata Prefecture, Niigata-shi, 950–0915 Japan.
a) E-mail: mfujiyoshi@m.ieice.org

DOI: 10.1093/ietfec/e90–a.3.590

For JP2 coded images and/or MPEG-4 fine granularity scalability (FGS) [11] coded videos, scalabilities are taken into account in some partial encryption schemes [4]–[8]. Scalability provides easy access to subsets of a codestream, and several scalabilities that have a hierarchical structure are available in the JP2 or MPEG-4 FGS standard format. By utilizing these hierarchical scalabilities, conventional *hierarchical encryption* schemes [7], [8] achieve

- all users receive one identical encrypted codestream,
- only one key (the master key) is managed,

though each user has one's own access permission. Since these schemes focus encryption of a single image or video, these schemes fit neither multiple images nor composite multimedia contents. Moreover, these schemes cannot help but decrypt at least one component in all the scalabilities, therefore expansion to medium oriented encryption in which all entities in a medium are often keep as encrypted is difficult.

In this paper, an encryption scheme for composite multimedia contents is proposed that enables versatile hierarchical access control [12], [13]. The proposed scheme manages one master key for a composite multimedia content and delivers decryption keys generated from the master key to users like schemes for JP2 codestreams [7], [8]. All users access only one encrypted content, although permission to access to decrypted content differs from each other. The proposed scheme introduces *unusable keys* to keep all entities encrypted in a particular medium and to simultaneously decrypt several entities in other media. In contrast to the proposed scheme, expansion of conventional schemes always decrypt at least one entity in all media. Moreover, to support several images coded by a scalable coding technology, a *numbering key* is used in the proposed scheme. The proposed scheme simultaneously and partially decrypts multiple images using this new concept.

2. Conventional Scheme for JP2

First in this section, the structure of JP2 codestreams [9], [10] and the conventional hierarchical encryption scheme [7] for JP2 coded images are briefly described. Then, differences in application and conditions between the conventional and the proposed schemes are mentioned to clarify the aim of this work.

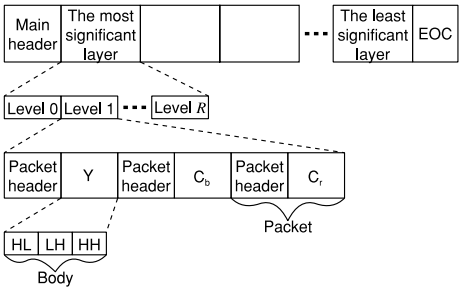


Fig. 1 A structure of JPEG 2000 codestreams [9], [10].

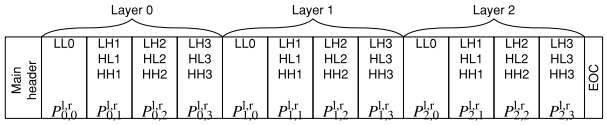


Fig. 2 A JPEG 2000 codestream of grayscale image (three layers, $L = 3$, and four resolution levels, $R = 4$) [9], [10].

2.1 JP2 Codestream

Figure 1 shows a JP2 codestream using YC_bC_r as the color space. This JP2 codestream's progression order is layer - resolution level - component - position (LRCP).

The main header is followed by the most significant layer and so on to the least significant layer. A codestream is terminated by the end of codestream (EOC) marker. Each layer is composed of data from each resolution level that corresponds to visual significance. A resolution level of zero only contains data from the LL subband, and the other resolution levels contain three subbands, i.e., HL, LH, and HH. If an original image has color components, a JP2 packet contains one color component.

All JP2 packets are usually decoded to reconstruct an image as well as other coding technologies. In addition, images that differ from the usually decoded image can be reconstructed by controlling the number of JP2 packets to be decoded, and this feature is *scalability*. Several scalabilities such as quality scalability served by layers and resolution scalability are based on hierarchy in which less important data are subordinate to more important data. That is, decoding subordinate data without decoding superordinate data is meaningless in a *hierarchical scalability*.

2.2 Hierarchical Encryption for JP2

The conventional scheme [7] subordinately generates keys from a single master key and controls access for a JP2 codestream along all hierarchical scalabilities. Now, a JP2 codestream of a grayscale image is assumed to be composed of L layers and R resolution levels. Figure 2 shows a codestream with 12 JP2 packets from $P^{\mathrm{l,r}}_{0,0}$ to $P^{\mathrm{l,r}}_{2,3}$ under conditions that $L = 3$ and $R = 4$.

Figure 3 shows that this scheme divides $K^{\mathrm{l,r}}_{L-1,R-1}$ into two partial keys of equal length. Each partial key is allocated

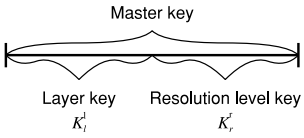


Fig. 3 Master key divided into two partial keys [7].

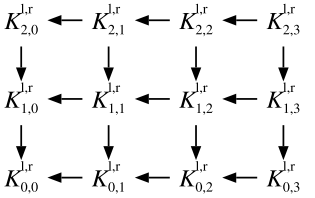


Fig. 4 Order of generating keys [7].

to each hierarchical scalability, and a key for a JP2 packet is subordinately generated from the previously generated key. Partial keys for hierarchy of layers, K^{l}_{l}'s, are generated by

$$K^{\mathrm{l}}_{l} = H^{L-1-l}\left(K^{\mathrm{l}}_{L-1}\right) = H\left(H^{L-1-l-1}\left(K^{\mathrm{l}}_{L-1}\right)\right), \quad l = L-2, \ldots, 1, 0, \tag{1}$$

where $H(\cdot)$ is an one way hash function [14] and $H^0(\cdot)$ output the input as it is. Partial keys for hierarchy of resolution levels are similarly generated by

$$K^{\mathrm{r}}_{r} = H^{R-1-r}\left(K^{\mathrm{r}}_{R-1}\right), \qquad r = R-2, \ldots, 1, 0. \tag{2}$$

For the JP2 codestream shown in Fig. 2, the order of generating keys is summarized as Fig. 4.

Partial keys K^{l}_{l} and K^{r}_{r} are combined to form key $K^{\mathrm{l,r}}_{l,r}$ that corresponds to JP2 packet $P^{\mathrm{l,r}}_{l,r}$. Packet $P^{\mathrm{l,r}}_{l,r}$ is encrypted using key $K^{\mathrm{l,r}}_{l,r}$, where $l = \{0, 1, \ldots, L-1\}$ and $r = \{0, 1, \ldots, R-1\}$. Encrypted JP2 codestreams are distributed to users. Users who receive key $K^{\mathrm{l,r}}_{L-1,R-1}$ are permitted to access the fully decrypted image, whereas users who receive $K^{\mathrm{l,r}}_{0,0}$ are able to access the image having the least quality. This scheme is easily extended to three or more scalabilities, including color components, by dividing the master key into multiple partial keys.

2.3 Limitation of Conventional Scheme

Application and conditions of the conventional scheme [7] are the following.

- The target medium is an image (JP2 coded).
- One content is equal to one image.
- At least one JP2 packet has to be decrypted.

On the other hand, composite multimedia contents have the following characteristics.

- Media other than just images simultaneously exist in one content.
- Simultaneous access control to multiple images has to be considered.

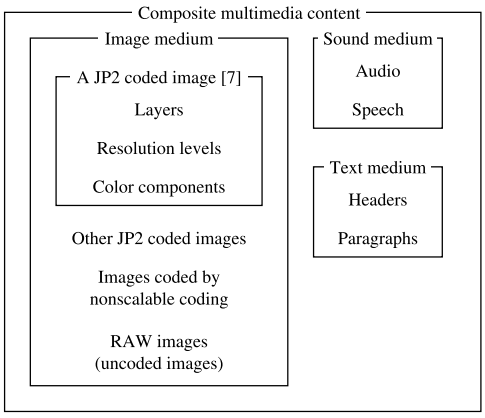


Fig. 5 Application and conditions for the access controlling of composite multimedia contents.

- All entities in one particular medium remain encrypted, whereas several entities in other media are decrypted.

As shown in Fig. 5, one composite multimedia content consists of several media. Furthermore, several entities exists in each medium and each entities may be uncoded or coded without scalabilities. Since the conventional scheme [7] controls only one JP2 coded image, the kind of medium and the number of entities are restricted.

In addition, because of the design of hierarchical scalabilities in JP2 coding, one JP2 packet belong to a layer and simultaneously to a resolution level. That is, it cannot decrypt a JP2 packet based on layer scalability but not based on resolution scalability, though medium based access control is desired for composite multimedia contents.

Therefore, expansion of the conventional scheme [7] for controlling access to composite multimedia contents by dealing with media rather than scalabilities does not work well. Since above mentioned problems are essential for access controlling of composite multimedia contents, novel and unique solutions are desired.

In the next section, a hierarchical encryption scheme is proposed for controlling access to composite multimedia contents. The proposed scheme fits composite multimedia contents and simultaneously keeps the advantages of the conventional scheme described in this section by overcoming above mentioned problems with simple solutions.

3. Proposed Scheme [12], [13]

Composite multimedia content consists of several media which several entities furthermore belong to a medium. Here, a content assumed to consist of P text paragraphs, I images, and M music. A paragraph and a sound file are entities in text and sound media, respectively, and these entities are units for access control. Whereas, in image medium, each component in an image scalable-encoded is an unit for access control. If all images are encoded by a non scalable coding technology rather than scalable coding technologies, an image file is a unit for access control.

The proposed scheme introduces two new concepts,

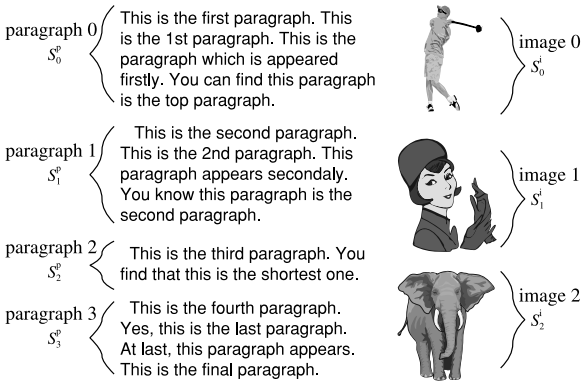


Fig. 6 A multimedia content consisting of four text paragraphs and three images ($P = 4, I = 3$, and $M = 0$).

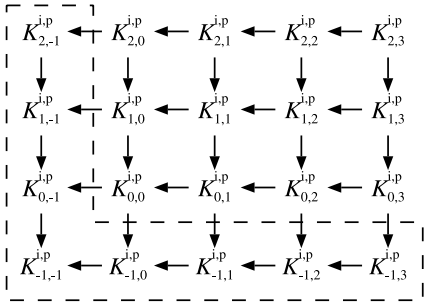


Fig. 7 Order of generating keys for keeping all objects in a particular medium encrypted (keys in the L-shaped box with dashed line are unusable keys).

namely *unusable keys* and *numbering keys*. Unusable keys realize that all entities in one particular medium remain encrypted and simultaneously several objects in other media are decrypted. Otherwise, a numbering key offers control of the number of images to be accessed. Although this paper describes these keys separately, these keys are able to cooperate with each other.

It is noted that this scheme assumes a hierarchy exists in a medium. Here, "hierarchy" includes not only those for scalabilities in JP2 coded images but also so to say semantic hierarchies. In the text medium, the appearing order of paragraphs has its own meaning, and it is referred to as a *semantic* hierarchy here. The proposed scheme, therefore, does not require entities themselves coded by scalable coding technologies.

3.1 Unusable Keys

Consider the composite multimedia content shown in Fig. 6 that consists of four text paragraphs and three images, i.e., $P = 4, I = 3$, and $M = 0$. To support that no entity is decrypted in one particular medium, this scheme generates keys $K^{\mathrm{i,p}}_{i,p}$'s ($i = -1, 0, \ldots, I-1$, $p = -1, 0, \ldots, P-1$) using the process outlined in Fig. 7.

More definitively, master key $K^{\mathrm{i,p}}_{I-1,P-1}$ is split into two partial keys, in which the former is for images and the latter

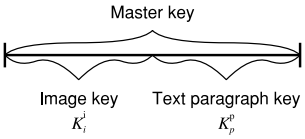


Fig. 8 The master key for a multimedia content shown in Fig. 6.

is for text paragraphs as shown in Fig. 8. Partial key K_i^{i} for image S_i^{i} is subordinately generated by

$$K_i^{\mathrm{i}} = H^{I-1-i}\left(K_{I-1}^{\mathrm{i}}\right), \qquad i = I-2, \ldots, 1, 0, -1, \tag{3}$$

and for text paragraph S_p^{p}, key K_p^{p} is similarly generated by

$$K_p^{\mathrm{p}} = H^{P-1-p}\left(K_{P-1}^{\mathrm{p}}\right), \qquad p = P-2, \ldots, 1, 0, -1. \tag{4}$$

No image is encrypted with K_{-1}^{i}, and K_{-1}^{p} does not correspond to any paragraph. These partial keys are referred to as *unusable keys*. For the composite multimedia content shown in Fig. 6, an user who receives $K_{-1,3}^{\mathrm{i,\,p}}$ is permitted to access all four paragraphs but is not permitted to access any images. On the other hand, $K_{1,-1}^{\mathrm{i,\,p}}$ allows an user to access two of the three images but does not allow access to the text paragraphs. The proposed scheme, thus, offers versatile access control based on media as well as versatile access control in a medium.

3.2 Numbering Keys

A numbering key is quite simple but highly effective. Consider I images, each of which consists of L layers and R resolution levels. Figure 9 shows an example in which $I = 2$, $L = 3$, and $R = 4$.

To support that multiple images with scalabilities, the proposed scheme generates key $K_{i,l,r}^{\mathrm{i,\,l,\,r}}$ ($i = 0, 1, \ldots, I-1$, $l = 0, 1, \ldots, L-1$, $r = 0, 1, \ldots, R-1$) for JP2 packet $P_{i,l,r}^{\mathrm{i,\,l,\,r}}$ by the rule shown in Fig. 10. To comply with Fig. 10, master key $K_{I-1,L-1,R-1}^{\mathrm{i,\,l,\,r}}$ is split into three partial keys as shown in Fig. 11; The first part, K_i^{i}, the second part, K_l^{l}, and the third part, K_r^{r}, are for images themselves, layers in images, and resolution levels in images, respectively. Keys K_i^{i}, K_l^{l}, and K_r^{r} are subordinately generated by Eqs. (1), (2), and (3), respectively.

For the codestreams shown in Fig. 9, $K_{1,2,1}^{\mathrm{i,\,l,\,r}}$ allows an user to obtain all two images with all three layers and two lower resolution levels. An user who receives $K_{0,2,3}^{\mathrm{i,\,l,\,r}}$ is permitted to access the fully decoded first image. This scheme, thus, is applicable to multiple images having hierarchical scalabilities.

3.3 Key Length and Running Costs

In practical use, the costs to manage and deliver keys are important. If it gives security preference, storage and transmission costs of keys increases. Whereas, reducing storage and transmission of keys makes the system insecure. Therefore,

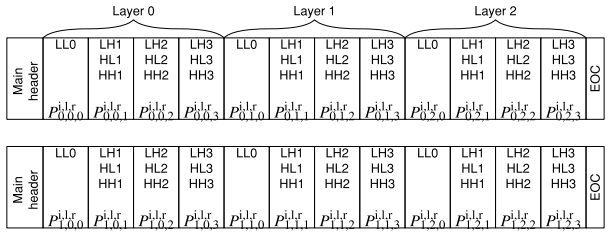


Fig. 9 An example of multiple images having hierarchical scalabilities (two images having three layers and four resolution levels, $I = 2$, $L = 3$, and $R = 4$).

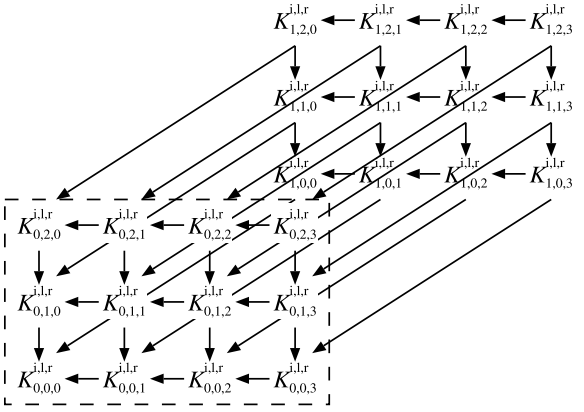


Fig. 10 Order of generating keys for supporting multiple images having scalabilities (keys in the box with dashed line are numbering keys).

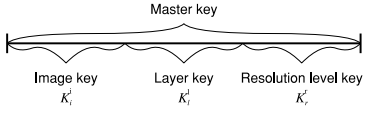


Fig. 11 The master key for multiple images shown in Fig. 9.

in this section, the total length (number) of keys required in the proposed scheme is simply analyzed for estimation of costs. In this paper, the analysis covers wider range of composite multimedia contents than Ref. [13]. That is, this paper gives an analysis more general and precise than it.

Since all entities in all the media are independently encrypted in a straightforward approach that is similar to the conventional scheme for JP2 images [3], a number of keys are requested to be managed and delivered to an user for enabling versatile access control. In contrast, the proposed scheme has only one master key and delivers only one key to an user who is permitted to access composite multimedia content. This advantage of the proposed scheme improves security and reduces costs in key management and delivery.

Consider composite multimedia content with P text paragraph, I images, and M music. Furthermore, an image consists of L layers and R resolution levels. The proposed scheme manages and delivers AN bytes-long key to enable versatile access control under the condition where each partial key is N bytes long, where

$$A = \sum_{k \in P,I,M} f(k), \tag{5}$$

$$f(P) = \begin{cases} 0, & P = 0 \\ 1, & P \geq 1 \end{cases}, \tag{6}$$

$$f(I) = \begin{cases} 0, & I = 0 \\ 1, & I = 1, L = 1, R = 1 \\ & \text{or } I \geq 2, L = 1, R = 1 \\ & \text{or } I = 1, L \geq 2, R = 1 \\ & \text{or } I = 1, L = 1, R \geq 2 \\ 2, & I = 1, L \geq 2, R \geq 2 \\ & \text{or } I \geq 2, L = 1, R \geq 2 \\ & \text{or } I \geq 2, L \geq 2, R = 1 \\ 3, & I \geq 2, L \geq 2, R \geq 2 \end{cases}, \tag{7}$$

$$f(M) = \begin{cases} 0, & M = 0 \\ 1, & M \geq 1 \end{cases}. \tag{8}$$

It is noted that $0 \leq A \leq 5$ in this explanation. In contrast, the ordinary approach has to deal with $(P + ILR + M)$ of Q bytes-long keys for the composite multimedia content. An user, thus, receives a concatenated key with $(P + ILR + M)Q$ bytes long in the ordinary approach.

If the length of key Q and partial key N are equal, i.e., $Q = N$, the total length of a key to be delivered to an user in the ordinary way is

$$\frac{P + ILR + M}{A} \tag{9}$$

times larger than that of the proposed scheme. In particular, the sum of images, layers, and resolution levels strongly affect the total length of a key in the ordinary way. Figure 12 shows the total length of a key versus the sum of entities. The proposed scheme suppress the total length of a key to be delivered to an user, whereas the ordinary way increases the length of a key according to the sum of entities.

On the other hand, under the condition where the total amount of managed key for the proposed and ordinary schemes are equal, i.e.,

$$(P + ILR + M)Q = AN, \tag{10}$$

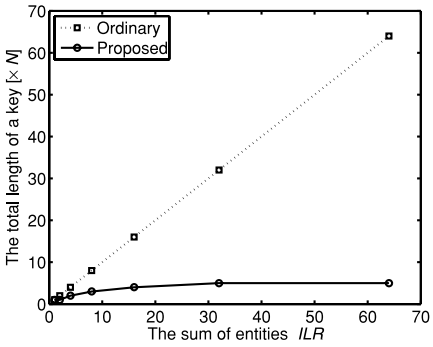


Fig. 12 The total length of a key to be delivered to an user versus the sum of image-related entities.

it is found that

$$N = \frac{P + ILR + M}{A} Q. \tag{11}$$

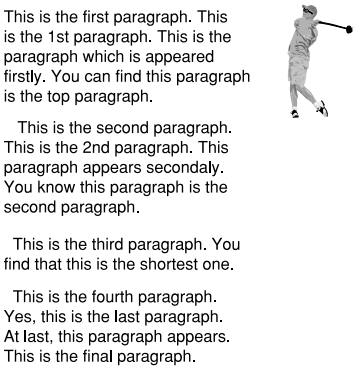
The proposed scheme is able to increase the length of each partial key, N, as mentioned in Eq. (11), and this improves the security of the proposed scheme.

4. Simulation

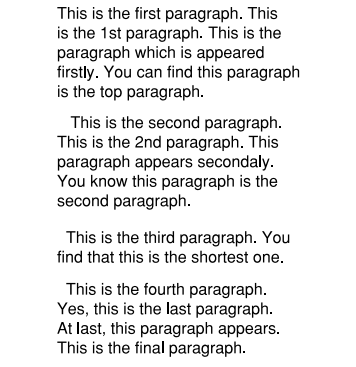
Encrypted entities in each medium are not shown and encrypted components in JP2 coded images are not decoded in this section. Any arbitrary one way hash function and any arbitrary encryption algorithm are used in the proposed scheme, this paper uses SHA-256 [15] and Blowfish [16], respectively.

4.1 Unusable Key

Consider an user who is permitted to access all text paragraphs but who is not permitted to access any images in the multimedia content shown in Fig. 6. Direct application of the conventional scheme [7] in this example would see that the user receives key $K_{0,3}^{\mathrm{i,p}}$ and accesses all the text paragraphs and image $\mathrm{S}_0^{\mathrm{i}}$ as shown in Fig. 13(a). In contrast, the proposed scheme that uses unusable keys is able to precisely



(a) By the conventional scheme [7]. One image is decrypted, though it is desired to be encrypted.



(b) By the proposed scheme. No image is decrypted.

Fig. 13 An example of access control to the composite multimedia content shown in Fig. 6. All text paragraphs are accessible and all images are desired to be encrypted.

(a) Lena (b) Barbara

Fig. 14 Obtained images by the proposed scheme (two images with three layers and four resolution levels, $I = 2$, $L = 3$, and $R = 4$, and two resolution levels over all layers in both images are obtained).

control the user's access by sending key $K^{\mathrm{i,\,p}}_{-1,3}$ to the user, as shown in Fig. 13(b).

4.2 Numbering Keys

Two 512×512-sized 8-bits quantized grayscale images "Lena" and "Barbara," were losslessly compressed using JP2 encoder of Kakadu [17] under conditions of three layers and four resolution levels, i.e., $I = 2$, $L = 3$, and $R = 4$, and two codestreams are encrypted by the proposed scheme. By receiving only one key, $K^{\mathrm{i,\,l,\,r}}_{1,2,1}$, JP2 packets $P^{\mathrm{i,\,l,\,r}}_{i,l,r}$'s, where $i = 0, 1$, $l = 0, 1, 2, 3$, and $r = 0, 1$ are simultaneously decrypted. The obtained two images that are half sized images of the original images are shown in Fig. 14.

However, when the conventional scheme [7] is applied to this example, two keys are required for the two images. The more images exist, the more keys have to be managed and delivered.

5. Conclusions

A hierarchical encryption scheme has been proposed for composite multimedia contents that enables versatile access control. The proposed scheme has the only one master key and delivers one key to an user. This scheme can keep all the entities in a particular medium encrypted and simultaneously decrypt several entities in other media by using unusable keys. Moreover, the scheme supports multiple images with scalabilities by numbering keys.

Further work include considering resilience to collusion attacks in which several malicious users generate a new key from those own keys to access further entities.

References

[1] B.B. Zhu, M.D. Swanson, and S. Li, "Encryption and authentication for scalable multimedia: Current state of the art and challenges," Proc. SPIE Int. Sympo. Inf. Technology & Commun., vol.5601, pp.157–170, Philadelphia, PA, US, Oct. 2004.
[2] H.L. Jin, M. Fujiyoshi, Y. Seki, and H. Kiya, "A data hiding method for JPEG 2000 coded images using modulo arithmetic," IEICE Trans. Fundamentals (Japanese Edition), vol.J89-A, no.3, pp.234–242, March 2006.
[3] H. Kiya, S. Imaizumi, and O. Watanabe, "Partial-scrambling of JPEG2000 images without generating marker codes," IEICE Trans. Inf. & Syst. (Japanese Edition), vol.J86-D-II, no.11, pp.1628–1636, Nov. 2003.
[4] C. Peng, R.H. Deng, Y. Wu, and W.-Z. Shao, "A flexible and scalable authentication scheme for JPEG2000 image codestreams," Proc. ACM Multimedia Conf., pp.433–441, Berkeley, CA, US, Nov. 2003.
[5] H.H. Yu, "Scalable encryption for multimedia content access control," Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Process., pp.417–420, Hong Kong, PRC, April 2003.
[6] B.B. Zhu, C. Yuan, Y. Wang, and S. Li, "Scalable protection for MPEG-4 fine granularity scalability," IEEE Trans. Multimed., vol.7, no.2, pp.222–233, April 2005.
[7] S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized hierarchical encryption of JPEG 2000 codestreams for access control," Proc. IEEE Int. Conf. Image Process., pp.II-1094–II-1097, DVD-ROM, Genoa, Italy, Sept. 2005.
[8] D. Mukherjee and M. van der Schaar, "Compact dependent key generation methods for encryption-based subscription differentiation for scalable bit-streams," Proc. IEEE Int. Conf. Image Process., pp.II-1114–II-1117, DVD-ROM, Genoa, Italy, Sept. 2005.
[9] Information technology—JPEG 2000 image coding system—Part 1: Core coding system. Int. Std. ISO/IEC IS-15444-1, Dec. 2000.
[10] D.S. Taubman and M.W. Marcellin, JPEG2000—Image Compression Fundamentals, Standards and Practice, Kluwer Academic Publishers, Boston, 2001.
[11] Streaming Video Profiles (FGS), ISO/IEC 14496-2/FDAM 4, 2001.
[12] W. Saitou, M. Fujiyoshi, and H. Kiya, "Encryption of hierarchical multimedia contents for access control," ITE Technical Report, ME2006-78, pp.37–40, Feb. 2006.
[13] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," Proc. IEEE Int. Conf. Image Process., pp.1977–1980, Atlanta, GA, US, Oct. 2006.
[14] B. Schneier, Applied Cryptography—Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, New York, 1996.
[15] "Secure hash standard," US National Institute of Science and Technology, Federal Information Processing Standard 180-2, Aug. 2002.
[16] B. Schneier, "Description of a new variable-length key, 64-bit block cipher," Proc. Int. Workshop Fast Software Encryption, pp.191–204, Cambridge, UK, Feb. 1996.
[17] Kakadu Software, "A comprehensive framework for JPEG2000," http://www.kakadusoftware.com/

Masaaki Fujiyoshi received his B.Arts, M.Eng., and Ph.D. degrees from Saitama University, Japan in 1995, 1997, and 2001, respectively. In 2001, he joined Tokyo Metropolitan University, Japan, where he is currently a Research Associate of Information and Communication Systems Engineering, Faculty of System Design. His research interests include image processing, secure communications, and spread spectrum communications. Dr. Fujiyoshi serves as an Associate Editor for the Special Section on Selected Papers from the 19th Workshop on Circuits and Systems in Karuizawa of the IEICE Trans. Fundamentals. He has also served as an Associate Editor for the J. IEICE from 2005. He is a Member of the ITE (Institute of Image Information and Television Engineers, Japan) and the IEEE. He received the Young Engineer Award from the IEICE in 2001.

Shoko Imaizumi received her B.Eng. and M.Eng. degrees from Tokyo Metropolitan University, Japan in 2002 and 2005, respectively. From 2003 to 2005, she was with the Ministry of Education, Culture, Sports, Science and Technology of Japan. Since 2005, she has been with the Industrial Research Institute of Niigata Prefecture, Japan. Since 2006, she has been also a Ph.D. candidate at Tokyo Metropolitan University. Her research interests include image processing and security for multimedia. She is a Student Member of the ITE (Institute of Image Information and Television Engineers, Japan).

Hitoshi Kiya received his B.E. and M.E. degrees from Nagaoka University of Technology, Japan in 1980 and 1982, respectively, and his D.E. degree from Tokyo Metropolitan University, Japan in 1987. In 1982, he joined Tokyo Metropolitan University, where he is currently a Professor of Information and Communication Systems Engineering, Faculty of System Design. He was a Visiting Fellow at the University of Sydney, Australia from Oct. 1995 to March 1996. His research interests include digital signal processing, multirate systems, adaptive filtering, image processing, and security for multimedia. Prof. Kiya served as an Associate Editor for the IEICE Trans. Fundamentals (Japanese Edition) and the IEEE Trans. Signal Processing from 1998 to 2002 and from 1998 to 2000, respectively. He served as the Guest Editor for the Special Sections on Papers Selected from ITC-CSCC 2005 and on VLSI for Digital Signal Processing of the IEICE Trans. Fundamentals. He has been a vice chair of the Signal Processing Committee of the IEICE and the chair of the Media Engineering Committee of the ITE (Institute of Image Information and Television Engineers, Japan) from 2005. He is a Member of the ITE and the IIEEJ (Institute of Image Electronics Engineers of Japan), and a Senior Member of the IEEE.