Efficient Collusion Attack-Free Access Control for JPEG 2000 Coded Images

Shoko IMAIZUMI*†, Masaaki FUJIYOSHI†, and Hitoshi KIYA†
*Industrial Research Institute of Niigata Prefecture, Niigata, Niigata 950–0915, Japan
†Dept. of Information and Communication Systems Eng., Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan
Email: shoko.imaizumi@m.ieice.org, mfujiyoshi@m.ieice.org, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes an efficient access control method for JPEG 2000 coded images with multiple dimensions of hierarchical scalability. An access control method is required to 1) be resilient to collusion attack and 2) manages less number keys from the perspective of the key management cost. The proposed method is resilient to collusion attack and manages only one key. Moreover, the proposed method reduces the length of managed key in comparison with the conventional methods satisfying above two requirements. This feature serves an efficient key management.**

I. Introduction

As a huge variety of communication channels and terminals exist, *scalable* transmission becomes popular in which a lower quality content is displayed by decompression of a certain portion from the head of the compressed codestream. To protect scalable compressed images, *scalable access control* has been studied [1]–[9]. Security for JPEG 2000 (JP2) [10] is emphasized in JPEG 2000 Part8 [9], and JP2 coded images must be secured closely. This paper proposes a novel access control to multidimensionally scalable JP2 coded image in which several kinds of scalability exist.

Three conventional methods [6]–[8] controlling access to multidimensional scalable coded JP2 images are focused here. The first method [7] controls access in one dimension, so many codestreams and keys have to be managed. The second one [6] manages single codestream and single key, but it is vulnerable to collusion attacks. The last [8] manages single codestream and single key, and it becomes resistant to collusion attacks by adding extra partial keys to the managed key.

This paper proposes an access control method that improves the conventional method [8]. The proposed method takes account into collusion attack and key generation order in the managed key generation, and this reduces the number of partial keys in comparisons with the conventional method [8]. This feature serves an efficient key management.

II. JP2 Codestream and Access Control

This section briefly describes JP2 codestream structure [10], scalable access control for JP2. It further describes the requirement for hierarchical access control methods by introducing two conventional methods [7], [8].

A. JP2 Codestream

Fig. 1 outlines a JP2 codestream using YC_bC_r as the color space. JP2 supports five different *progression order*s that are

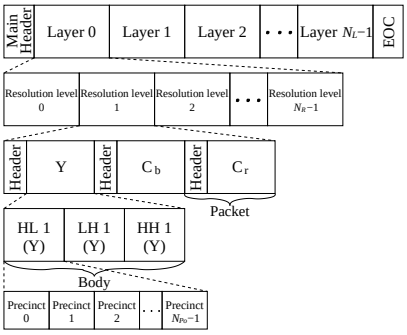
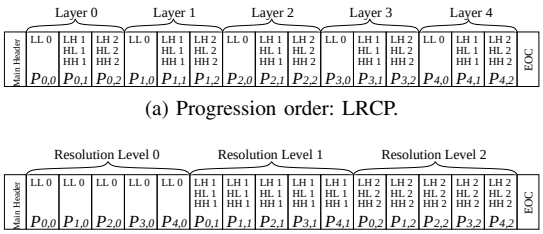


Fig. 1. JP2 codestream with color components, Y, C_b, and C_r.



(a) Progression order: LRCP.

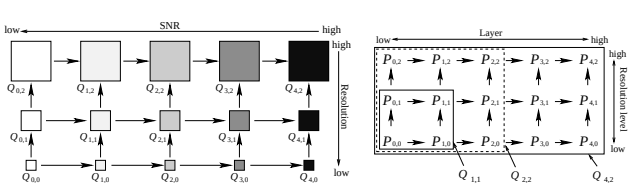
(b) Progression order: RLCP.

Fig. 2. Ordered JP2 packets in a grayscale image: $N_L = 5$ and $N_R = 3$.

orders of scalability dimensions, and the default order, that is also used in Fig. 1, is LRCP (Layer-Resolution-Component-Position). It is primarily progressive by quality.

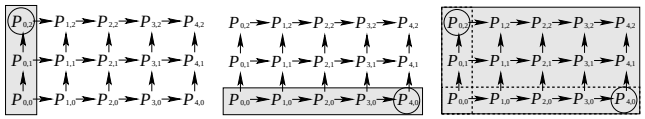
Layers are in order of SNR in which each layer is composed of data for resolution levels. If the original image has color components, each resolution level has Y, C_b, and C_r components. Resolution level zero only contains the LL data, whereas the other levels contain three subbands; HL, LH, and HH. These subbands have precincts that have non-hierarchically positional information. Thus, a color JP2 codestream has three dimensions of hierarchical scalability; layer, resolution revel, and components ($\alpha = 3$), whereas a grayscale one has two; layer and resolution level ($\alpha = 2$). Each JP2 packet is composed of a header and a body and contains partial data for each subband.

Fig. 2 lists examples of JP2 codestreams with LRCP and RLCP progression orders. Both have five layers and three resolution levels, which are represented as $N_L = 5$ and $N_R = 3$, respectively, in this paper. Hereafter, $P_{l,r}$ is the JP2 packet at the l-th layer and r-th resolution level.



(a) Quality at $Q_{l,r}$. (b) Decompression to $P_{l,r}$.

Fig. 3. Hierarchical decompression of a grayscale image: $N_L = 5$ and $N_R = 3$.



(a) Packets legally deciphered by Alice. (b) Packets legally deciphered by Bob. (c) Packets deciphered by collusion attack.

Fig. 4. Alice and Bob's collusion attack in the vulnerable method [6] (the shaded are deciphered).

B. Hierarchically Scalable Access Control

Fig. 3 outlines an example of scalable decoding in which different image products are obtained by decompression in many ways, where $\alpha = 2$, $N_L = 5$, and $N_R = 3$. It is noted that this representation holds regardless of progression orders. The original image is compressed at quality $Q_{4,2}$, and the image at $Q_{4,2}$ is obtained by decompressing all packets. To produce the image at $Q_{1,1}$, four packets $P_{0,0}$, $P_{0,1}$, $P_{1,0}$, and $P_{1,1}$ are decompressed. To serve a versatile access control in terms of quality, resolution, and so on, a scalable access control method for JP2 should encipher a JP2 codestream packet-by-packet using $N_L \times N_R$ different keys. Though the electronic codebook mode is used for inter-packet encipherment, any mode is applicable to intra-packet encipherment. The proposed method enciphers the packet body but does not encipher the packet headers.

C. Requirements

This section describes three requirements for hierarchical access control for JP2 coded images, i.e., collusion attack-resilience, the less number of managed keys, and the shorter length of managed keys.

1) Collusion Attack-Resilience: A *collusion attack* is made by multiple users to obtain an image with higher quality than those allowed, and the conventional method [6] allows users to collude. In Fig. 4 (a), Alice is allowed to access the image at $Q_{0,2}$ and receives key $K_{0,2}$ to decipher $P_{0,2}$, $P_{0,1}$, and $P_{0,0}$. Whereas, Bob, in Fig. 4 (b), has $K_{4,0}$ to decipher $P_{4,0}$, $P_{3,0}$, $P_{2,0}$, $P_{1,0}$, and $P_{0,0}$ for access the image at $Q_{4,0}$. In this method, they are possible to illegally generate $K_{4,2}$, so they can decipher all packets as shown in Fig. 4 (c) and access the image at $Q_{4,2}$. The proposed method is resistant to collusion attack.

2) The Less Number of Managed Keys: Though a hierarchical access control method requires $N_L \times N_R$ of keys as mentioned in Sect. II-B, two methods that manage less keys and subordinately generate $N_L \times N_R$ keys from the managed keys have been proposed [7], [8].

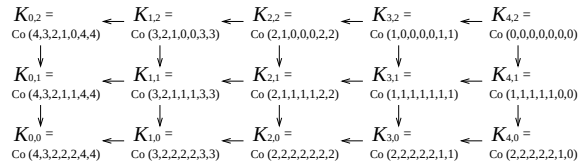


Fig. 5. The key generation order in Method II [8]. Co is a key concatenating function.

The former method [7] controls access to JP2 codestreams according to the hierarchy in the prior scalability. This method, Method I hereafter, subordinately generates keys for $P_{l,r}$ from the managed key, *master key*, by a one-way hash function. It, thus, requires five master keys and five codestreams for five progression orders. The number of master keys in Method I, $N_{\mathrm{MK,I}}$, is

$$N_{\mathrm{MK,I}} = 5. \tag{1}$$

The latter method [8], Method II hereafter, simultaneously controls access in every dimensions of hierarchical scalability with a single codestream. The number of master keys in Method II, $N_{\mathrm{MK,II}}$, is

$$N_{\mathrm{MK,II}} = 1. \tag{2}$$

Method II reduces the number of master keys and managed codestreams to 1/5 from Method I. The proposed method have the same features as Method II.

3) The Less Length of Managed Keys: This paper assumes that the length of $N_L \times N_R$ keys are the same, as in the conventional methods. A key in the proposed method consists of partial keys as Method II [8]. The length of a key affects encipher strength and the key management cost and is determined by multiplying the number of partial keys and the length of a partial key.

Method II introduces the partial key concept to offer hierarchical access control with single managed codestream. Fig. 5 shows the concept of the key generation order in this method, where $\alpha = 2$, $N_L = 5$, and $N_R = 3$. In Fig. 5, $K_{l,r}$ is the key for packet $P_{l,r}$ and consists of seven partial keys. The number of partial keys in Method II, $N_{\mathrm{PK,II}}$, depends on N_L and N_R as

$$N_{\mathrm{PK,II}} = N_L + N_R - 1. \tag{3}$$

Under the condition that the length of a partial key is V [bits], the total length of master keys in Method II, $L_{\mathrm{MK,II}}$, is

$$L_{\mathrm{MK,II}} = N_{\mathrm{MK,II}} \times N_{\mathrm{PK,II}} \times V = (N_L + N_R - 1)V \ [\mathrm{bits}]. \tag{4}$$

Since Method I does not have the partial key concept, the number of partial keys in Method I, $N_{\mathrm{PK,I}}$, is

$$N_{\mathrm{PK,I}} = 1, \tag{5}$$

and the total length of master keys in Method I, $L_{\mathrm{MK,I}}$, is

$$L_{\mathrm{MK,I}} = N_{\mathrm{MK,I}} \times N_{\mathrm{PK,I}} \times V = 5V \ [\mathrm{bits}]. \tag{6}$$

The total length of master keys is determined by the length of a partial key, the number of partial keys, and the used one-way hash function. Moreover, the number of partial keys affects the number of the usage of the hash function.

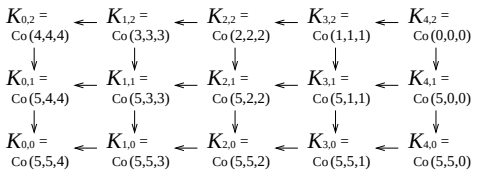


Fig. 6. Key generation order in the proposed method for a JP2 coded image having five layers and three resolution levels. $K_{l,r}$ is the key for packet $P_{l,r}$. Co is a concatenating function.

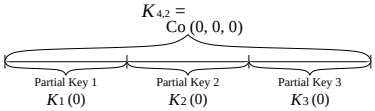


Fig. 7. The master key in the proposed method is divided to three partial master keys for a JP2 coded image having five layers and three resolution levels.

III. Proposed Method

This section proposes a method for access control to JP2 coded images that reduces the total length of master keys from Method II [8]. The proposed method simultaneously controls access in every dimensions of hierarchical scalability with single master key and single managed codestream. The proposed method is resistant to collusion attack as Method II.

A. Key Generation and Codestream Encipherment

As an example of content for explanation, the JP2 codestream with two-dimensional scalability ($\alpha = 2$) shown in Fig. 2 is used, where it is composed of five layers ($N_L = 5$) and three resolution levels ($N_R = 3$). The proposed method controls access regardless of progression orders.

Fig. 6 shows the outline of totally new key generation order, where $K_{l,r}$ is the key for packet $P_{l,r}$. This order is resilient to collusion attacks, and the assignment method of three partial keys is described hereinafter. By using the representation that the minimum depth of hierarchy of two scalability as

$$N_{\min} = \min(N_L, N_R), \tag{7}$$

this method divides the master key, $K_{4,2}$, to $N_{\min}$ of partial master keys; $K_1(0)$, $K_2(0)$, and $K_3(0)$ as shown in Fig. 7.

From these partial master keys, partial keys are subordinately generated as

$$K_1(i_1+1) = H(K_1(i_1)), \qquad i_1 = 0,1,\ldots,4, \tag{8}$$
$$K_2(i_2+1) = H(K_2(i_2)), \qquad i_2 = 0,1,\ldots,4, \tag{9}$$
$$K_3(i_3+1) = H(K_3(i_3)), \qquad i_3 = 0,1,\ldots,3, \tag{10}$$

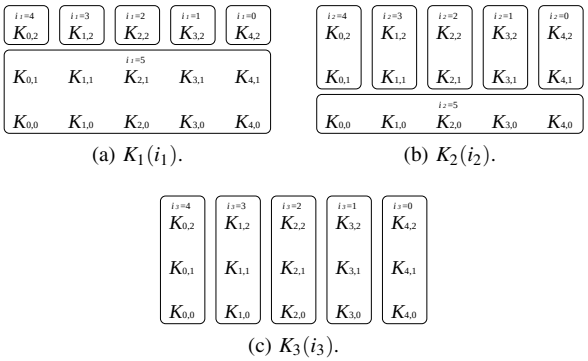
where $H(\cdot)$ is a one-way hash function. These partial keys are assigned to keys according to Fig. 8. Key $K_{l,r}$ is formed by concatenating three partial keys that are assigned to $K_{l,r}$ as

$$K_{l,r} = \mathrm{Comb}(K_1(i_1), K_2(i_2), K_3(i_3)), \tag{11}$$

where Comb is any arbitrary function concatenating partial keys and is represented as

$$\mathrm{Co}(i_1,i_2,i_3) = \mathrm{Comb}(K_1(i_1), K_2(i_2), K_3(i_3)) \tag{12}$$

in Fig. 6. The length of $K_{l,r}$ in Fig. 6 is $3V$ [bits] under the condition that the length of a partial key is V [bits].



(a) $K_1(i_1)$. (b) $K_2(i_2)$.

(c) $K_3(i_3)$.

Fig. 8. Partial key assignment to keys in the proposed method. A partial key is assigned to all keys in the square.

TABLE I
The number of and the total length of master keys among the three methods. The length of a partial master key: V [bits].

	Method I [7]	Method II [8]	Method III (Proposed)
N_{MK}	5	1	1
L_{MK} [bits]	$5V$	$(N_L+N_R-1)V$	$N_{\min}V$

With key $K_{l,r}$, the body data of packet $P_{l,r}$ in the JP2 codestream is enciphered, where $l = 0,1,\ldots,N_L-1$ and $r = 0,1,\ldots,N_R-1$. It is noted that any arbitrary symmetric encipher algorithm can be used in the proposed method.

B. Decipherment and decompression of Codestream

Here, it is considered that a user allowed to access the image with quality $Q_{2,2}$, c.f. Fig. 3. The user receives key $K_{2,2}$. Since $K_{2,2}$ consists of $K_1(2)$, $K_2(2)$, and $K_3(2)$ as shown in Figs. 6 and 8, partial keys that the user needs are generated by

$$K_1(i_1+1) = H(K_1(i_1)), \qquad i_1 = 2,3,4, \tag{13}$$
$$K_2(i_2+1) = H(K_2(i_2)), \qquad i_2 = 2,3,4, \tag{14}$$
$$K_3(i_3+1) = H(K_3(i_3)), \qquad i_3 = 2,3. \tag{15}$$

These generated partial keys are assigned to keys according to Fig. 8, and are concatenated by Eq. (11) to form keys.

By using obtained keys $K_{0,0}$, $K_{0,1}$, $K_{0,2}$, $K_{1,0}$, $K_{1,1}$, $K_{1,2}$, $K_{2,0}$, $K_{2,1}$, and $K_{2,2}$, corresponding packets are deciphered and decompressed to present the image at $Q_{2,2}$.

C. Features

This section describes that the proposed method meets three requirements described in Sect. II-C.

1) The Number of and the Total Length of Master Key: Using Eq. (7), the number of partial keys in the proposed method (Method III hereafter), i.e., $N_{\mathrm{PK,III}}$ is

$$N_{\mathrm{PK,III}} = N_{\min}. \tag{16}$$

Under the condition that a partial key is V [bits] long, the total length of master keys in Method III, $L_{\mathrm{MK,III}}$, is

$$L_{\mathrm{MK,III}} = N_{\mathrm{MK,III}} \times N_{\mathrm{PK,III}} \times V = N_{\min}V \ [\mathrm{bits}]. \tag{17}$$

Table I summarizes the number of and the length of master key for Methods I [6], II [8], and III. Method I requires five master keys to handle five progression orders, whereas

Methods II and III manages only one key. Moreover, from Eqs. (3), (7), (16), $N_{\mathrm{PK,III}} \leq N_{\mathrm{PK,II}}$, so the proposed method reduces the total length of the master key from Method II. The proposed method, thus, offers an efficient key management.

It is noted that the proposed method controls access to JP2 images with three dimensional scalability, i.e., $\alpha = 3$, by simply applying the algorithm twice to the image. When N_1, N_2, and N_3 are the depth of hierarchy in scalability of the image in ascending order, $N_{\mathrm{PK,III}}$ only increases up to

$$N_{\mathrm{PK,III}} = N_1 N_2 \tag{18}$$

in the proposed method, whereas Method II reaches

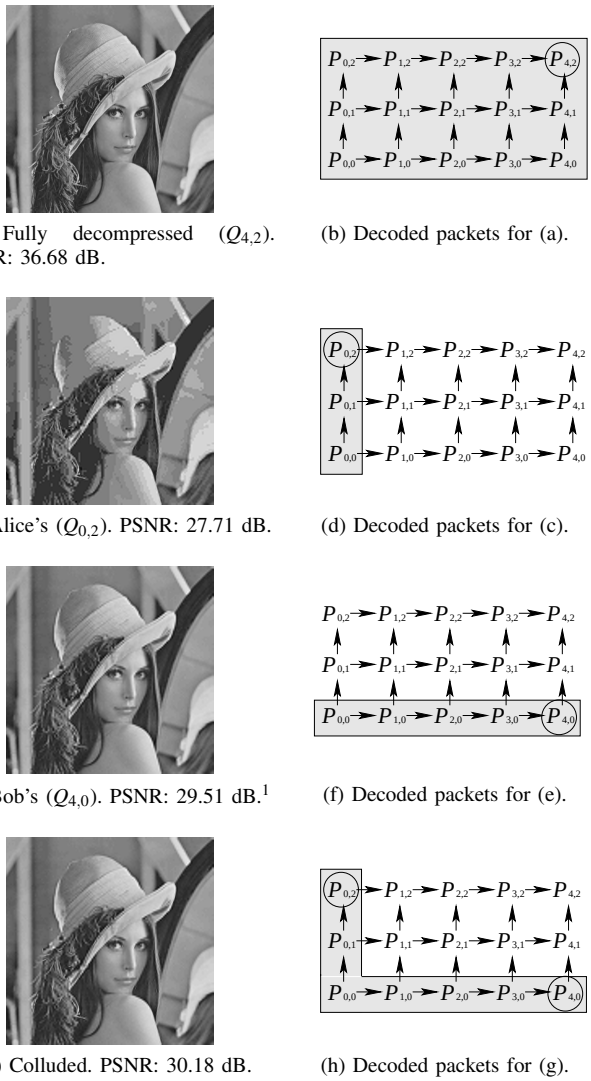
$$N_{\mathrm{PK,II}} = N_1 \left(N_2 + N_3 - 1\right). \tag{19}$$

2) Collusion Attack-Resistance: Alice and Bob appeared in Sect. II-C1 reappear here. Since Alice can access the image at $Q_{0,2}$, she receives key $K_{0,2}$. Bob receives $K_{4,0}$ to access the image at $Q_{4,0}$. In the proposed method, key $K_{0,2}$ is divided to $K_1(4)$, $K_2(4)$, and $K_3(4)$, and they obtain $K_1(5)$, $K_2(5)$, and $K_3(0)$ from key $K_{4,0}$. By using these six partial keys, they obtain only seven valid keys $K_{0,0}$, $K_{0,1}$, $K_{0,2}$, $K_{1,0}$, $K_{2,0}$, $K_{3,0}$, $K_{4,0}$, and these keys are the identical to that obtained legally.

Thus, the proposed method is enough resistant to collusion attacks, though this paper does not explicate all patterns of collusion attack to save the space.

IV. Experimental Results

Grayscale image "lena" is compressed by Kakadu to generate a codestream with five layers ($N_L = 5$) and three resolution levels ($N_R = 3$). The bitrate of a layer is 0.1 bits/pixel, and Fig. 9 (a) shows the fully decompressed image, i.e., at quality $Q_{4,2}$. Alice can access the image with quality $Q_{0,2}$ shown in Fig. 9 (c), and Bob obtains the image shown in Fig. 9 (e) as $Q_{4,0}$. In Method I [7], Method II [8], and the proposed method, Alice and Bob illegally generate the image shown in Fig. 9 (g). Since no illegally deciphered packet contributes the quality of this image, two users do not benefit from the collusion attack. Simulations with other images give similar results.



(a) Fully decompressed ($Q_{4,2}$). PSNR: 36.68 dB. (b) Decoded packets for (a).

(c) Alice's ($Q_{0,2}$). PSNR: 27.71 dB. (d) Decoded packets for (c).

(e) Bob's ($Q_{4,0}$). PSNR: 29.51 dB.[1] (f) Decoded packets for (e).

(g) Colluded. PSNR: 30.18 dB. (h) Decoded packets for (g).

Fig. 9. Image examples. 512×512-sized lena is compressed. Five 0.1 bits/pixel-rate layers ($N_L = 5$) and three resolution levels ($N_R = 3$).

V. Conclusions

This paper has proposed an access control method for JP2 coded images with multidimensionally hierarchical scalability. The proposed method is enough resilient to collusion attack as well as the conventional methods [7], [8], it manages only a single codestream and a single short master key. The proposed method reduces the total length of managed key from the conventional methods, so it offers an efficient key management.

References

[1] D. Xie and C.-C.J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," in *Proc. IEEE ISCAS*, 2005, pp.5533–5536.

[2] Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos, and S. Wee, "Rate-distortion-authentication optimized streaming of authenticated video," *IEEE Trans. Circuits Syst. for Video Technol.*, vol.17, pp.544–557, May 2007.

[3] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," in *Proc. SPIE*, vol.4472, 2001, pp.95–104.

[4] O. Watanabe, A. Nakazaki, and H. Kiya, "A scalable encryption method allowing backward compatibility with JPEG2000 images," in *Proc. IEEE ISCAS*, 2005, pp.6324–6327.

[5] A. Haggag, M. Ghoneim, J. Lu, and T. Yahagi, "Progressive encryption and controlled access scheme for JPEG 2000 encoded images," in *Proc. IEEE ISPACS*, 2006, pp.895–898.

[6] S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized hierarchical encryption of JPEG 2000 codestreams for access control," in *Proc. IEEE ICIP*, 2005, pp.1094–1097.

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

[8] 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*, 2007, pp.II-137–II-140.

[9] ISO/IEC IS 15444-8: "Information technology — JPEG 2000 image coding system: Secure JPEG 2000," 2007.

[10] ISO/IEC IS 15444-1: "Information technology — JPEG 2000 image coding system — Part 1: core coding system," 2004.

[1] Decompression of the LL subband and other subbands filled with zero.