I.J. Wireless and Microwave Technologies, **2011, 3, 54-61**
Published Online June 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.03.09

Available online at http://www.mecs-press.net/ijwmt

Format-Compliant Encryption of JPEG2000 Codestreams

Zhiguo Chang[a], Jian Xu[b]

[a]*School of Information Engineering, Chang'an University, Xi'an, P.R. China*
[b]*School of Communication and Information Engineering Xi'an University of Posts & Telecommunications, School of Electronic and information Engineering, Xi'an Jiaotong University, Xi'an, P.R. China*

Abstract

In this paper, we propose two format-compliant encryption schemes for JPEG2000, which preserve the syntax of the original codestream and do not introduce superfluous markers into the encrypted bitstream. The proposed efficient scheme randomly encrypts either low or upper half bytes of those randomly selected bytes in Codeblock Contribution to Packets (CCPs). The secure scheme encrypts both low and upper half bytes and can protect the nearly whole codestream except for the header information. The proposed schemes can provide efficient, secure, scalable and completely format-compliant protection of JPEG2000, which is proved by lots of experiments.

Index Terms: JPEG2000; format-compliant; encryption

1. Introduction

Digital imagery is pervading in everyone's daily life. In order to save the storage and bandwidth, raw images are usually represented efficiently by compression. JPEG2000 [1] is the latest worldwide standard for compression of still images. JPSEC[2] is Part 8 of the JPEG2000 standard. One major technical issue in JPSEC is encryption. A JPEG2000 code stream consists of markers and auxiliary data (i.e., packet data). All markers are byte-aligned, and the code stream is always an integral number of bytes.

Norcen and Uhl [3] partially encrypt JPEG2000 code stream with an AES symmetric block cipher in CFB mode. They report that encryption of 20% bitstream can provide a high level confidentiality. The scheme isn't compliant to JPEG2000 codestream.

Wu and Deng [4] recursively encrypt Codeblock Contribution to Packets (CCPs) using arithmetic addition module until the cipher text meet two requirements: no word exceed [0,0xFF90); the end byte is not 0xFF. For many CCPs more than one encryption pass are needed.

Kiya et al [5] randomly select some bytes from body data and scramble their lower half bytes by bit-shift operation. The scheme is efficient and can output the compliant bitstreams.

Conan et al [6] present a similar algorithm, if any byte has a value less than 0xF0, its four LSBs (Least Significant are encrypted with a block cipher. Apparently the security of the simple schemes [5][6] is weak.

Lian et al [7] selectively encrypt some sensitive frequency subbands, bit-planes or encoding-passes with conventional ciphers, such as RC4 and AES. The scheme could introduce superfluous markers in the encrypted codestreams.

Fang and Sun [8] proposed format-compliant, complete encryption of JPEG2000 bitstreams. Relationship between contiguous bytes is exploited for encryption. If one byte is damaged during the transmission it would influence the decryption of its following bytes.

This paper presents two scalable, format-compliant encryption schemes. The efficient scheme can protect the codestream very well by encryption the small portion of data. The other one can provide high security protection of JPEG2000 codestream.

The rest of this paper is organized as follows. Section 2 firstly introduces the structure of JPEG2000 packet, and then describes our compliant encryption schemes in detail. Section 3 analyzes the security of the proposed scheme. Experimental results in Section 4 demonstrate the effective and efficiency of the proposed scheme. Conclusions are summarized in Section 5.

2. The Proposed Schemes

2.1. JPEG2000 Packet Structre

The data representing a specific tile, layer, component, resolution and precinct appears in the code stream in a contiguous segment called a packet. Packet data is aligned at 8-bit (one byte) boundaries. A packet consists of packet header (between SOP and EPH) and packet body (Figure 1). Packet body is composed of CCPs, information about which is introduced tag tree in packet header. The data in a packet is ordered such that the contribution from the LL, HL, LH and HH sub-bands appear in that order. Resolution r = 0 contains only the LL band and resolutions r > 0 contain only the HL, LH and HH bands. Codewords (i.e., two contiguous bytes) in the packet are not in the interval [0xFF90, 0xFFFF] and the last byte is not 0xFF.

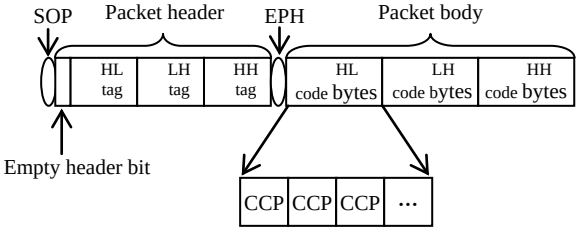


Fig 1. JPEG2000 packet structure.

Two requirements can assure that the syntax of the original bitstream is preserved:

1. No extra $0xFF$ is introduced into the encrypted codestream.
2. Keep the byte, which is less than $0x90$, being below $0x90$.

2.2. Techniques for Compliant Encryption of JPEG2000 Bitstreams

In the proposed schemes, the following encryption techniques are employed to meet the two requirements and make the scheme more efficient.

1. Select a CCP as the encryption unit, which can maintain the scalability of original codestreams. Each CCP is partitioned into a byte sequence: $CCP \to \{P_1, P_2, \cdots, P_k, \cdots\}$, P_k is 1-byte data.
2. Randomly selected some bytes in the CCP for encryption, which can decrease the computation complexity. Let $\{r_i\}$ be a set of random integers generated by a secret key. λ is a parameter used to control the length of codestream to be encrypted. $\{\lambda_i\}$ is a set of random incremental steps. $\{T(\lambda_i)\}$ determines which bytes in the CCP are encrypted. The maximum of $\{T(\lambda_i)\}$ must be less than or equal to the length of CCP. Elements in $\{\lambda_i\}$ and $\{T(\lambda_i)\}$ can be calculated by (1) and (2) respectively.

$$\lambda_i \leftarrow r_i \bmod \lambda + 1 \tag{1}$$

$$T(\lambda_i) = T(\lambda_{i-1}) + \lambda_i \tag{2}$$

3. The randomly selected byte P can be divided into two half bytes: Upper half byte P_U (the four MSBs of P) and low half byte P_L (the four LSBs of P). P_U and P_L are individually encrypted by (3) and (4).
4. Encrypt low half byte P_L with (3).

$$C_L = \begin{cases} (P_L + r) \bmod 0x10, & P < 0xF0 \\ (P_L + r) \bmod 0xF, & 0xF0 \le P < 0xFF \\ 0xF, & P = 0xFF \end{cases} \tag{3}$$

5. Encrypt upper half byte P_U with (4).

$$C_U \leftarrow \begin{cases} (P_U + r) \bmod 0x9, & P_U < 0x9 \\ (P_U - 0x9 + r) \bmod 0x6 + 0x9, & 0x9 \le P_U < 0xF \\ 0xF & P_U = 0xF \end{cases} \tag{4}$$

2.3. Efficient, Format-Compliant Encryption Scheme

We can combine the above techniques and design an efficient, format-compliant JPEG2000 encryption scheme.

1. Assume JPEG2000 codestream is organized in layer-resolution-component-position (LRCP) progressive order. Lower layer in the codestream contains significant information. We selectively encrypt the packets in the lower layers.
2. We choose large parameter λ and encrypt less data to achieve the efficiency. The larger λ will result in leak of more information. However, compression is also a scramble, and so leak of some compressed data will not make the decrypted image dramatically distinguishable, which can be shown in the experimental section.
3. We randomly encrypt either low or upper half bytes of the randomly selected bytes.

2.4. Secure, Format-Compliant Encryption Scheme

We take following measures to design a high-level of security, complaint encryption scheme.

1. Choose all layers in the codestream for encryption.
2. Decrease parameter λ to encrypt more bitstream. Extremely if $\lambda = 1$, all bytes are to be encrypted.
3. Both low and upper half bytes are encrypted with (3) and (4)

The procedure of proposed secure, compliant encryption scheme is shown in Figure 2.

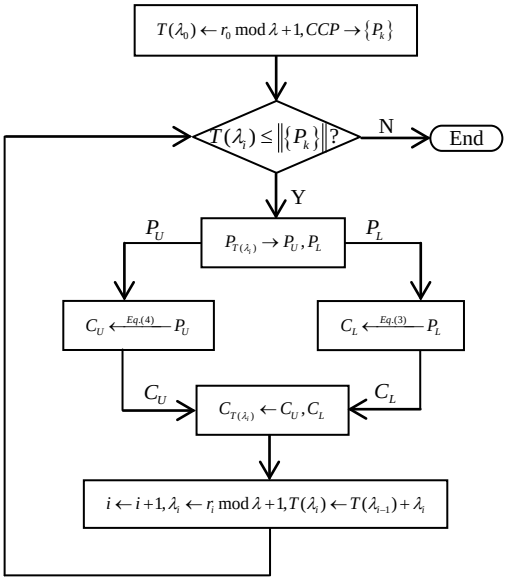


Fig 2. Diagram of encrypt a CCP

$\|\{P_k\}\|$ is the length of $\{P_k\}$ or the number of elements in the it. Decrypt low half byte C_L with (5).

$$P_L = \begin{cases} (C_L - r) \bmod 0x10, & C < 0xF0 \\ (C_L - r) \bmod 0xF, & 0xF0 \le C < 0xFF \\ 0xF, & C = 0xFF \end{cases} \tag{5}$$

Decrypt upper half byte C_U with (6).

$$P_U \leftarrow \begin{cases} (C_U - r) \bmod 0x9, & C_U < 0x9 \\ (C_U - 0x9 - r) \bmod 0x6 + 0x9, & 0x9 \le C_U < 0xF \\ 0xF & C_U = 0xF \end{cases} \tag{6}$$

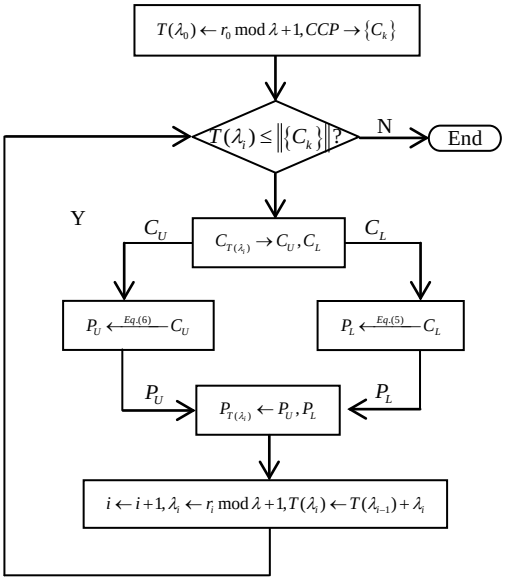


Fig 3. Diagram of decrypt a CCP

3. Security Analysis

In this section the security of the secure encryption scheme is analyzed. For simplicity we assume that bytes in the CCP are uniformly distributed random integers. Low and upper half bytes are random integers too.

Averagely for each byte there are Γ possible values

$$\begin{aligned} \Gamma &= (16 \times \Pr_{low1} + 15 \times \Pr_{low2}) \times (9 \times \Pr_{upper1} + 6 \times \Pr_{upper2}) \\ &= (16 \times \frac{240}{256} + 15 \times \frac{15}{256}) \times (9 \times \frac{9}{16} + 6 \times \frac{6}{9}) \qquad \Pr_{low1} = \Pr(P < 0xF0) \\ &= 15.88 \times 10.75 \\ &= 170.71 \end{aligned}$$

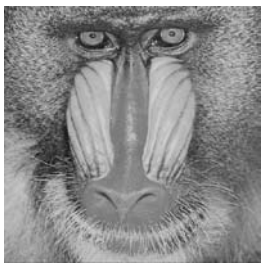
$\Pr_{upper1} = \Pr(P_U < 0x9)$ $\Pr_{low2} = \Pr(0xF0 \le P < 0xFF)$ $\Pr_{upper2} = \Pr(0x9 \le P_U < 0xF)$

For a CCP whose length equals to $\left\|\{P_k\}\right\|$, there are $\Gamma^{\left\|\{P_k\}\right\|}$ possibilities. Since it's a very large number, our scheme is secure.

4. Experiments

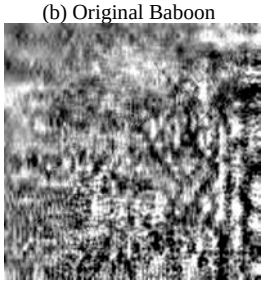
Lots of experiments have been done to verify the effectiveness and efficiency of the proposed efficient scheme. Test images are 512×512 8-bit grayscale standard images. 5-level DWT is applied to the test images and 16 subbands (LL0, LH0, HL0, HH0, …， LH4， HL4， HH4). According to rate=0.1,0.2,0.3,0.4,0.5, five layers are generated and the codestream is ordered in LRCP. The efficient encryption scheme is simulated and compared with Norcen's method [3].

(a) Original Lena

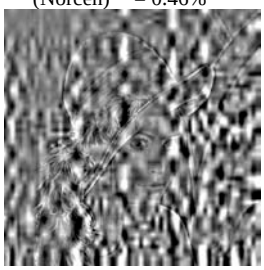


(b) Original Baboon

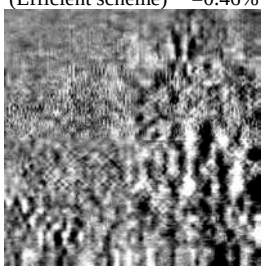
(c) Encrypted Lena (Norcen) r = 0.46%



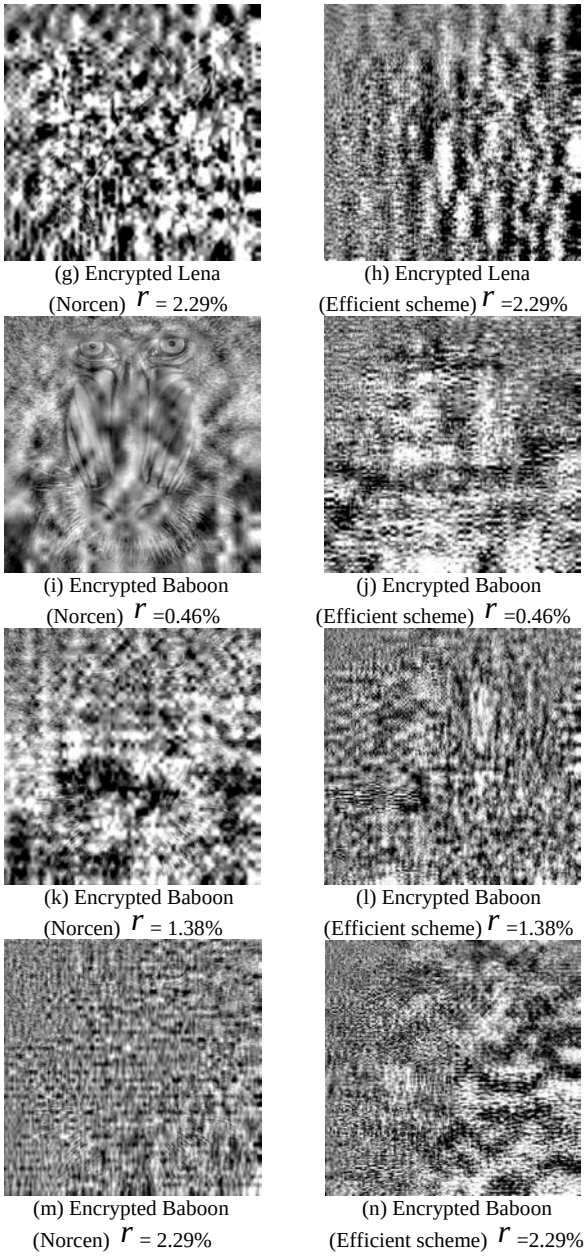
(d) Encrypted Lena (Efficient scheme) r =0.46%



(e) Encrypted Lena (Norcen) r = 1.38%



(f) Encrypted Lena (Efficient scheme) r =1.38%



(g) Encrypted Lena (Norcen) r = 2.29%

(h) Encrypted Lena (Efficient scheme) r =2.29%

(i) Encrypted Baboon (Norcen) r =0.46%

(j) Encrypted Baboon (Efficient scheme) r =0.46%

(k) Encrypted Baboon (Norcen) r = 1.38%

(l) Encrypted Baboon (Efficient scheme) r =1.38%

(m) Encrypted Baboon (Norcen) r = 2.29%

(n) Encrypted Baboon (Efficient scheme) r =2.29%

Fig 4. Comparison between Norcen's method and our efficient scheme

Experiments show our efficient scheme protect Lena and Baboon better than Norcen's method. When 0.46% data are encrypted, original contents are hardly distinguished from the protected images with our efficient scheme. However main contents encrypted by Norcen's method can be clearly saw. When about 2% codestreams are encrypted, our scheme can protect images very well, but Norcen's scheme is still leak some important information.

5. Conclusions

Two scalable, format-compliant encryption schemes for JPEG2000 are presented. The efficient scheme can protect images by encryption of only a few data. The computation complexity is low and can be easily implemented. The secure encryption scheme can provide high-level of security protection.

Acknowledgment

The project was supported by the special fund for basic scientific research of central colleges, Chang'an University (CHD2009JC156) and Science Foundation for The Excellent Youth Scholars, Xi'an University of Posts & Telecommunications (ZL2010-21).

References

[1] ISO/IEC International Standard 15444-1, "Information Technology - JPEG 2000 Image Coding System," Mar 2000.
[2] ISO/IEC International Standard 15444-8, "Information Technology - JPEG 2000 Image Coding System – part 8: Secure JPEG 2000," Nov 2004
[3] R. Norcen and A. Uhl, "Selective encryption of the JPEG2000 bitstream," Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS, 3: pp. 194–204.
[4] Y. D. Wu and R. Deng, "Compliant encryption of JPEG2000 codestreams," IEEE Intl. Conf. Image Process. Oct. 2004, Singapore, ISBN0-7803-8555-1.
[5] H. Kiya, S. Imaizumi, and O. Watanabe, "Partial-scrambling of images encoded using JPEG2000 without generating marker codes," Proceedings of 2003 IEEE International Conference on Image Processing (ICIP 2003).
[6] Vania Conan, Yulen Sadourny and St-eve Thomann, "Symmetric Block Cipher Based Protection: Contribution to JPSEC," ISO/IEC JTC 1/SC 29/WG1 N2771, Oct. 2003
[7] S. Lian, et al., "A Selective Image Encryption Scheme Based on JPEG2000 Codec," Proceedings of 5th Pacific Rim Conference on Multimedia. 2004: Springer.
[8] J. Fang and J. Sun, "A Format-Compliant Encryption Framework for JPEG2000 Image Code-Streams in Broadcasting Applications," in Advances in Multimedia Information Processing - PCM 2006, Lecture Notes in Computer Science. 2006: Springer.