COLLUSION ATTACK-RESILIENT HIERARCHICAL ENCRYPTION OF JPEG 2000 CODESTREAMS WITH SCALABLE ACCESS CONTROL

Shoko IMAIZUMI[*†], *Masaaki FUJIYOSHI*[*], *Yoshito ABE*[†], *and Hitoshi KIYA*[*]

[*]Dept. of Info. and Comm. Syst. Eng., 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 a collusion attack-resilient method of encryption for access control of JPEG 2000 codestreams with hierarchical scalabilities. The proposed method generates one encryption key from one single key by multi-dimensional scanning to serve encryption keeping the scalability of codestrems. To avoid collusion attacks in which multiple users generate an illegal key from their own keys to overcome the access control, sufficient conditions are considered in this method. Moreover, a skip encryption is introduced to decrease the computational complexity and key management-and-delivery cost of encryption. Simulation results show the effectiveness of the proposed method.

Index Terms— Access control, Symmetric key cryptography, One-way hash function, Scalability, Internet

1. INTRODUCTION

Exchanging digital images commercially or non-commercially has became very common with the growth in network technology. Protecting copyrights and the 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 protecting such digital images, i.e., naïve encryption (encrypting the entire content) [1], digital watermarking [2], and *partial encryption* [3–8]. A scheme for partial encryption is proposed in this paper to control access to hierarchical JPEG 2000 (JP2) codestreams.

There are *scalability* functions to enable easy access to subsets of a JP2 [9] codestream. Hence, an encryption scheme for JP2 codestreams should be *scalable*. There are several methods of encryption for *hierarchically* scalable codestreams. These can be categorized into three classes. The first [4, 5] needs multiple keys to encrypt an entire codestream.The second [6] scans JP2 packets by one-dimensional order to generates a single key consisting of partial keys for each JP2 packets, but it requires another key for a codestream with another kind of *progression order*. The third [7, 8] generates a single key by multi-dimensionalscan from the managed key to solve the above redundancy, but it suffers from problem, i.e., collusion attacks.

This paper proposes a new method of encryption for JP2 codestreams with hierarchical scalabilities to overcome collusion attacks. The proposed method also generates a single key by multi-dimensional scanning, it introduces extra partial keys to resist collusion attacks based on analysis. Furthermore, a *skip encryption* scheme is proposed to reduce the number of keys to be generated and the number of packets to be encrypted. This effectively avoids computational complexity when there are many hierarchical stages in a JP2 codestream.

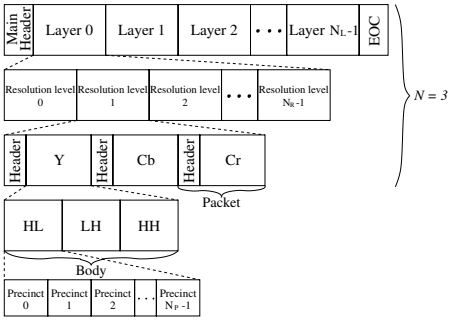


Fig. 1. JP2 codestream with color components, Y, C_b, and C_r.

2. JP2 CODESTREAM AND CONVENTIONAL ENCRYPTION METHODS FOR ACCESS CONTROL

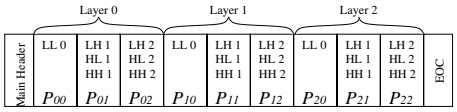
2.1. JP2 Codestream [9]

Fig. 1 outlines a JP2 codestream using YC_bC_r as the color space. Here, each scalability function has its order of priority called a *progression order*. Its progression order is LRCP (Layer-Resolution level-Component-Position), i.e., the layer scalability function is the first priority. Each layer is composed of the data for each 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 LL, and the other resolution levels contain three sub-bands (HL, LH, and HH). These sub-bands have precincts that have non-hierarchically positional information. Thus, a color JP2 codestream has three hierarchical scalability functions ($N = 3$) and a grayscale one has two ($N = 2$). Each packet is composed of a header and a body and contains partial data for each sub-band. The proposed method encrypts the data in the body but does not encrypt the headers.

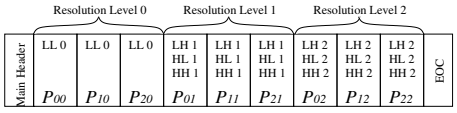
Fig. 2 lists examples of JP2 codestream with LRCP or RLCP order of progression. Both has three layer hierarchies and three resolution-level hierarchies, which are represented as $N_L = 3$ and $N_R = 3$ in this paper. Hereafter, P_{lr} is the JP2 packet at l-th layer and r-th resolution level.

2.2. Hierarchical Encryptions and Their Restrictions

Since an image data is separated according to the hierarchy of scalability functions as shown in Fig. 2, an encryption method must maintain the hierarchy. Fig. 3 outlines an example where a grayscale image is hierarchically decoded with $N = 2$. The original image is



(a) Progression order: LRCP.



(b) Progression order: RLCP.

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

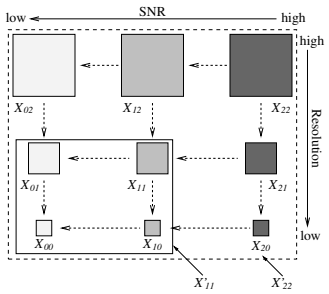


Fig. 3. Hierarchical decoding of grayscale image: $N_L = 3$ and $N_R = 3$.

coded at quality X'_{22}, that is $N_L = 3$ and $N_R = 3$. When an user wants to get the image at quality X'_{11}, four partial image data, i.e., X_{00}, X_{01}, X_{10}, and X_{11} are decrypted and decoded.

Single key encryption with multi-dimensional scanning [7, 8] generates keys from the single managed key, *master key*, and controls access to multiple scalability functions simultaneously. Generating encryption keys two-dimensionally by this method is shown in Fig. 4. The encryption key for packet P_{lr} is K_{lr}, and K_{22} is the master key. The arrows indicate the directions of key generation. As shown in Fig. 5, master key K_{22} with M bytes is divided into two partial keys $K_{\mathrm{l},2}$ with M_L bytes and $K_{\mathrm{r},2}$ with M_R bytes. Each partial key is allocated to each hierarchy, and the partial keys $K_{\mathrm{l},l}$ and $K_{\mathrm{r},r}$ for packet P_{lr} are generated from the previous partial keys $K_{\mathrm{l},l+1}$ and $K_{\mathrm{r},r+1}$, using a one-way hash function. By concatenating them, $K_{lr} = (K_{\mathrm{l},l}, K_{\mathrm{r},r})$, is generated.

However, this method is not resilient against collusion attacks. In the next section, collusion attacks is explained and a collusion attack-resilient method of hierarchical encryption is proposed.

3. PROPOSED METHOD

This section proposes an encryption method for JP2 codestreams that is resilient against collusion attacks. Moreover, a skip encryption method considering computational complexity is proposed. It is noteworthy that the proposed method encrypts color images as well as grayscale images, though JP2 codestreams with only layer and resolution-level hierarchies are used for its simplicity hereafter.

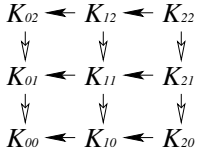


Fig. 4. Key-generating order in single-key encryption with multi-dimensional scanning [7, 8].

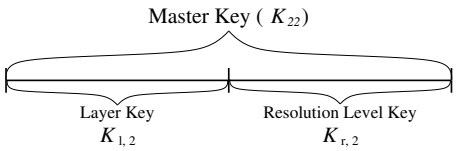
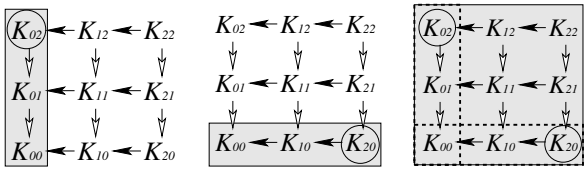


Fig. 5. Master key in conventional single-key encryption with multi-dimensional scanning [7, 8].



(a) Keys authorized to a user with K_{02}.

(b) Keys authorized to a user with K_{20}.

(c) Keys generated by the users with K_{02} and K_{20}.

Fig. 6. Keys generated by collusion attack (the shaded keys are generated).

3.1. Collusion Attacks

A collusion attack occurs when multiple users share their keys maliciously and decode images of higher quality than those authorized. Conventional methods [7, 8] do not have resilience against collusion attacks.

In Fig. 4, it is assumed that Alice has received key K_{02} and Bob has received key K_{20}. K_{02} is divided into $K_{\mathrm{l},0}$ and $K_{\mathrm{r},2}$. K_{20} is divided into $K_{\mathrm{l},2}$ and $K_{\mathrm{r},0}$. As seen in Fig. 6, if the two users conspire, all the other keys including the master key, $K_{22} = \left(K_{\mathrm{l},2}, K_{\mathrm{r},2}\right)$, can be generated illegally. The purpose of the proposed method is to avoid this kind of collusion attack.

3.2. Scheme of Key Generation

The order of key generation in the proposed method is outlined in Fig. 7, where $K_{lr,a_1a_2a_3}$ is a key for packet P_{lr}, and the master key is $K_{22,222}$ with M bytes. The proposed method with resilience against collusion attacks divides the master key into five partial master keys, $K_{\mathrm{l},2}$, $K_{\mathrm{r},2}$, $K_{\mathrm{a}_1,2}$, $K_{\mathrm{a}_2,2}$ and $K_{\mathrm{a}_3,2}$, as outlined in Fig. 8. These partial master keys are with M_L, M_R, M_{A_1}, M_{A_2}, and M_{A_3} bytes, and are allocated to each hierarchy. When M_{A_1}, M_{A_2}, and M_{A_3} are zero bytes, $K_{lr,a_1a_2a_3}$ is represented as $K_{lr,***}$ and has the relation

$$K_{lr,***} = K_{lr}. \tag{1}$$

The five partial keys for each packet P_{lr} are generated from these keys as the $K_{\mathrm{l},l}$ for the layer hierarchy, $K_{\mathrm{r},r}$ for the resolution-level

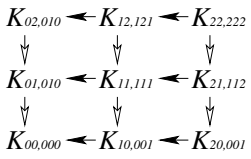


Fig. 7. Key-generating order in the proposed encryption scheme with resilience against collusion attacks.

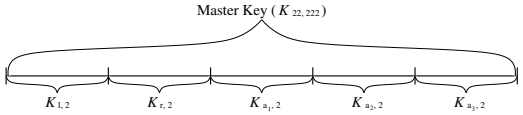
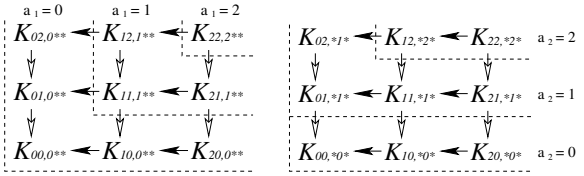
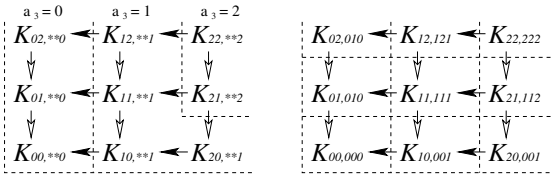


Fig. 8. Master key in proposed method.



(a) K_{lr,a_1**} with K_{a_1,a_1}. (b) $K_{lr,*a_2*}$ with K_{a_2,a_2}.



(c) $K_{lr,**a_3}$ with K_{a_3,a_3}. (d) $K_{lr,a_1a_2a_3}$ combined three partial keys.

Fig. 9. Additional partial keys for resilience against collusion attacks. By combining three additional partial keys, K_{a_1,a_1}, K_{a_2,a_2}, and K_{a_3,a_3}, the proposed encryption scheme is collusion attack-resilient.

hierarchy, and K_{a_1,a_1}, K_{a_2,a_2}, and K_{a_3,a_3} for resilience against collusion attacks. That is,

$$K_{l,l} = H^{(N_L-1)-l}\left(K_{l,N_L-1}\right) = H\left(H^{(N_L-1)-l-1}\left(K_{l,N_L-1}\right)\right), \quad l = N_L-2,\ldots,1,0, \tag{2}$$

$$K_{r,r} = H^{(N_R-1)-r}\left(K_{r,N_R-1}\right),\ r = N_R-2,\ldots,1,0, \tag{3}$$

$$K_{a_1,a_1} = H^{(N_{A_1}-1)-a_1}\left(K_{a_1,N_{A_1}-1}\right),\ a_1 = N_{A_1}-2,\ldots,1,0, \tag{4}$$

$$K_{a_2,a_2} = H^{(N_{A_2}-1)-a_2}\left(K_{a_2,N_{A_2}-1}\right),\ a_2 = N_{A_2}-2,\ldots,1,0, \tag{5}$$

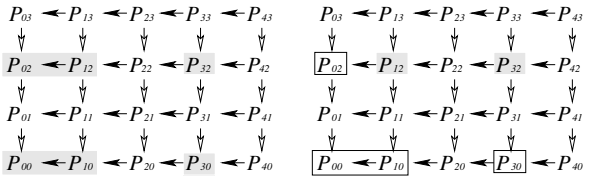
$$K_{a_3,a_3} = H^{(N_{A_3}-1)-a_3}\left(K_{a_3,N_{A_3}-1}\right),\ a_3 = N_{A_3}-2,\ldots,1,0, \tag{6}$$

where $H(\cdot)$ is an one-way hash function. Note that $N_L = 3$, $N_R = 3$, $N_{A_1} = 3$, $N_{A_2} = 3$, and $N_{A_3} = 3$ in Fig. 7. These partial keys are combined to generate an encryption key, $K_{lr,a_1a_2a_3} = \left(K_{l,l}, K_{r,r}, K_{a_1,a_1}, K_{a_2,a_2}, K_{a_3,a_3}\right)$.

3.3. Effectiveness of Additional Partial Keys for Resilience against Collusion Attacks

If the structure of a JP2 codestream is that shown in Fig. 2 (a), i.e., three layers ($N_L = 3$) and three resolution-levels ($N_R = 3$) in LRCP order, three partial keys, K_{a_1,a_1}, K_{a_2,a_2}, and K_{a_3,a_3} are introduced in this proposed encryption. That is, the master key is divided into five partial keys as shown in Fig. 8, and other keys are generated according to the multi-dimensional scanning shown in Fig. 7, where each key is generated by Eqs.(2), (3), (4), (5), and (6). Combining three additional partial keys makes the proposed encryption scheme resilient against collusion attacks as shown in Fig. 9.

Here, it is assumed that Alice having $K_{12,121}$ colludes with Bob having $K_{20,001}$. If K_{a_1,a_1} is only introduced as shown in Fig. 9 (a), they can illegally generate $K_{21,1**}$ that is beyond their permission. Moreover, if K_{a_2,a_2} is only used as shown in Fig. 9 (b), they can get all the keys including the master key. That is, they can share the image with the highest quality. However, by employing K_{a_3,a_3}, they involve no extra key ,because they do not have $K_{a_3,2}$ according to Fig. 9 (c).



(a) Encrypted packets. (b) Decryptable packets by Alice and Bob.

Fig. 10. Example of choosing packets to be encrypted and resilience against collusion attacks in the proposed skip encryption method (the number of packets to be encrypted is $\hat{N}_L\hat{N}_R = 6$).

The number of additional keys for resilience against collusion attacks depends on the number of layers and the number of resolution-levels, and it is given as $(N-1)N_L + (N-1)N_R - 3$. Because it is assumed that $N = 2$, $N_L = 3$, and $N_R = 3$ above, the number of additional partial keys is $(2-1)3 + (2-1)3 - 3 = 3$ as shown in Fig. 9. If three hierarchical scalability functions, i.e., layer, resolution-, and color components, are determined as scalability functions to be controlled ($N = 3$), the number of additional partial keys becomes

$$(N-1)N_L + (N-1)N_R + (N-1)N_C - 3, \tag{7}$$

where N_C represents the number of color components.

It is clear that the number of additional partial keys increases according to the number of JP2 packets which depends on the number of hierarchical scalability functions and the number of tiers in each scalability. To avoid introducing a number of partial keys that are for resilience against collusion attacks, a further method is proposed in the next section.

3.4. Skip Encryption Method

In this section, a further method is proposed to reduce the number of extra partial keys and computational complexity of operations with encryption. It is a skip encryption method that encrypts several JP2 packets rather than all packets, though it does not prevent all of collusion attacks. Because a packet that is less significant in a hierarchy is subordinate to more significant packets, protecting significant packets is determined to be enough in practice. Note that the skip encryption in this paper is different from Simple Key-management for Internet Protocol (SKIP) [10].

In definite, the proposed skip encryption method encrypts $\hat{N}_L\hat{N}_R$ packets under the conditions that layer and resolution-levels scalability functions are determined for controlling access, where $1 \le \hat{N}_L \le N_L$ and $1 \le \hat{N}_R \le N_R$. Now, the number of additional partial keys decreases to $(N-1)\hat{N}_L + (N-1)\hat{N}_R + 3$, and the number of packets to be encrypted also decreases from N_LN_R to $\hat{N}_L\hat{N}_R$. The latter reduces the computational complexity of operations with encryption. A JP2 codestream with $N = 2$, $N_L = 5$, and $N_R = 4$ is assumed. Fig. 10 (b) shows an example in which six packets, P_{00}, P_{02}, P_{10}, P_{12}, P_{30}, and P_{32} are selected to be encrypted, that is $\hat{N}_L = 3$ and $\hat{N}_R = 2$. If Alice who is authorized to decode the most significant layer, layer zero, colludes with Bob who is authorized to decode the most significant resolution-level, LL sub-band, for this configuration, they can only decrypt four packets, P_{00}, P_{02}, P_{10}, and P_{30}, as shown in Fig. 10 (b). Neither P_{12} nor P_{32} is decrypted by the conspirators.

(a) Conventional methods [7, 8]. (b) Proposed method. (c) Proposed skip encryption.

Fig. 11. Collusion attacks: Alice colludes with Bob.

Table 1. Comparisons of key length, the total length of codestreams to be managed, and the number of packets to be encrypted. I: the proposed encryption, II: the proposed skip encryption, III: encryption with multiple keys [5], and IV: single key encryption with one-dimensional scanning [6] (the length of a JP2 codestream that has N_L layers and N_R resolution-levels is N bytes, the length of a master key for a packet is M bytes, $\hat{N}_L \leq N_L$, and $\hat{N}_R \leq N_R$).

	I	II	III [5]	IV [6]
Key length [bytes]	M	M	$N_L N_R M$	$5M$
Codestream length [bytes]	N	N	N	$5N$
Encrypted packets	$N_L N_R$	$\hat{N}_L \hat{N}_R$	$N_L N_R$	$N_L N_R$

4. EXPERIMENTAL RESULTS

4.1. Resilience against Collusion Attacks

512×512-sized 24 bits color image "Lena" was encoded by JP2 VM8.6 Software.The number of layers was set to five, i.e., $N_L = 5$. From the most significant layer to the least significant layer, the coding rates were set to 0.05 bits/pixel (bpp), 0.1 bpp, 0.2 bpp, 0.5 bpp, and 1.0 bpp, respectively. Thus, the coding rate of the entire codestream was one bpp. The number of resolution-levels was four, i.e., $N_R = 4$. Blowfish [11], a block cipher of symmetric key algorithm, was used for scrambling and descrambling, though any symmetric key cryptography is applicable to the proposed method. The number of packets to be encrypted was set to six that corresponds to Fig. 10 (a) where $\hat{N}_L = 3$ and $\hat{N}_R = 2$.

Here, it is assumed that Alice colludes with Bob as in Section3.4. In single key encryption with multi-dimensional scanning without resilience against collusion attacks [7, 8], if Alice and Bob maliciously share their keys, they can generate all the keys and can share the image shown in Fig. 11 (a) that is the image with the highest quality. Whereas the proposed method resisting collusion attacks does not allow the conspirators to decrypt any additional packets. If they forcibly decode the codestream having encrypted packets, they just share the image shown in Fig. 11 (b). By introducing extra partial keys, the proposed method of encryption prevents collusion attacks. Furthermore, if the proposed skip encryption method encrypts the image according to Fig. 10 (b), forcible decoding of the codestream by Alice and Bob displays the image shown in Fig. 11 (c). Though the proposed skip encryption reduces the key length, the computational cost for encrypting a packet, and the number of packets to be encrypted in comparison with the proposed method described in Section 3.3, it serves practical resilience against collusion attacks.

4.2. Comparison in Storing and Computational Complexity

It is assumed that the length of a JP2 codestream that consists of N_L layers and N_R resolution-levels is N bytes. It is also assumed that the length of the master key is M bytes. Table 1 summarizes the comparisons of key length, the total length of codestreams to be managed, and the number of packets to be encrypted in the four methods, i.e., the proposed encryption method, the proposed skip encryption method, encryption with multiple keys [5], and single key encryption with one-dimensional scanning [6].

Because the number of master keys and codestreams are ones in the proposed encryption method and the proposed skip encryption method, the key length's are M bytes and the total length's of codestreams are N bytes. Whereas encryption with multiple keys [5] requires keys as many as packets to be encrypted, the key length grows to $N_L N_R M$ bytes. According to the number of orders of progression, five, single key encryption with one-dimensional scanning [6] requires five codestreams and the corresponding five master keys. Thus, the keys length and the total length of codestreams become $5M$ and $5N$ bytes, respectively. From the perspective of the number of packets to be encrypted, the proposed encryption method, encryption with multiple keys, and single key encryption with one-dimensional scanning are the same as one another, i.e., $N_L N_R$. On the other hand, the proposed skip encryption method encrypts $\hat{N}_L \hat{N}_R$ packets, where $\hat{N}_L \leq N_L$ and $\hat{N}_R \leq N_R$.

5. CONCLUSIONS

This paper has proposed a collusion attack-resilient encryption for scalable JP2 codestreams to access control. To avoid collusion attack and simultaneously serve scalable encryption, the proposed method simply introduces additional partial keys. Furthermore, a skip encryption has been proposed to decrease the computational complexity and key management-and-delivery costs of the proposed collusion attack-resilient method.

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] 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] Y. Suga, and K. Iwamura, "Key management schemes for Hierarchy-based access control using one-way hash functions," in *Proc. IPSJ CSS*, pp.295–300, 2003.

[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*, pp.895–898, 2006.

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

[7] 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.

[8] 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.

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

[10] A. Aziz, M. Patterson, and G. Baehr, "Simple Key-Management for Internet Protocol (SKIP)," in *Proc. ISOC INET*, 1995.

[11] B. Schneier, "Description of a new variable-length key, 64-bit block cipher," in *Proc. FSE*, pp.191–204, 1996.