2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

Effects of Random Sign Encryption in JPEG 2000-Based Data Hiding

Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA
Department of Information and Communication Systems,
Tokyo Metropolitan University,
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan
E-mail: saetang-wannida@ed.tmu.ac.jp, mfujiyoshi@ieee.org, kiya@tmu.ac.jp.

***Abstract*—This paper proposes random sign encryption in JPEG 2000-based data hiding. By multiplying random signs to the discrete wavelet transformed coefficients of an image, the image is visually encrypted. Full and partial random sign encryption is studied in this paper, and effects of both are investigated. From experimental results, both full and partial random sign encryption does not degrade the quality of compressed images. In addition, the compression ratio can still be controlled well when random sign encryption is applied. Moreover, partial random sign encryption is enough for image visual encryption. With data hiding, random sign encryption does not degrade the quality of images containing hidden data, and 100% correct hidden data extracting rate has been achieved.**

***Keywords*-partial encryption; privacy protection; reversible data hiding; image compression;**

I. Introduction

Recently, the growth in multimedia has been phenomenal because of rapid growth of the Internet. Data hiding techniques which insert data to media documents such as images [1], [2] help the development of applications in some aspects. A number of data hiding techniques have been proposed for images and videos regarding to compression in various applications such as multimedia management [3], copyright protection [4], [5], error concealment [6], [7], and so on.

Anyway, privacy protection is desired in some multimedia applications [8], [9]. In those applications, images are visually protected. In some works [10], [11], privacy protection has been studied simultaneously with the data hiding. Furthermore, the combination of data hiding, compression, and image visual protection is desired in future applications.

This paper proposes random sign encryption in JPEG 2000-based data hiding. By multiplying random signs to the discrete wavelet transformed coefficients of an image, the image is visually encrypted. Full and partial random sign encryption is studied in this paper, and effects of both are investigated.

The rest of this paper is organized as follows. Section II describes a data hiding method for encrypted JPEG 2000 code streams. Section III gives the definitions of full random sign encryption and partial random sign encryption. Experimental results and discussions are given in section IV. Finally, section V concludes this paper.

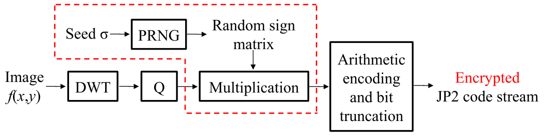

Seed σ
PRNG
Random sign matrix
Image f(x,y)
DWT
Q
Multiplication
Arithmetic encoding and bit truncation
Encrypted JP2 code stream

Figure 1. Image compression by JPEG 2000, where a dash box indicates random sign encryption (DWT: discrete wavelet transformation, Q: quantization, PRNG: pseudo random number generator).

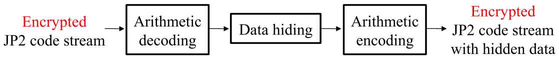

Encrypted JP2 code stream
Arithmetic decoding
Data hiding
Arithmetic encoding
Encrypted JP2 code stream with hidden data

Figure 2. Data hiding in JPEG 2000 code streams.

II. JPEG 2000-Based Data Hiding

Fig. 1 shows the image compression using JPEG 2000 [12] performed by the image owner. In cases of lossless compression, the image is transformed to the discrete wavelet transformed (DWTed) domain, and then arithmetic encoding is performed. In cases of lossy compression, DWT coefficients are quantized, and then the arithmetic encoding with bit truncation is performed. The JPEG 2000 code streams are then sent to the data hider. They are subsequently arithmetically decoded, and then the data is hidden into the DWT coefficients or quantized DWT coefficients for lossy compression. Finally, the DWT coefficients containing the hidden data is arithmetically encoded without bit truncation to obtain the JPEG 2000 code streams containing the hidden data as shown in Fig. 2.

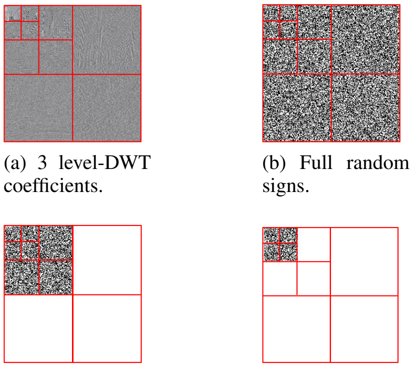
III. Random Sign Encryption in JPEG 2000-Based Data Hiding

This section proposes random sign encryption in JPEG 2000-based data hiding.

A. Encryption and Data Hiding

Fig. 1 shows random sign encryption in JPEG 2000 by a dash box. The image is visually encrypted by multiplying a random sign matrix, which is generated by a pseudo random number generator (PRNG) and which consists of 1 and -1, to DWT coefficients or quantized DWT coefficients for lossy compression. Then, the arithmetic encoding is performed to obtain the encrypted JPEG 2000 code streams. For data

978-1-4799-5390-5/14 $31.00 © 2014 IEEE
DOI 10.1109/IIH-MSP.2014.134



(a) 3 level-DWT coefficients.

(b) Full random signs.

(c) Quarter random signs.

(d) 1/16 random signs.

Figure 3. Random sign encryption.

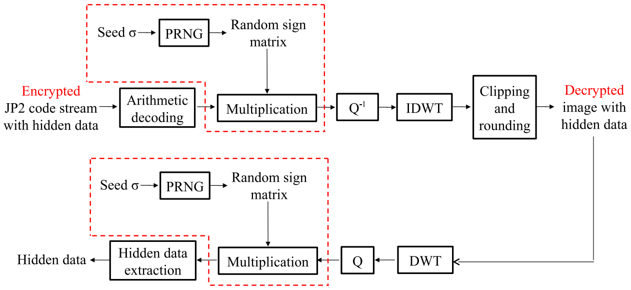


Figure 4. Image decryption and hidden data extraction. (Q^{-1}: inverse quantization, IDWT: inverse discrete wavelet transformation).

hiding, the process is the same as described in Section II, but the data hider has no information to see the image.

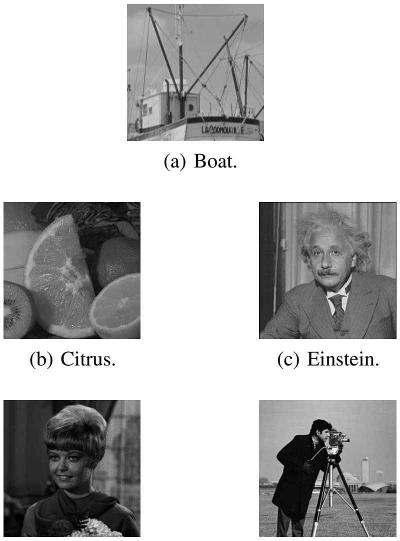
Random sign encryption is divided into two types: full and partial random sign encryption.

1) Full Random Sign Encryption: By using full random sign encryption, every DWT coefficient is multiplied by a random sign. Fig. 3 (a) shows 3 level-DWT coefficients of "Boat," and Fig. 3 (b) shows full random signs.

2) Partial Random Sign Encryption: Instead of full random sign encryption, partial random sign encryption can be used to visually encrypt the image as shown in Fig. 3 (c) and (d). Top-left coefficients or low frequency bands are encrypted.

B. Decryption and Hidden Data Extraction

There are a number of applications in aspect of image decryption and hidden data extraction. The image can be decrypted even if the user does not know the information to extract the hidden data. The image is decrypted by using the same random sign matrix as used in the encryption process. On the other hand, another user can extract the hidden data even if he/she does not have the authority to see the image, i.e., the image is not decrypted. In addition, if the user is allowed for both image vision and hidden data extraction, he/she can select the order of process. This paper focuses on the application that the image is decrypted before extracting the hidden data as illustrated in Fig. 4.



(a) Boat.

(b) Citrus.

(c) Einstein.

(d) Girl.

(e) Cameraman.

Figure 5. Test images.

100% correct hidden data extraction is not guaranteed theoretically because the hidden data may be distorted by clipping and rounding once the image is decrypted and decoded. However, by using a correlation detector, 100% correct hidden data extraction can be obtained as confirmed in the next section.

IV. Experimental Results

Random sign encryption is evaluated in terms of image visual protection, quality of the decrypted image without data hiding, quality of the decrypted image containing the hidden data, and data hiding performance.

A. Materials and Tools

1) Materials: Five 256×256 pixel-sized gray images shown in Fig. 5 are used in the experiment. JASPER [13] which is a JPEG 2000-based software is applied in the experiment.

2) Data Hiding Technique: This paper uses a simple non-blind additive digital data hiding technique in the DWT domain which is based on the essence of [14]. A hidden data is extracted by a correlation-based detector.

$X \times Y$-sized visually protected DWT coefficients are firstly divided into $X_B \times Y_B$ coefficient-blocks where $X_B = Y_B = 8$ in the experiments. Then, an XY/X_BY_B-sized binary hidden data sequence is generated. Each single bit of the hidden data, $b \in \{0, 1\}$, is represented by an M-sequence, where the length of M-sequences used in the experiments is the smallest, i.e., $L = 3$, even longer sequences serve better correct hidden data extracting rate.

M-sequences differ from each other for different single bits of the hidden data. Each M-sequence is subsequently embedded to a divided block of visually protected DWTed coefficients by linearly scaling and adding it to three bottom-right coefficients of the block as

$$C'_l = \mathrm{sgn}\left(C_l\right)\left(|C_l| + \delta W_{b,l}\right), \tag{1}$$

where C'_l denotes the l-th visually protected DWTed coefficient containing the hidden data in the block, C_l denotes the l-th original visually protected DWTed coefficient, δ is a scaling factor for data hiding, and $W_{b,l} \in \{0,1\}$ denotes the l-th chip of the M-sequence for bit b in a coefficient block where $l = 1, 2, \ldots, L$. It is noted that all variables in Eq. (1) are integers regardless of lossy/lossless compression. The image is reconstructed before extracting hidden data where the hidden data bit is extracted by a correlation-based detector as

$$b' = \arg\max_{b\in\{0,1\}} \sum_{l=1}^{L} \left(W_{b,l} - 0.5\right)\left(\frac{|C''_l| - |C_l|}{\delta} - 0.5\right), \tag{2}$$

where b' is an extracted hidden data bit, and $|C''_l|$ denotes the l-th fingerprinted and visually protected DWTed coefficient in the block obtained after reconstructing the fingerprinted image, applying DWT, and random sign scrambling again. It is noted that $|C''_l|$ may be different from $|C'_l|$ by clipping errors in JPEG 2000 decoding performed by the consumer, since digital fingerprinting could make the intensity range of the fingerprinted image over $[0, 255]$. However, the data hiding technique is still flexible for the proposed system, i.e., any DWT-based data hiding technique could be applied.

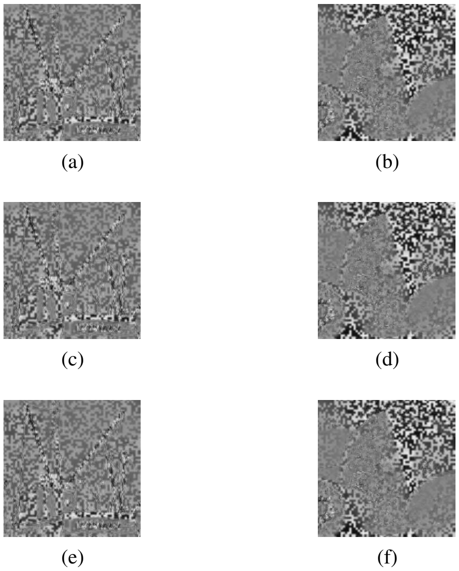
3) Encryption Conditions: 3 level-DWT is used in the experiment, while 3 cases of random sign encryption are evaluated: 1). Full random sign encryption, 2). Quarter random sign encryption, and 3). 1/16 random sign encryption as shown in Fig. 3.

B. Image Visual Protection Performance

Fig. 6 shows the encrypted images decompressed by using standard JPEG 2000 for lossless compression mode without data hiding. The results show that the random sign encryption, even the partial random sign encryption is effective in terms of visual protection.

C. Compression Performance

Here, the compression performance of random sign encryption-based JPEG 2000 is evaluated in terms of peak signal-to-noise ratios (PSNRs) of decrypted images. Tables I shows the results of 3 cases of random sign encryption comparing to that of the standard JPEG 2000 without encryption. The results confirm that random sign encryption does not degrade the compression performance of JPEG 2000. In addition, the compression ratio can still be controlled well when random sign encryption is applied.



(a) (b)

(c) (d)

(e) (f)

Figure 6. Visually protected images for "Boat" (left) and "Citrus" (right). First row: full random signs (seed $\sigma = 13$), Second row: quarter random signs (seed $\sigma = 13$), and third row: 1/16 random signs (seed $\sigma = 13$).

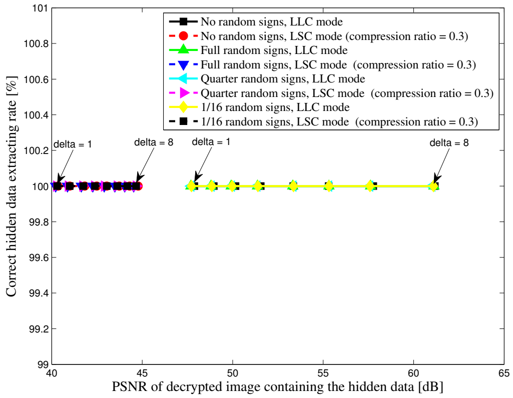


Figure 7. PSNR of the decrypted image containing the hidden data-correct hidden data extracting rate curves, where the scaling factor for data hiding, δ is varied from 1 to 8 with stepping by 1 (LLC: lossless compression, LSC: lossy compression).

D. Quality of Decrypted Images Containing Hidden Data and Data Hiding Performance

This section evaluates the quality of decrypted images containing hidden data in terms of PSNR and the data hiding performance in terms of correct hidden data extracting rate. As shown in Fig. 7, the results confirm that both full and partial random sign encryption maintains high quality of images containing hidden data, and the hidden data are extracted without errors in any case thanks to the correlation-based detector. For lossy compression, even though the image quality becomes lower, 100% correct hidden data extracting rate can also be achieved, because only arithmetic

Table I
COMPRESSION PERFORMANCE OF RANDOM SIGN ENCRYPTION-BASED JPEG 2000 WITHOUT DATA HIDING.

Compression ratio	0.1	0.2	0.3	0.4
PSNR [dB]	36.9357	41.9412	44.9435	47.8714
File size [Byte]	6521	13104	19401	25695
Compression ratio	0.5	0.6	0.7	Lossless
PSNR [dB]	51.93	60.5172	60.5172	Inf
File size [Byte]	32463	35016	35016	35646

(a) Standard JPEG 2000 without encryption.

Compression ratio	0.1	0.2	0.3	0.4
PSNR [dB]	36.1177	41.555	44.6703	47.5668
File size [Byte]	6403	13001	19407	25888
Compression ratio	0.5	0.6	0.7	Lossless
PSNR [dB]	51.397	60.5172	60.5172	Inf
File size [Byte]	32704	35950	35950	36579

(b) Full Random Sign Encryption-Based JPEG 2000.

Compression ratio	0.1	0.2	0.3	0.4
PSNR [dB]	36.1177	41.755	44.8155	47.8714
File size [Byte]	6213	13092	19457	26148
Compression ratio	0.5	0.6	0.7	Lossless
PSNR [dB]	51.397	60.5172	60.5172	Inf
File size [Byte]	32230	35475	35475	36105

(c) Quarter Random Sign Encryption-Based JPEG 2000.

Compression ratio	0.1	0.2	0.3	0.4
PSNR [dB]	36.1177	41.755	44.8155	47.8714
File size [Byte]	6157	13014	19361	26039
Compression ratio	0.5	0.6	0.7	Lossless
PSNR [dB]	51.397	60.5172	60.5172	Inf
File size [Byte]	32121	35360	35360	35990

(d) 1/16 Random Sign Encryption-Based JPEG 2000.

encoding without bit truncation is performed after data hiding.

V. CONCLUSIONS

Full and partial random sign encryption is studied in this paper. From experimental results, both full and partial random sign encryption does not degrade the quality of compressed images. In addition, the compression ratio can still be controlled well when random sign encryption is applied. Moreover, partial random sign encryption is enough for image visual encryption. With data hiding, random sign encryption does not degrade the quality of images containing hidden data, and 100% correct hidden data extracting rate has been achieved for any case.

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] H. Cao and A. Kot, "On establishing edge adaptive grid for bi-level image data hiding," in *IEEE Trans. Information Forensics and Security*, 2013.

[2] Wang, Xing-Tian, C.C. Chang, T.S. Nguyen, and M.C. Li, "Reversible data hiding for high quality images exploiting interpolation and direction order mechanism," in *Digital Signal Processing*, 2013, pp.569–577.

[3] H. Kiya, Y. Noguchi, A. Takagi, and H. Kobayashi, "A method of inserting binary data into MPEG bitstreams for video index labeling," in *Proc. IEEE ICIP*, 1999.

[4] D. Rosiyadi, S.J. Horng, P. Fan, X. Wang, M.K. Khan, and Y. Pan, "Copyright protection for e-government document images," in *MultiMedia, IEEE*, 2012, pp.62–73.

[5] K. Deb, M. Al-Seraj, M. Hoque, M. Sarkar, and I. Hasan, "Combined DWT-DCT based digital image watermarking technique for copyright protection," in *Proc. IEEE ICECE*, 2012, pp.458–461.

[6] M. Ebian, M. E.-Sharkawy, and S. E.-Ramly, "Enhanced dynamic error concealment algorithm for multiview coding based on lost MBs sizes and adaptively selected candidates MBs," in *Proc. Springer ICSIP*, 2013, pp.435–443.

[7] A. Talari, S. Kumar, N. Rahnavard, S. Paluri, and J.D. Matyjas, "Optimized cross-layer forward error correction coding for H. 264 AVC video transmission over wireless channels," in *EURASIP Journal on Wireless Communications and Networking*, 2013, pp.1–13.

[8] Z. Erkin, T. Veugen, T. Toft, and R.L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," in *IEEE Trans. Inform. Forensics Security*, 2012, vol.7, no.3, pp.1053–1066.

[9] R.L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol.30, no.1, pp.82–105, Jan. 2013.

[10] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," in *SPIE Opt. Eng.*, vol.45, pp.080 510-1–080 510-3, Aug. 2006.

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

[12] D. Taubman and M. Marcellin Eds., "JPEG2000 image compression fundamentals, standards and practice," *The Springer International Series in Engineering and Computer Science*, vol.642, 2002.

[13] M.D. Adams and F. Kossentini, "JASPER: A Software-based JPEG-2000 codec implementation," in *Proc. IEEE ICIP*, 2000, pp.53–56.

[14] S. Pereira, S. Voloshynoskiy, and T. Pun, "Optimal transform domain watermark embedding via linear programing," *Signal Processing 81*, pp.1251–1260, 2001.