Technical Note

An Improved QIM-JPEG2000 Steganography and Its Evaluation by Steganalysis

Takayuki Ishida,[†1] Kazumi Yamawaki,[†1]
Hideki Noda[†1] and Michiharu Niimi[†1]

This paper presents a modified QIM-JPEG2000 steganography which improves the previous JPEG2000 steganography using quantization index modulation (QIM). It does not increase the post-embedding file size, producing less degraded stego images. Steganalysis experiments show that the modified QIM-JPEG2000 is more secure than the previous QIM-JPEG2000 and is the most secure among major steganographic methods for JPEG2000 ever proposed.

1. Introduction

Steganography is the process of hiding secret data in an innocent looking container. This container may be a digital still image, audio file, or video file. Once the data has been embedded, it may be transferred across insecure lines or posted in public places. Therefore, the container should seem innocent under most examinations. On the other hand, steganalysis is the task of attacking steganographic systems. Considering the aim of steganography, it might be sufficient if an attacker can only detect the presence of hidden data in a container. The main requirement of steganography is undetectability, which means that no steganalysis algorithm should exist that can determine whether data is embedded in a given container.

In steganography using digital images, data embedding into compressed images should be primarily considered, since images are usually compressed before being transmitted. JPEG compression using the discrete cosine transform (DCT) is now the most common compression standard for still images, and therefore many steganographic methods have already been proposed for JPEG images, including Refs. 1)–6). Several steganalysis methods for JPEG steganography have also been proposed to detect whether messages are embedded or not in a JPEG image [2),7)]. Steganalysis methods in Refs. 2), 7) exploit some changes in the histogram of quantized DCT coefficients caused by embedding. Steganalysis in Ref. 8) exploits higher order statistics as well as the first order statistics such as the histogram of DCT coefficients.

JPEG2000 using the discrete wavelet transform (DWT) is an upcoming image coding standard which has improved features over JPEG and is expected to be used widely. Since steganographic methods for JPEG2000 images might be commonly used in the near future, development of secure JPEG2000 steganography will be required soon. Among already proposed JPEG2000 steganographic methods [9)–11)], QIM-JPEG2000 steganography [11)], which uses quantization index modulation (QIM) [12)] in the DWT domain, has a significant feature in that it approximately preserves the histograms of the quantized DWT coefficients. The histogram preservation should be a necessary requirement for secure JPEG2000 steganography since steganalysis for JPEG2000 steganography is likely to first exploit histogram changes by embedding. QIM-JPEG2000 steganography, however, has a drawback in that the file size of a post-embedding stego image increases significantly compared with that of the corresponding cover image; the increase in file size is much more than the size of the embedded data. The increase in stego image size is not considered to be directly related to the detectability of the presence of hidden data, since steganography assumes that an attacker cannot access the original cover image. However, excessive increase in file size is not desirable since it negates the advantage of embedding information as opposed to appending it [13)].

This paper presents a modified QIM-JPEG2000 steganography which does not increase the post-embedding file size while still keeping the post-embedding histogram almost unchanged. It is realized by embedding data without changes of quantized DWT coefficients between 0 and ±1. As a by-product, this modification produces less degraded stego images and reduces detectability by steganalysis, i.e., it improves the security of JPEG2000 steganography.

[†1] Kyushu Institute of Technology

2. QIM-JPEG2000 Steganography

In this section, we briefly review QIM-JPEG2000 steganography[11]. In QIM-JPEG2000 steganography, QIM[12] with two different quantizers is used to embed binary data at the quantization step of the DWT coefficients. Each bit (zero or one) of binary data is embedded in such a way that one of two quantizers is used for the quantization of a DWT coefficient, which corresponds to embedding a zero, while the other quantizer embeds a one. In the following discussion, it is assumed that the probabilities of zero and one are same in binary data to be embedded. This assumption is quite natural since any compressed data has such property.

Assuming that DWT coefficients belonging to a codeblock[⋆1] are divided by its quantization step size in advance, two codebooks, C^0 and C^1, for two quantizers can be defined as $C^0 = \{0,\ \pm(2j+0.5); j \in \{1,2,\ldots\}\}$ and $C^1 = \{\pm(2j+1.5); j \in \{0,1,2,\ldots\}\}$[⋆2] for all frequency subbands. Let N_i and N_{-i}, $i \in \{1,2,\ldots\}$ denote the number of DWT coefficients whose values w are in the interval $i \leq w < i+1$ and $-i-1 < w \leq -i$, respectively, and N_0 in the interval $-1 < w < 1$. Let N_i^L and N_i^H denote the number of DWT coefficients in the lower and upper half-intervals of N_i, respectively, and therefore $N_i^L + N_i^H = N_i$. After embedding by QIM, the histogram N_i is changed to $N_i^{'}$ as

$$N_i^{'} = \frac{1}{2}N_i + \frac{1}{2}\left(N_{i-1}^H + N_{i+1}^L\right). \tag{1}$$

Equation (1) indicates that if $N_i = N_{i-1}^H + N_{i+1}^L$, then the number in the bin i does not change. In particular for $i = 0, \pm 1$, however, much difference between N_i and $N_{i-1}^H + N_{i+1}^L$ causes the significant change on $N_i^{'}$ after embedding. That is, since N_0 is usually larger than N_1 and N_{-1}, the most significant changes are a decrease of N_0 and an increase of N_1 and N_{-1}. In order to preserve N_0, N_1 and N_{-1} after embedding, a dead zone for DWT coefficients w, $t_d^- < w < t_d^+$ $(-1 < t_d^- < 0 < t_d^+ < 1)$ is introduced, where DWT coefficients are not used for embedding. Let N_d^+ and N_d^- denote the number of positive and negative DWT coefficients in the dead zone, i.e., the number of coefficients in the interval $0 < w < t_d^+$ and $t_d^- < w < 0$, respectively. t_d^+ and t_d^- are determined by optimal N_d^+ and N_d^- values which minimize the histogram changes for the bins 0 and ±1. Note that in QIM-JPEG2000 steganography, the quantized coefficients 0s cannot be treated as having zeroes embedded in them, because they cannot be discriminated from the 0s in the dead zone. Also note that in the data extraction stage, information on the dead zone (t_d^+ and t_d^-) is not necessary and data extraction is simply carried out based on whether non-zero coefficients are even or odd.

3. Modified QIM-JPEG2000 Steganography

We investigate the reason why the file size of post-embedding image using QIM-JPEG2000 steganography increases significantly compared with that of its cover image. **Figure 1** (a) shows the relationship between the file size increase and the number of quantized DWT coefficients which changes from 0 to ±1 after embedding, and Fig. 1 (b) shows the relationship between the file size increase and the number of changes from ±1 to 0 after embedding. Figure 1 (c) shows the relationship between the file size increase and the increase of ±1 after embedding. Data in these figures are derived using eight standard images described in Section 4.1. These figures show that the file size increase is correlated with the number of changes between 0 and ±1 and is not correlated with the increase of ±1 after embedding. This evidence may indicate that the file size increase is caused by violating the adaptive encoding of the arithmetic encoder in JPEG2000 which considers the context of nearby pixels. That is, the change between 0 and ±1 by embedding is made independently of the context and it could cause the increase.

In order to avoid the changes of quantized DWT coefficients between 0 and ±1, we modify QIM-JPEG2000 as follows.

(1) DWT coefficients in the interval $-1 < w < 1$ whose quantized values are 0s are not used for embedding.

(2) For DWT coefficients in the interval $1 < w < 2$ and $-2 < w < -1$, dead zones, $1 < w < t_d^+$ and $t_d^- < w < -1$ $(1 < t_d^+ < 2,\ -2 < t_d^- < -1)$ are

[⋆1] The codeblock is a unit processing block in JPEG2000 coding. The quantization step size can be different from codeblock to codeblock.

[⋆2] In the codebooks, 0.5 is added to the absolute values of representatives except 0 corresponding to the reconstructed DWT coefficients during the decoding stage and the quantized DWT coefficients themselves are of course integers.

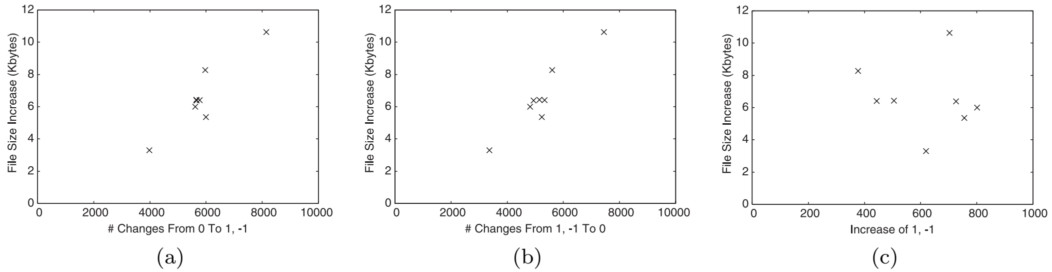


Fig. 1 File size increase by QIM-JPEG2000 steganography: (a) file size increase vs. the number of changes from 0 to ±1, (b) file size increase vs. the number of changes from ±1 to 0, (c) file size increase vs. increase of ±1.

introduced, where DWT coefficients are not used for embedding. The two dead zones are introduced to make histogram changes as small as possible for the bins 1 and 2 and for −1 and −2. The dead zones can be set in a similar way to one in the previous QIM-JPEG2000 [11]. For DWT coefficients outside the dead zones, half of the coefficients in $t_d^+ < w < 2$ and half of the coefficients in $-2 < w < t_d^-$ are quantized to 2 and −2, respectively, for embedding zeros.

Note that in the modified QIM-JPEG2000 steganography, quantized coefficients ±1s cannot be treated as ones embedded in them, because they cannot be discriminated from ±1s in the dead zones. Also note that in the data extraction stage, information on the dead zones (t_d^+ and t_d^-) is not necessary and data extraction is simply carried out based on whether coefficients other than 0 and ±1 are even or odd.

4. Experiments

4.1 General Performance Evaluation

The modified QIM-JPEG2000 was evaluated by comparing it with major steganographic methods for JPEG2000 ever proposed: the previous QIM-JPEG2000 [11], JPEG2000-BPCS [9], JPEG2000 steganography with lazy mode [10] and the least significant bit (LSB) flipping steganography. These methods were evaluated using eight standard images: Lena, Barbara, Mandrill, Airplane, Boat, Goldhill, Peppers, and Zelda (from http://sampl.eng.ohio-state.edu/˜sampl/database.htm). These images are 512 × 512 pixels in size, 8 bits per pixel (bpp) gray-scale images, and were compressed with 1 bpp as the pre-embedding target bit rate. The histogram change was measured by the Kullback-Leibler divergence [14]. Smaller KL divergence values represent better histogram preservation. Experiments were carried out 100 times for each image using different random data to be embedded. Experimental results are shown in **Table 1**, where each result is the mean value for eight images. Considering that the embedding capacity of the lazy mode JPEG2000 steganography is the smallest among the five methods evaluated, the size of the embedded data is adjusted to that of the lazy mode JPEG2000 steganography. The amount was adjusted by randomly selecting the DWT coefficients used for embedding. The KL divergence in the table has been averaged over three subbands (LH, HL, and HH subband) of the third-level of the five-level wavelet transform used. The third-level subbands are here selected considering the balance between the total number of DWT coefficients and the number of non-zero DWT coefficients in a subband.

Table 1 shows that file size increase is suppressed by the modified QIM-JPEG2000. Additionally, the modified QIM-JPEG2000 produces the highest PSNR stego images among the five methods. In the lazy mode JPEG2000 steganography, file size increase does not occur in principle since special bits for which arithmetic coding is bypassed are used for embedding. The KL divergence value for the modified QIM-JPEG2000 is comparable to that for the

Table 1 Results of embedding experiments where the size of the embedded data is adjusted to that of the lazy mode JPEG2000 steganography.

method	embedded data size (bytes)	compressed image size (bytes)	file size increase (bytes)	PSNR (dB)	KL divergence
(no embedding)	-	32,793	-	38.0	-
modified QIM-JPEG2000	1,867	33,144	352	37.4	0.0016
previous QIM-JPEG2000	1,866	36,221	3,428	36.4	0.0014
JPEG2000-BPCS	1,876	35,488	2,696	36.2	0.0041
lazy mode	1,866	32,756	38	33.0	0.0095
LSB	1,864	39,138	6,346	35.2	0.0119

previous QIM-JPEG2000, and those for the two QIM-based methods are much smaller than those for the other three methods.

4.2 Steganalysis

Steganalysis experiments were carried out to determine whether messages are embedded in JPEG2000 images. For the experiments, 500 natural images were used which are 8 bpp gray-scale images of 408 × 306 pixels in size and were compressed with 1 bpp as the pre-embedding target bit rate. A classifier using Fisher linear discriminant analysis [15] was used to classify whether a given image is a stego or cover image. Two kinds of features were used for the classifier: higher-order image statistics extracted from a wavelet decomposition [16] and histograms of wavelet coefficients. The former feature consists of 72 components which are the mean, variance, skewness and kurtosis of the wavelet coefficients at the three subbands of the first three (first to third) levels, as well as those of the errors in an optimal linear predictor of coefficient magnitude [16]. The latter consists of 55 components which represent the positive part of the histogram of wavelet coefficients, i.e., N_0 to N_{10} for all of five levels[⋆1].

Given 500 cover images, the corresponding stego images were generated by each of the above five methods described in Section 4.1. Randomly selected 250 cover images and the corresponding stego images were used for training the classifier, and the remaining 250 cover and 250 stego images were used for testing. At the training stage, the decision threshold for the classifier was set so that the false positive rate becomes 2%, i.e., correct detection rate for a cover image is 98%. Then the derived decision threshold was used in testing. Experiments were carried out 100 times using randomly selected images for training and testing, and the average of correct detection rates is shown in **Table 2**.

Table 2 Correct detection rates (%) in steganalysis experiments where the size of the embedded data is adjusted to that of the lazy mode JPEG2000 steganography.

	higher-order statistics		histograms	
method	cover	stego	cover	stego
modified QIM-JPEG2000	91.6	9.2	95.3	16.3
previous QIM-JPEG2000	92.5	20.3	94.4	25.0
JPEG2000-BPCS	93.7	33.4	95.5	74.1
lazy mode	91.3	12.2	96.0	92.7
LSB	93.5	64.2	96.2	76.9

Results in Table 2 show that regarding the features, steganalysis using histograms works better than that using higher-order statistics. Comparing the correct detection rates for a stego image by the five methods, it is confirmed that the modified QIM-JPEG2000 is more secure than the previous QIM-JPEG2000 and it is the most secure method among the five methods.

5. Conclusions

We have presented a modified QIM-JPEG2000 steganography which does not increase the post-embedding file size, while keeping the post-embedding histogram change comparable to that by the previous QIM-JPEG2000. Furthermore, post-embedding decrease of PSNR value by the modified QIM-JPEG2000 is smaller than that by the previous QIM-JPEG2000. Steganalysis experiments show that the modified QIM-JPEG2000 is more secure than the previous QIM-JPEG2000 and it is the most secure among the major steganographic methods considered for JPEG2000.

[⋆1] Considering nearly symmetrical shape of a histogram, negative part was omitted.

Acknowledgments This work was partly supported by Grants-in-Aid for Scientific Research (No.18360183).

References

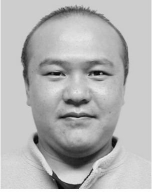
1) Upham, D.: http://ftp.funet.fi/pub/crypt/cypherpunks/steganography/jsteg/
2) Westfeld, A.: F5 – A steganographic algorithm: High capacity despite better steganalysis, *Lecture Notes in Computer Science*, Vol.2137, pp.289–302 (2001).
3) Provos, N.: Defending against statistical steganalysis, *10th USENIX Security Symposium* (2001).
4) Eggers, J.J., Bauml, R. and Girod, B.: A communications approach to image steganography, *Proc. SPIE*, Vol.4675, pp.26–37 (2002).
5) Sallee, P.: Model-based steganography, *Lecture Notes in Computer Science*, Vol.2939, pp.154–167 (2004).
6) Noda, H., Niimi, M. and Kawaguchi, E.: High performance JPEG steganography using quantization index modulation in DCT domain, *Pattern Recognition Letters*, Vol.27, pp.455–461 (2006).
7) Fridrich, J., Goljan, M. and Hogea, D.: New methodology for breaking steganographic techniques for JPEGs, *Proc. SPIE*, Vol.5020, pp.143–155 (2003).
8) Fridrich, J.: Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes, *Lecture Notes in Computer Science*, Vol.3200, pp.67–81 (2004).
9) Noda, H., Spaulding, J., Shirazi, M.N. and Kawaguchi, E.: Application of bitplane decomposition steganography to JPEG2000 encoded images, *IEEE Signal Processing Letters*, Vol.9, No.12, pp.410–413 (2002).
10) Su, P.C. and Kuo, C.C.J.: Steganography in JPEG2000 compressed images, *IEEE Trans. Consumer Electronics*, Vol.49, No.4, pp.824–832 (2003).
11) Noda, H., Tsukamizu, Y. and Niimi, M.: JPEG2000 steganography which preserves histograms of DWT coefficients, *IEICE Trans. Information and Systems*, Vol.E90-D, No.4, pp.783–786 (2007).
12) Chen, B. and Wornell, G.W.: Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Information Theory*, Vol.47, No.4, pp.1423–1443 (2001).
13) Fridrich, J., Goljan, M., Chen, Q. and Pathak, V.: Lossless data embedding with file size preservation, *Proc. SPIE*, Vol.5306, pp.354–365 (2004).
14) MacKay, D.J.C.: *Information Theory, Inference, and Learning Algorithm*, Cambridge University Press (2003).
15) Duda, R.O., Hart, P.E. and Stork, D.G.: *Pattern Classification*, Wiley-Interscience Publication (2001).
16) Lyu, S. and Farid, H.: Detecting hidden messages using higher-order statistics and support vector machines, *Lecture Notes in Computer Science*, Vol.2578, pp.340–354 (2003).

(Received February 5, 2009)
(Accepted July 2, 2009)
(Released October 7, 2009)

Takayuki Ishida received B.E. from Kagoshima National College of Technology in 2007 and M.E. from Kyushu Institute of Technology in 2009. His research interests include image processing and information hiding.

Kazumi Yamawaki received B.E., M.E. degrees in computer engineering from Kyushu Institute of Technology, Japan, in 1996 and 1998 respectively. She is currently a research assistant in the Department of Systems Design and Informatics, Kyushu Institute of Technology. Her research interests include image processing and information hiding. She is a member of IEICE.

Hideki Noda received B.E., M.E. from Kyushu University in 1973 and 1975, respectively, and Dr.Eng. from Kyushu Institute of Technology in 1993. He worked in National Research Institute of Police Science and then in Communications Research Laboratory. In 1995, he moved to Kyushu Institute of Technology where he is now a professor. His research interests include speech processing, image processing and information security. He is a member of IEICE, ASJ and IEEE.



Michiharu Niimi received B.E., M.E. degrees in computer engineering from Kyushu Institute of Technology, Japan, in 1992 and 1994 respectively, and Dr.Eng. degree in electrical engineering from Kyushu Institute of Technology in 2003. He is currently an associate professor in the Department of Systems Design and Informatics, Kyushu Institute of Technology. His research interests include image processing, natural language processing and information hiding. He is a member of IEICE, ITE, JSAI and IEEE.