A Commutative Scheme of Perceptual Cryptography and Image Compression for JPEG 2000

Shenchuan LIU, Masaaki FUJISHOSI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan
Tel: +81–42–585–8454
E-mail: liu-shenchuan@sd.tmu.ac.jp, mfujiyoshi@m.ieice.org, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes a commutative scheme of perceptual cryptography and image compression for JPEG 2000 image coding standard. The commutative property of the proposed scheme allows to cipher a compressed image without interfering with image decompression and or to compress a encrypted images still allowing a perfect deciphering. The conventional schemes having the same feature use proprietary compression techniques, whereas the proposed scheme suits JPEG 2000. In the proposed scheme, the encryption strength can be controlled a parameter, and the visibility of the encrypted and compressed image can be changed according to DWT levels. The advantages of the proposed scheme are 1) better compression performance and 2) usage of an international standard and its reliable implementation. Moreover, the image can be decrypted even from lossy compressed one. Experimental results show the effectiveness of the proposed scheme**

I. Introduction

With the development of digital equipments, a lot of digital images and videos boost on the Internet. In many practical scenarios, multimedia data need to be encrypted before being transmitted over the Internet. At the same time, multimedia data are need to be compressed due to the limited bandwidth. So, compression of encrypted data has attracted considerable research interest. In order to meet the two needs, many schemes have been proposed [1]–[3].

If an encryption is done properly, the encrypted data becomes random data for which most comression techniques cannot gain good performance. So, classical ways firstly compress multimedia data to reduce the redundancy, and then encrypt the compressed data. However, it has been shown that, based on the theory of source coding with side information at the decoder, the efficiency of compressing encrypted data may be as good as that of compressing non-encrypted data in theory [4].

As for images, lossless [5] and lossy [6] schemes have been proposed for encrypting images while compressing them as much as possible: These schemes try to generate nearly random images to reduce the possibility of recognizing the original image. In another application in which partially encrypted or low quality images are generated for preview, perceptual cryptography schemes have been proposed for JPEG compressed images [7] and for Embedded Zerotree Wavelet (EZW) and Set Partitioning In Hierarchical Trees (SPIHT) [8].

This paper proposes a new perceptual cryptography scheme based on JPEG 2000. Similar to the conventional scheme [8], the proposed scheme encrypts an image by random sign inversion of discrete wavelet transformed (DWT) coefficients, which DWT is used in JPEG 2000, EZW, and SPIHT. The advantages of the proposed method are 1) better compression performance of encrypted images and 2) usage of an international standard and its reliable implementation instead of a proprietary technique and implementation. It is noted that the proposed method decrypts an image even from encrypted and lossy compressed images.

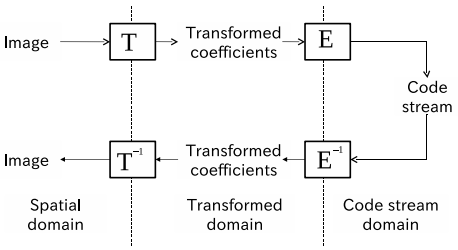


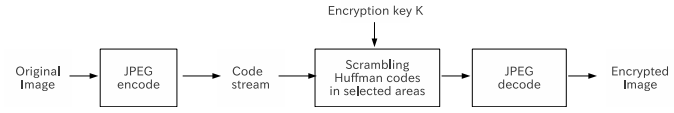
Fig. 1. Transform image coding (T: transformation, E: entropy encoding, T^{-1}: inverse transformation, E^{-1}: entropy decoding).

The rest of the paper is arranged as follows. In Section II, the conventional schemes will be reviewed. The new scheme is proposed in Section III. Experimental results are showed in Section IV, and conclusions and future work are given in Section V.

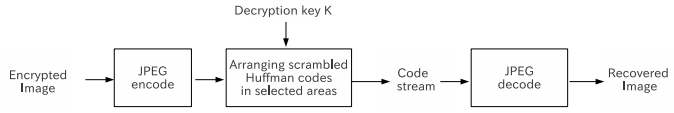
II. Conventional Schemes

This section briefly describes two conventional encryption and compression schemes for images; one for JPEG [7] and the other for EZW and SHIPT [8]. According to Fig. 1, these schemes encrypt images in the codestream [7] and transformed [8] domains, respectively. Moreover, the former is non-separable [9], but the latter is commutative [10].

Figure 2 shows the block diagram of the conventional scheme for JPEG [7]. As shown in Fig. 2 (a) for the process of compression and encryption, the discrete cosine transformation (DCT) is firstly applied to an original image, and the transformed coefficients are quantized based on user defined quality parameter Q. Quantized coefficients are then encoded by a Huffman encoder to form a JPEG codestream. In the codestream, the Huffman codes of selected areas of the image are scrambled by using encryption key K. The encrypted image is obtained by applying inverse DCT to the Huffman decoded



(a) Encryption and compression.



(b) Decryption and decompression.

Fig. 2. Block diagram of the conventional scheme for JPEG [7] in which images are encrypted in the codestream domain. This scheme is non-separable [9] in which the operation order is fixed.

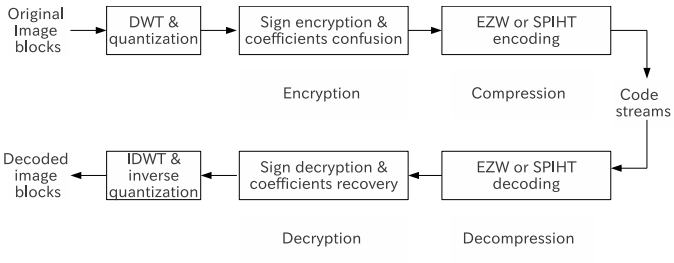


Fig. 3. Block diagram of the conventional scheme for EZW and SPHIT codec [8] in which images are encrypted in the transformed domain. This scheme is commutative [10] in which encryption and compression are commutative.

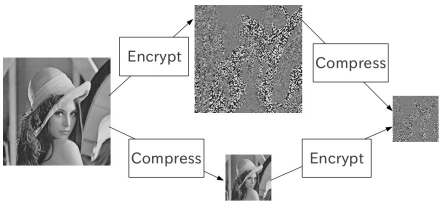
codestream.

It is noted that compression must be done first, and then encryption can be processed in this scheme, as shown in Fig. 2 (a). Figure 2 (b) shows the process of decryption and decompression in which the encrypted image is processed in the opposite way. It is noted again that the process order is strictly fixed: The decryption must be done first, and then the decompression can be processed in this scheme. It is non-separable [9].

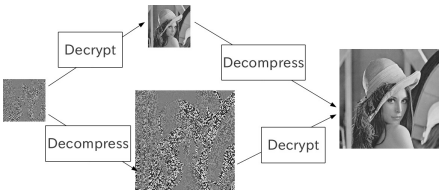
Figure 3 shows the block diagram of conventional scheme for EZW and SPHIT [8]. In this scheme, an original image is processed block-by-block. An image block is transformed by DWT and quantized, and then the encryption mechanism is applied to DWT coefficients. The encryption consists of two steps: The former is sign encryption and the latter is coefficients confusion based on quad-tree. Finally, applying EZW or SPIHT compression to the encrypted coefficients, the encrypted codestream can be obtained.

Vice versa, after applying EZW or SPIHT decoding, sign decryption and coefficients recovery are applied to the decoded coefficients for decryption, and, then, inverse quantization and DWT generate a decoded image block. It is noted that this scheme is *commutative* [10]; after applying DWT to an original image to encrypt the transformed coefficients, the inverse DWT generate the encrypted image. This encrypted image, then, can be compressed by DWT-based EZW or SPHIT.

In the next section, a new commutative scheme of perceptual cryptography and image compression for JPEG 2000 is proposed.



(a) Encryption and compression.



(b) Decryption and decompression.

Fig. 4. The proposed scheme. This scheme is a commutative perceptual encryption and image compression for JPEG 2000.

III. PROPOSED SCHEME

This section proposes a new commutative compression and encryption scheme for JPEG 2000.

A. System Overview

In the proposed scheme, an original image is firstly transformed into the DWT domain. Then, perceptual cryptography and compression can be done without considering the processing order, i.e., the proposed scheme encrypts images in the transformed domain. As shown in Fig. 4, an encrypted and compressed image can be decrypted firstly, then be decompressed to recover the image. Also, the encrypted and compressed image can be decompressed firstly, then be decrypted to recover the image. In other words, the proposed scheme is commutative which the scheme offers a flexibility in processing order of two techniques.

In the next section, algorithms for perceptual encryption and compression in the proposed scheme will be described in detail.

B. Perceptual Encryption and Compression

Even perceptual encryption and compression are commutative in the proposed scheme, algorithms are described in the order of perceptual encryption and compression.

1) Perceptual Encryption: The proposed scheme perceptually encrypts an image by randomly inverting the positive and negative sign of DWT coefficients of the image, viz., sign encryption.

Step 1. A user set the parameter for encryption strength, n, to an integer between 1 and 50, and key matrix K is generated in which n percentage of elements are -1's and the remaining elements are 1's.

Step 2. Image I is transformed into DWT domain. The two dimensional DWT coefficients of image I are divided into positive and negative sign matrix S and its corresponding magnitude matrix M.

Step 3. Randomly invert n percentage of sign matrix S by multiplying key matrix K to get encrypted matrix S', i.e., $S' = S \circ K$ where $\circ$ represents Hadamard product.

Step 4. Encrypted sign matrix S' and magnitude matrix M compose encrypted DWT coefficients, and the coefficients are inversely transformed to form perceptually encrypted image I'.

2) Compression: Standard JPEG 2000 compression is used in this scheme. Let $\hat{M}$ be the magnitude matrix of the compressed image, while M is the magnitude matrix of the original image. JPEG 2000 quantizes DWT coefficients by the bit truncation and it mainly affects magnitude M. So, $\hat{M}$ can be represented as $\hat{M} = f(M)$ where $f(\cdot)$ stands for standard JPEG 2000 compression. It is noted that the bit truncation of JPEG 2000 compression drops bits from the least significant bit (LSB) to the most significant bit (MSB), so it does not change signs at all. Consequently, the coefficients of the encrypted and compressed image can be represented as $S' \circ \hat{M}$, whereas those of a compressed image are $S \circ \hat{M}$.

C. Decryption and Decompression

Though decryption and decompression are also commutative, this section firstly describes decryption algorithm and then it mentions decompression.

1) Decryption:

Step 1. Perceptually encrypted image I' is transformed into the DWT domain. The two dimensional DWT coefficients are divided into encrypted sign matrix $S1$ and magnitude matrix $M1$.

Step 2. Flip the n percentage of signs in $S1$ by multiplying key matrix K to get decrypted matrix $S1'$, i.e., $S1' = S1 \circ K$.

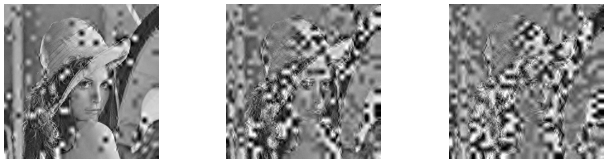
Step 3. Decrypted DWT coefficients are compound of decrypted sign matrix $S1'$ and magnitude matrix $M1$, and decrypted image $I1'$ can be obtained by the inverse transformation of the coefficients.

2) Decompression: According to the compression in section III-B2, the corresponding standard JPEG 2000 decompression is applied to compressed images in the proposed scheme. It is noted that the decompression of JPEG 2000 neither changes magnitude matrix $M1$ nor the sign matrix.

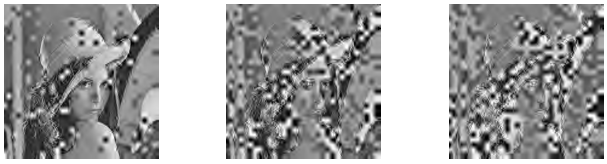
D. Features

This section summarizes the three main features of the proposed scheme, namely commutative perceptual cryptography and image compression, either separated or joint, and adoption of JPEG 2000.

1) Commutative: The sign encryption and JPEG 2000 compression are used in the proposed scheme, and these techniques won't affect each other as described in Section III-B2. So, these techniques can be commutative as in the conventional scheme [8]. From an encrypted and compressed image, a user can obtain either the decrypted but compressed codestream, uncompressed but encrypted image, and decrypted or uncompressed and decrypted image, based on his/her authority.



(a) $n = 10$ (4.379 bpp). (b) $n = 30$ (4.410 bpp). (c) $n = 50$ (4.414 bpp).
Lossless compression.



(d) $n = 10$. (e) $n = 30$. (f) $n = 50$.
Lossy compression (0.08 bpp).

Fig. 5. Encrypted and compressed Lena (4-level DWT).

2) Separated or Joint: Even the sign encryption and JPEG 2000 compression are separately described in Fig. 4 (b) and Section III-B, these techniques can be jointly applied to images in the proposed scheme.

Step 1. A user set n to an integer between 1 and 50, and key matrix K.

Step 2. Image I is transformed into DWT domain, and the two dimensional DWT coefficients are divided into sign matrix S and magnitude matrix M.

Step 3. Randomly invert n percentage of sign matrix S by $S' = S \circ K$.

Step 4. Matrices S' and M compose the encrypted DWT coefficients, and the coefficients are entropy encoded to form the encrypted JPEG 2000 codestream.

Decoding and decryption also can be jointly applied to the encrypted codestream.

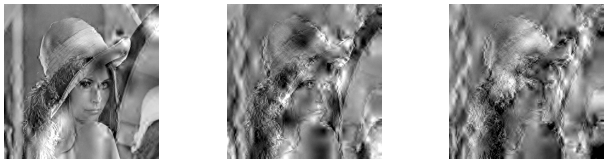
3) Adoption of JPEG 2000: The proposed scheme adopts JPEG 2000 as its compression technique, which JPEG 2000 is an international standard for image compression. This makes the proposed scheme compatible to the international standard and based on the reliable implementation.

IV. Experimental Results

Figures 5 and 6 show the perceptually encrypted and compressed images where 4- and 6-level DWT decomposition for encryption, respectively. It was confirmed that the visual quality of the encrypted image decreases as n becomes larger. It was also confirmed that different visual quality can be obtained by choosing different DWT decomposition level.

The compression ratio of the lossless compression of original, i.e., unencrypted, "Lena" by JPEG 2000 is 4.317 bits/pixel, and that of encrypted with 4- and 6-level DWTs are 4.379 and 4.350 bpps, respectively. So, it was found that the encryption of the proposed scheme affects the compression efficiency slightly.

Table I shows the PSNRs of decrypted and decompressed images of Lena in which $n = 0$ is for the unencrypted images,



(a) $n = 10$ (4.350 bpp). (b) $n = 30$ (4.380 bpp). (c) $n = 50$ (4.373 bpp). Lossless compression.

(d) $n = 10$. (e) $n = 30$. (f) $n = 50$. lossy compression (0.08 bpp).

Fig. 6. Encrypted and compressed Lena (6-level DWT).

TABLE I
THE PSNRS OF DECRYPTED AND DECOMPRESSED LENA IN THE PROPOSED SCHEME.

Encryption strength n	DWT level	Compression ratio [bits/pixel] 8	0.8	0.4	0.2	0.08
0	—	∞	43.31	39.20	36.53	33.93
10	4	53.68	41.91	38.83	36.26	33.71
30		48.77	41.09	38.56	36.08	33.64
50		46.62	40.94	38.47	36.07	33.69
10	6	44.95	41.99	39.02	36.32	33.91
30		43.89	40.58	38.30	36.15	33.81
50		44.09	40.33	38.29	36.12	33.71

and Fig. 7 shows some tangible examples. It was confirmed that the degradation brought by proposed perceptual cryptography is very small, even the image is lossy compressed. So, it concludes that the proposed perceptual encryption can survive even in highly compressed images.

Table II shows the compression performance of sign encrypted images in the conventional [8] and proposed schemes. As it is described in scheme [8], SHIPT is an upgrade of EZW.

(a) Original. (b) $n = 0$ (unencrypted), 0.08 bpp (PSNR: 33.93 dB).

(c) $n = 10$ (33.91 dB). (d) $n = 30$ (33.81 dB). (e) $n = 50$ (33.71 dB). Lossy compression (0.08 bpp), encryption with 6-level DWT.

Fig. 7. Decrypted and decompressed Lena.

TABLE II
THE COMPRESSION RATIO (BPP) OF SIGN ENCRYPTED AND LOSSLESSLY COMPRESSED IMAGES IN THE CONVENTIONAL (SHIPT) [8] AND PROPOSED SCHEMES.

Encryption strength n	DWT level	Scheme	Images lena	airplane	peppers
30	4	Conventional	4.61	4.24	4.81
		Proposed	4.41	3.99	4.58
50		Conventional	4.59	4.23	4.77
		Proposed	4.41	4.10	4.60
	6	Conventional	4.50	4.20	4.70
		Proposed	4.37	4.05	4.54

It was found that the proposed scheme with JPEG 2000 is best in terms of the compression ratio.

V. CONCLUSIONS

This paper has proposed a commutative perceptual cryptography and compression scheme for international standard JPEG 2000, whereas the conventional scheme [8] uses proprietary compression techniques. The commutative property of the proposed scheme allows to encrypt compressed images and to compress encrypted images. The proposed scheme is superior to the conventional scheme [8] in terms of compression performance even images are encrypted.

Future works include the improvement in the PSNR of decrypted and decompressed images while keeping the compression ratio low.

ACKNOWLEDGMENT

This work has been partially supported by the Grand-in-Aid for Scientific Research (C), No.24560468, from the Japan Society for the Promotion of Science.

REFERENCES

[1] J.M. Shapiro, "Embedded image coding using zerotrees of wavelets coefficients," *IEEE Trans. Signal Process.*, vol.41, pp.3445–3462, Dec. 1993.

[2] A. Said and W.A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Image Process.*, vol.5, pp.1303–1310, Sep. 1996.

[3] H. Cheng and X.B. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol.48, pp.2439–2451, Aug. 2000.

[4] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol.52, pp.2992–3006, Oct. 2004.

[5] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in *Proc. EURASIP EUSIPCO*, 2008.

[6] X.P. Zhang, "Lossy compression and iterative reconstruction for encrypted Image," *IEEE Trans. Inf. Forensics and Security*, vol.6, pp.–, Mar. 2011.

[7] T. Andres and M. Francisco, "Perceptual cryptography of JPEG compressed images on the JFIF bit-stream domain," in *Proc. IEEE ISCE*, 2003, pp.58–59.

[8] S.G. Lian, J.S. Sun, and Z.Q. Wang, "Perceptual cryptography on SPIHT compressed images or videos," in *Proc. IEEE ICME*, 2004, pp.III-2195–III-2198.

[9] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics and Security*, vol.7, pp.826–832, Apr. 2012.

[10] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natalee, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Process.: Image Commun.*, vol.26, pp.1–12, Jan. 2011.