HIERARCHICAL ENCRYPTION USING SHORT ENCRYPTION KEYS FOR SCALABLE ACCESS CONTROL OF JPEG 2000 CODED IMAGES

Noriaki HASHIMOTO[*], *Shoko IMAIZUMI*[†], *Masaaki FUJIYOSHI*[*], *and Hitoshi KIYA*[*]

[*]Dept. of Electronics and Information Engineering, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan
[†]Industrial Research Institute of Niigata Prefecture
1–11–1 AbumiNishi, Chuo-ku, Niigata-shi, Niigata 950–0915, Japan

ABSTRACT

This paper proposes an encryption method that uses short keys to enable hierarchical access controls for JPEG 2000 codestreams. The proposed method provides images of various quality levels that may be different from the quality at encoding, though it uses a single codestream and a single managed key (masterkey). Only one key generated from the masterkey is delivered to a user authorized to access a reserved quality image. This method also stems users' collusion to access superior-quality images. Some conventional methods of this proposed method serve the above features, but those keys are much longer than the proposed method. The proposed method uses the smaller number of partial keys than the conventional methods.

Index Terms— Access control, One-way hash function, Scalability, Collusion attack, Internet

1. INTRODUCTION

Exchanging digital images commercially or non-commercially has become very common because of the growth in network technology. Protecting copyrights and privacy of digital images, whether they are encoded or not, is an important issue because digital images can be easily duplicated and re-distributed. There are three main approaches to protect such digital images, i.e., naïve encryption (encrypting the entire content) [1], digital watermarking [2], and *partial encryption* [3–9]. This paper proposes a method for partial encryption to control access to hierarchical JPEG 2000 (JP2) codestreams.

JP2 [10] has *scalability* functions to serve easy access to subsets of a codestream. So an encryption method for JP2 codestream should be *scalable*, and several *hierarchically* scalable encryption methods with a single managed key for JP2 codestreams exist. The first method [7] scans JP2 packets one-dimensionally to manage a single key, but it needs another key for a codestream with a different *progression order*. The second one [8] actually manages a single key by using a multi-dimensional scan, but it suffers from *collusion attack*. The third [9] overcomes collusion attacks, but its key length bursts according to the hierarchy levels of the scalability functions.

This paper proposes a new encryption method for hierarchically scalable JP2 codestreams to reduce the key length. This method uses a single codestream and manages only one key. It is also resistant to collusion attacks.

2. JP2 CODESTREAM AND CONVENTIONAL ENCRYPTION METHODS FOR ACCESS CONTROL

This section describes the hierarchical structure of a JP2 codestream and the conventional methods of hierarchical encryption [7–9].

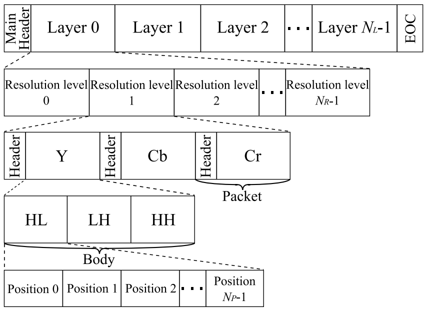


Fig. 1. JP2 codestream with color components, Y, C_b, and C_r.

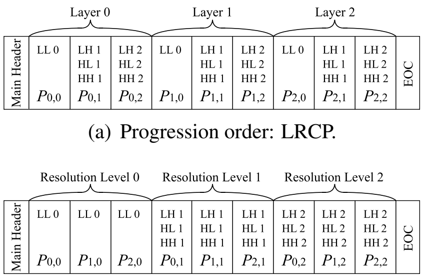
2.1. JP2 codestream [10]

2.1.1. Structure of JP2 Codestream

Fig. 1 outlines a JP2 codestream using YC_bC_r as the color space. Here, scalability functions are put in order of priority called a *progression order*. JP2 has five different orders, and the default order is LRCP (Layer-Resolution level-Component-Position), i.e., the layer scalability function is given the first priority. Each layer is composed of the data for resolution level corresponding to visual significance. If an original image has color components, each resolution level has Y, C_b, and C_r components. Resolution level zero only contains the data of the LL subband, and the other resolution 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 hierarchical scalability functions, whereas a grayscale one has two. Each packet is composed of a header and a body, and a packet contains partial data for each subband. The proposed method encrypts the body but does not encrypt the headers.

2.1.2. Hierarchical Decoding of JP2 Codestream

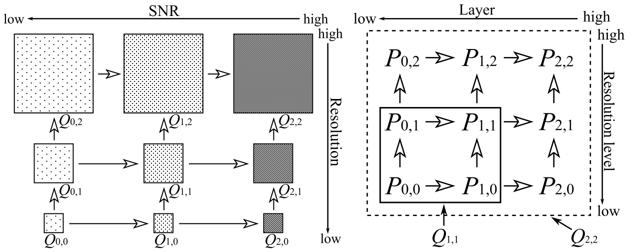
Fig. 2 lists examples of JP2 codestream with LRCP and RLCP orders of progression. Both have three layer and three resolution level hierarchies, which are represented as $N_L = 3$ and $N_R = 3$ in this paper. Hereafter, $P_{l,r}$ represents the JP2 packet at the l-th layer and the r-th resolution level. Fig. 3 outlines an example where a grayscale image is hierarchically decoded. The original image is encoded at quality $Q_{2,2}$, that is $N_L = 3$ and $N_R = 3$. To serve the image at quality $Q_{1,1}$, four packets $P_{1,1}$, $P_{1,0}$, $P_{0,1}$, and $P_{0,0}$ are decoded. Since image data are divided up according to the hierarchy of the scalability functions


Layer 0
Layer 1
Layer 2
Main Header
LL 0
LH 1 HL 1 HH 1
LH 2 HL 2 HH 2
$P_{0,0}$ $P_{0,1}$ $P_{0,2}$ $P_{1,0}$ $P_{1,1}$ $P_{1,2}$ $P_{2,0}$ $P_{2,1}$ $P_{2,2}$
EOC
Resolution Level 0
Resolution Level 1
Resolution Level 2
$P_{0,0}$ $P_{1,0}$ $P_{2,0}$ $P_{0,1}$ $P_{1,1}$ $P_{2,1}$ $P_{0,2}$ $P_{1,2}$ $P_{2,2}$

(a) Progression order: LRCP.

(b) Progression order: RLCP.

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



(a) Decoding at quality $Q_{l,r}$.

(b) Decoding Packets $P_{l,r}$.

Fig. 3. Hierarchical decoding of a grayscale image: $N_L = 3$ and $N_R = 3$. White arrows indicate the decoding order.

as shown in Fig. 2, an encryption method must maintain this hierarchy and decrypt packets according to the required quality.

2.2. Conventional Encryption Methods [7–9]

This section mentions the three conventional methods of JP2 access control [7–9] and their problems.

The collusion attack-resistant one-dimensional scan-based method (method I) [7] generates keys from the single managed key, *masterkey*, but controls access to only one scalability function with a single JP2 codestream. If another scalability function is controlled access, another codestream for which the scalability function is the first priority in the progression order must be prepared. Under the assumption that the length of a JP2 codestream is U and the length of a masterkey is V, the total length of codestream, $L_{C,\mathrm{I}}$, and the total length of masterkeys, $L_{K,\mathrm{I}}$, in this method [7] are

$$L_{C,\mathrm{I}} = 5U, \qquad L_{K,\mathrm{I}} = 5V, \tag{1}$$

respectively, as JP2 has five different progression orders. So one masterkey is determined as a single partial key, though a masterkey is not divided into partial keys actually. Thus the total number of partial keys, $N_{K,\mathrm{I}}$, and the length of a partial key, $L_{P,\mathrm{I}}$, are

$$N_{K,\mathrm{I}} = 5, \tag{2}$$

$$L_{P,\mathrm{I}} = \frac{L_{K,\mathrm{I}}}{N_{K,\mathrm{I}}} = \frac{5V}{5} = V, \tag{3}$$

respectively.

$$\begin{tikzcd}
K_{0,2} \arrow[d] & K_{1,2} \arrow[l] \arrow[d] & K_{2,2} \arrow[l] \arrow[d] \\
K_{0,1} \arrow[d] & K_{1,1} \arrow[l] \arrow[d] & K_{2,1} \arrow[l] \arrow[d] \\
K_{0,0} & K_{1,0} \arrow[l] & K_{2,0} \arrow[l]
\end{tikzcd}$$

Fig. 4. Key-generating order in the collusion attack-vulnerable multi-dimensional scan-based method [8]. Arrows indicate the generating order.

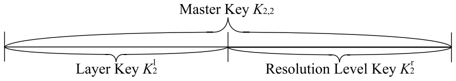


Fig. 5. The masterkey in the collusion attack-vulnerable multi-dimensional scan-based method is divided into two partial keys [8].

Fig. 4 shows key-generating order of the collusion attack-vulnerable multi-dimensional scan-based method [8] in which the encryption key for packet $P_{l,r}$ is $K_{l,r}$. As shown in Fig. 5, the master key, $K_{2,2}$, is divided into the partial masterkey for layer, K_2^{l}, and for resolution level, K_2^{r}. From these partial keys, the other partial keys are generated subordinately, and two partial keys are concatenated to form a key, e.g., K_1^{l} and K_0^{r} form $K_{1,0}$ in Fig. 4. Therefore, as shown in Fig. 6, this method is vulnerable to *collusion attacks* in which several users collude to access superior-quality images.

Fig. 7 shows key-generating order of the collusion attack-resistant multi-dimensional scan-based method (method II) [9]. This method adds three partial keys to a key in its previous method [8] (referred to as a *core key* hereafter), and Fig. 8 shows the generating order of additional partial keys (referred to as *additional keys* hereafter). Thus, five partial keys, K_l^{l}, K_r^{r}, $K_{a_1}^{\mathrm{a}_1}$, $K_{a_2}^{\mathrm{a}_2}$, and $K_{a_3}^{\mathrm{a}_3}$ form a key, K_{l,r,a_1,a_2,a_3}, in Fig. 7. Since a single codestream and a single masterkey are used in this method, the total length of codestreams, $L_{C,\mathrm{II}}$, and masterkeys, $L_{K,\mathrm{II}}$, are

$$L_{C,\mathrm{II}} = U, \qquad L_{K,\mathrm{II}} = V, \tag{4}$$

respectively. To control access to the layer and the resolution level scalabilities, the number of partial keys, $N_{K,\mathrm{II}}$, increases to

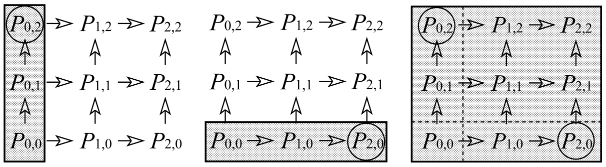
$$N_{K,\mathrm{II}} = N_L + N_R - 1. \tag{5}$$

Therefore, the partial key length, $L_{P,\mathrm{II}}$, is

$$L_{P,\mathrm{II}} = \frac{L_{K,\mathrm{II}}}{N_{K,\mathrm{II}}} = \frac{V}{N_L + N_R - 1}. \tag{6}$$

If N_L and N_R are large, it vastly increases $N_{K,\mathrm{II}}$. Simultaneously, $L_{P,\mathrm{II}}$ becomes too short to be secure. In other words, if $L_{P,\mathrm{II}}$ is enough long for security, $L_{K,\mathrm{II}}$ can be huge in this method [9].

In the next section, a new method (method III) is proposed. The proposed method is resistant to collusion attacks, whereas it


$P_{0,2}$ $P_{1,2}$ $P_{2,2}$
$P_{0,1}$ $P_{1,1}$ $P_{2,1}$
$P_{0,0}$ $P_{1,0}$ $P_{2,0}$

(a) By a user having $K_{0,2}$.

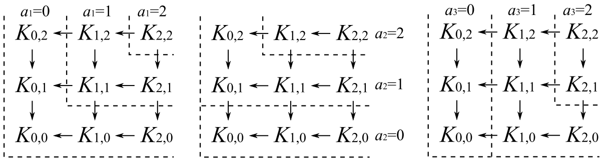
(b) By a user having $K_{2,0}$.

(c) By the collusion attack of two users in (a) and (b).

Fig. 6. Packets decryption in the collusion attack-vulnerable multi-dimensional scan-based method [8] (shaded packets are decrypted).

$$\begin{tikzcd}
K_{0,2,0,1,0} \arrow[d] & K_{1,2,1,2,1} \arrow[l] \arrow[d] & K_{2,2,2,2,2} \arrow[l] \arrow[d] \\
K_{0,1,0,1,0} \arrow[d] & K_{1,1,1,1,1} \arrow[l] \arrow[d] & K_{2,1,1,1,2} \arrow[l] \arrow[d] \\
K_{0,0,0,0,0} & K_{1,0,0,0,1} \arrow[l] & K_{2,0,0,0,1} \arrow[l]
\end{tikzcd}$$

Fig. 7. Key-generating order in the collusion attack-resistant multi-dimensional scan-based. $N_L = N_R = 3$.



(a) $K^{\mathrm{a}_1}_{a_1}$. (b) $K^{\mathrm{a}_2}_{a_2}$. (c) $K^{\mathrm{a}_3}_{a_3}$.

Fig. 8. Generating order of additional keys and those corresponding core keys in the collusion attack-resistant multi-dimensional scan-based method [9]. Core key $K_{1,1}$ is combined with additional keys $K^{\mathrm{a}_1}_1$, $K^{\mathrm{a}_2}_1$, and $K^{\mathrm{a}_3}_1$ to form a key in this method.

efficiently reduces the number of partial keys in comparison with method II [9]. It also uses a single codestream and a single masterkey in contrast to method I [7]. The proposed method, thus, reduces the redundancy of the methods I and II [7, 9].

3. PROPOSED METHOD

This section proposes a multi-dimensional scan-based JP2 encryption method using short keys that is resistant to collusion attacks. As method II [9], the proposed method adds an *additional key* to a *core key*, a key in the collusion attack-vulnerable method [8].

3.1. Condition for Collusion Attack-Resistance

This section describes the condition for serving resistance against collusion attacks.

Here, a JP2 codestream has N_L layers and N_R resolution levels as shown in Fig. 1. Keys for packets $P_{l,r}$ ($l = 0,1,\ldots,N_L-1$ and $r = 0,1,\ldots,N_R-1$) are generated from the key for the most backward packet P_{N_L-1,N_R-1}, i.e., the masterkey K_{N_L-1,N_R-1}, by using one-way hash function. Therefore,

- the key for $P_{l,r}$ can be generated from the key for a packet $P_{l',r'}$, where $l' \geq l$ and $r' \geq r$,
- the key for $P_{l,r}$ must not be generated from the keys for either $P_{l'',r}$, $P_{l,r''}$, or $P_{l'',r''}$, where $l'' < l$ and $r'' < r$.

According to the above restrictions, the condition that the encryption keys cannot be directly generated by combination of two keys is summarized as,

- A partial key in the key for packet $P_{l,r}$ must not be assigned to packets either $P_{l'',r}$, $P_{l,r''}$, or $P_{l'',r''}$, where $l'' < l$ and $r'' < r$.

If the above condition is satisfied among all packets, it stems collusion attacks.

In the next section, the key generation satisfying the above condition is proposed.

$$\begin{tikzcd}
K_{0,2,2} \arrow[d] & K_{1,2,3} \arrow[l] \arrow[d] & K_{2,2,4} \arrow[l] \arrow[d] \\
K_{0,1,1} \arrow[d] & K_{1,1,2} \arrow[l] \arrow[d] & K_{2,1,3} \arrow[l] \arrow[d] \\
K_{0,0,0} & K_{1,0,1} \arrow[l] & K_{2,0,2} \arrow[l]
\end{tikzcd}$$

Fig. 9. Key-generating order in the proposed method.

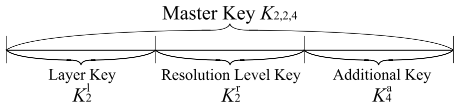


Fig. 10. The masterkey of the proposed method, $K_{2,2,4}$, is divided into three partial masterkeys K^{l}_2, K^{r}_2, and K^{a}_4.

3.2. Scheme of Key Generation

Key-generating order in the proposed method is shown in Fig. 9, where $K_{2,2,4}$ is the masterkey with length V. A key in this method is represented by $K_{l,r,a}$, and consists of a core key, $K_{l,r}$, and an *additional key*, K^{a}_a. The proposed method divides the masterkey into the three partial masterkeys, K^{l}_2, K^{r}_2, and K^{a}_4 as shown in Fig. 10. Partial keys of key $K_{l,r,a}$ for packet $P_{l,r}$ are generated from these partial masterkeys, as K^{l}_l for the layer hierarchy, K^{r}_r for the resolution level hierarchy, and K^{a}_a for resistant to collusion attacks. That is,

$$K^{\mathrm{l}}_l = H^{(N_L-1)-l}\left(K^{\mathrm{l}}_{N_L-1}\right) = H\left(H^{(N_L-1)-l-1}\left(K^{\mathrm{l}}_{N_L-1}\right)\right), \quad l = N_L-2,\ldots,1,0, \tag{7}$$

$$K^{\mathrm{r}}_r = H^{(N_R-1)-r}\left(K^{\mathrm{r}}_{N_R-1}\right), r = N_R-2,\ldots,1,0, \tag{8}$$

$$K^{\mathrm{a}}_a = H^{(N_A-1)-a}\left(K^{\mathrm{a}}_{N_A-1}\right), a = N_A-2,\ldots,1,0, \tag{9}$$

where $H(\cdot)$ is a one-way hash function and $N_A = N_L + N_R - 1$. Note $N_L = 3$, $N_R = 3$, and $N_A = 5$ in Fig. 9.

Fig. 11 shows the generating order of *additional key* K^{a}_a, and those corresponding core keys are indicated in this figure. In this method, K^{a}_a is combined with $K_{l,r}$'s, where $a = l + r$. For example, K^{a}_3 is combined with $K_{1,2}$ and $K_{2,1}$ as shown in Fig. 11 to form keys $K_{1,2,3}$ and $K_{2,1,3}$ shown in Fig. 9. The proposed method, thus, does not assign K^{a}_a to packets either $P_{l'',r}$, $P_{l,r''}$, or $P_{l'',r''}$, where $l'' < l$ and $r'' < r$. So the condition described in Sect. 3.1 is satisfied in this method, i.e., the proposed method forbids collusion attacks from generating keys directly. This method stems collusion attacks, i.e., it prevents collusion attacks partially, and it reduces the length of encryption keys.

3.3. Encryption and Decryption

This section mentions the encryption and decryption manner using the key generation described in Sect. 3.2.

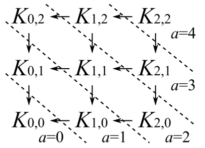


Fig. 11. Generating order of additional key, K^{a}_a, in the proposed method. K^{a}_a is assigned to core keys $K_{l,r}$, where $l + r = a$.

For a U-length JP2 codestream with N_L layers and N_R resolution levels, masterkey K_{N_L-1,N_R-1,N_A-1} is prepared, where $N_A = N_L + N_R - 1$. From this masterkey, keys are subordinately generated for all $N_L N_R$ packets by the scheme mentioned in Sect. 3.2. Packet $P_{l,r}$ is encrypted with key $K_{l,r,a}$, where $l = N_L - 1, \dots, 1, 0$, $r = N_R - 1, \dots, 1, 0$, and $a = l + r$. This encrypted JP2 codestream is only one codestream that is stored in the server and distributed to users.

A user who is allowed to obtain an image at quality Q_{U_L-1,U_R-1} receives key K_{U_L-1,U_R-1,U_A-1}, where $U_L \le N_L$, $U_R \le N_R$, and $U_A = U_L + U_R - 1$. Received key K_{U_L-1,U_R-1,U_A-1} is divided into three partial keys, and by using

$$K_l^{\mathrm{l}} = H^{(U_L-1)-l}\left(K_{U_L-1}^{\mathrm{l}}\right), l = U_L - 2, \dots, 1, 0, \qquad (10)$$

$$K_r^{\mathrm{r}} = H^{(U_R-1)-r}\left(K_{U_R-1}^{\mathrm{r}}\right), r = U_R - 2, \dots, 1, 0, \qquad (11)$$

$$K_a^{\mathrm{a}} = H^{(U_A-1)-a}\left(K_{U_A-1}^{\mathrm{a}}\right), a = U_A - 2, \dots, 1, 0, \qquad (12)$$

other partial keys are subordinately generated. Now, the user has all $U_L U_R$ keys for decrypt $P_{l,r}$ where $l = U_L - 1, \dots, 1, 0$ and $r = U_R - 1, \dots, 1, 0$. The image at quality Q_{U_L-1,U_R-1} is, thus, decoded from decrypted $U_L U_R$ packets.

3.4. Short Key Length

In the proposed method, the total length of codestreams, $L_{C,\mathrm{III}}$, and masterkeys, $L_{K,\mathrm{III}}$, are

$$L_{C,\mathrm{III}} = U, \qquad L_{K,\mathrm{III}} = V, \qquad (13)$$

respectively, as long as method II [9]. However, the number of partial keys, $N_{K,\mathrm{III}}$, is

$$N_{K,\mathrm{III}} = 3, \qquad (14)$$

as mentioned in Sect. 3.2, whereas method II uses partial keys as many as Eq. (5), i.e., $N_{K,\mathrm{II}} = N_L + N_R - 1 = 5$ under the identical conditions that $N_L = N_R = 3$. Since $N_{K,\mathrm{III}}$ is independent from N_L and N_R, the proposed method does not require the huge number of partial keys, though N_L and/or N_R become large. The partial key length, $L_{P,\mathrm{III}}$, is

$$L_{P,\mathrm{III}} = \frac{L_{K,\mathrm{III}}}{N_{K,\mathrm{III}}} = \frac{V}{3}. \qquad (15)$$

Since $L_{P,\mathrm{III}}$ is also independent from N_L and N_R, the proposed method serves the identical security level, though N_L and/or N_R vary.

4. COMPARISON IN STORING

Firstly, the proposed and conventional [7, 9] methods are compared under the condition that a U-length JP2 codestream is composed of N_L layers and N_R resolution levels and the length of a masterkey is V. Table 1 compares the total lengths of codestreams, the total lengths of masterkeys to be managed, and the length of a partial key among method I (the one-dimensional scan-based method [7]), method II (the multi-dimensional scan-based method [9]), and method III (the proposed method). If $N_L = 10$ and $N_R = 3$, $L_{P,\mathrm{II}} = V/12$ and $L_{P,\mathrm{III}} = V/3$. The proposed method is four times more secure than method II [9] in terms of the length of a partial key.

Then, three methods are compared under the condition that the length of a partial key is W. Table 2 compares the total lengths of codestreams, the length of a partial key, and the total length of masterkeys to be managed among three methods. If $N_L = 10$ and $N_R = 3$, $L_{K,\mathrm{II}} = 12W$ and $L_{K,\mathrm{III}} = 3W$. That is, the proposed method reduces the management and delivery costs of the masterkey by a quarter of method II [9].

Table 1. The total length of codestreams, the total length of masterkeys, and the length of a partial key. I: the one-dimensional scan-based method [7], II: the multi-dimensional scan-based method [9], and III: the proposed method. The length of a JP2 codestream that consists of N_L layers and N_R resolution levels is U and the length of a masterkey is V.

	I [7]	II [9]	III
Total codestream length L_C	$5U$	U	U
Total masterkey length L_K	$5V$	V	V
A partial key length L_P	V	$\frac{V}{N_L+N_R-1}$	$\frac{V}{3}$

Table 2. The total length of codestreams and the total length of masterkeys. I: the one-dimensional scan-based method [7], II: the multi-dimensional scan-based method [9], and III: the proposed method. The length of a JP2 codestream that consists of N_L layers and N_R resolution levels is U and the length of a partial key is W.

	I [7]	II [9]	III
Total codestream length L_C	$5U$	U	U
Total masterkey length L_K	$5W$	$(N_L + N_R - 1)W$	$3W$

5. CONCLUSIONS

This paper has proposed a new encryption method with a short length key for access control to scalable JP2 codestreams. The proposed method enables access control with a single codestream and a single masterkey for multiple JP2 scalability functions.

REFERENCES

[1] B.B. Zhu, M.D. Swanson, and S. Li, "Encryption and art and challenges," in *Proc. SPIE*, vol.5601, pp.157–170, 2004.

[2] M. Fujiyoshi, Y. Seki, H. Kobayashi, and H. Kiya, "Modulo arithmetic-based image watermarking and its theoretical analysis of image-quality," in *Proc. IEEE ICIP*, pp.969–972, 2005.

[3] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG2000 compressed domain," in *Proc. SPIE*, vol.4472, pp.95–104, 2001.

[4] H. Kiya, S. Imaizumi, and O. Watanabe, "Partial-scrambling of image encoded using JPEG2000 without generating marker codes," in *Proc. IEEE ICIP*, 2003.

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

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

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

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

[9] 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.137–140, 2007.

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