Journal of Information Hiding and Multimedia Signal Processing ©2011 ISSN 2073-4212
Ubiquitous International Volume **2**, Number **1**, January **2011**

Reversible Data Hiding By Adaptive IWT-coefficient Adjustment

Ching-Yu Yang[a], Chih-Hung Lin[b], and Wu-Chih Hu[a]

[a]Dept. of Computer Science and Information Engineering, National Penghu University
No. 300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan
{chingyu; wchu}@npu.edu.tw
[b]Dept. of Computer Science and Information Engineering
Southern Taiwan University of Technology
No.1, Nantai St., Yongkang City, Tainan County, 710 Taiwan
chuck@mail.stut.edu.tw

Received December 2009; revised July 2010

Abstract. *In this paper, a novel reversible watermarking method based on the adaptive IWT-coefficient adjustment is proposed. A host image is first decomposed into the integer wavelet transform (IWT) domain. Subsequently, a secret message is embedded into the low-high (LH), high-low (HL), and high-high (HH) sub-bands of the IWT using the adaptive IWT-coefficient adjustment. Experiments confirm that the proposed method not only completely recovers a host medium but also generates marked images of a high perceived quality and hiding capacity. Moreover, the marked images are robust against manipulations such as JPEG2000, JPEG, brightness adjustment, cropping, and inversion.*
Keywords: Adaptive IWT-coefficient adjustment, Integer wavelet domain.

1. **Introduction.** Due to the ubiquitous broadband services provided by the Internet Service Providers (ISPs), some popular applications such as world wide web (WWW), electronic mail (e-mail), file transfer protocol (FTP), and voice over IP (VoIP) are spread around the world. In addition, the transaction platform of electronic commerce (EC) such as business-to-business (B2B), business-to-customer (B2C), and customer-to-customer (C2C) render the users to easily transact business on the Internet. However, data can be eavesdropped, illicit tampered, or falsified during transmission. To guard against the intervention from the third parties, the individuals (and organizations) often use digital watermarking to achieve the goals [1-2]. Several major applications of digital watermarking can be found in the areas of proof of ownership, copyright protection, and content authentication. However, most of the reported watermarking schemes are irreversible [3-6]. To completely restore the original host medium, some authors [7-14] have presented lossless data hiding techniques to solve the issues. Based on the block difference histogram of a host image, Lin et al. [9] presented a high-performance reversible data hiding technique. To embed the secret message, a maximum-point at the difference of the block was first selected with a greedy approach. Then, the difference of the block at the maximum point was increased by 1 or remained unchanged if the secret bit is 1 or 0, respectively. In Weng et al.s [10] work, they proposed a novel integer transformation based on the invariability of the sum of pixel pairs and pair-wise difference adjustment. Hsiao et al. [12] suggested a delicate lossless data hiding algorithm. A host image was first divided

into two categories: data hiding area and overhead hiding area. The data hiding area was further classified as three kinds of blocks: normal, smooth, and complex. To preserve a good resulting visual quality, data bits were embedded only in the smooth blocks and normal blocks. The location map and auxiliary information used by the algorithm were hidden in the overhead hiding area. To obtain a reversible watermarking technique, Zeng et al. [13] used adjacent pixel difference and multi-layer embedding techniques on a scan path. Namely, they predetermined nine scan paths to dig out the space for hiding bits. The multi-layer employed in their technique was used to increase further the hiding capacity. The marked images generated by the above methods [9, 10, 12, 13] are vulnerable to manipulation as the methods hide bits in the spatial domain. Namely, data extraction can fail if even a slight alteration is made to the marked images. On the other hand, Yang et al. [14] utilized the coefficient-bias algorithm to propose the technique of combinational reversible watermarking in both spatial and frequency domains. The secret message (which can be divided into two parts) was embedded into the spatial domain and/or frequency domain of a host image. Although the approach has the capability of resisting manipulation, the payload size is still not good enough. To address these issues, the proposed method tried to embed a large number of bits into the frequency domain while minimizing distortion.

The rest of the paper is organized as follows. The proposed adaptive IWT-coefficient adjustment algorithm is described in Section 2. Both the procedures of data embedment and data extraction are described in this section. Two examples used to illustrate the process of bit embedding are also included. The overhead information for the proposed method was discussed in the last part of Sec. 2. Section 3 presents the simulations. The conclusion is given in Section 4.

2. **Proposed Method.**

To achieve a method with a high hiding capacity and robust performance, the authors embed a message into the frequency domain based on the adaptive IWT-coefficient adjustment. Firstly, an input image is decomposed to the integer wavelet transform (IWT) domain. Secondly, data bits are embedded into the blocks which derived from the three high sub-bands of the IWT. Prior to the embedding, a coefficient of the block is shifted to a new value (which is approximated to zero) when its value is either larger than γ or less than $-\gamma$. Subsequently, the (shifted) coefficients are labelled if their value fall outside the range between $-\beta$ and β The idea behind the labelled process is that we want to prevent the labelled coefficients from being used for hiding bits so as to reduce further the distortion. Finally, data bits are hidden in the shifted coefficients that lie between $-\beta$ and β by modulo 2^k substitution. Both β and γ are two control parameters and $|\beta| > |\gamma|$ while k is an integer.

2.1. **Data embedding.**

Let $C = \{c_{ij}\}_{i=0}^{n\times n-1}$ be the i-th non-overlapping block of size $n \times n$ that divided from the three high sub-bands of IWT domain, namely, the low-high (LH), high-low (HL), or high-high (HH) sub-bands, respectively. To dig out a higher hiding space, two adjustments for the IWT coefficients in a block are performed. More specifically, each coefficient c_{ij} is first shifted to a new value $\hat{c}_{ij}$ if it satisfies the following rules:

$$\hat{c}_{ij} = \begin{cases} c_{ij} + \gamma, & \text{if} \quad c_{ij} < -\gamma \\ c_{ij} - \gamma, & \text{if} \quad c_{ij} > \gamma. \end{cases} \tag{1}$$

A bitmap was used to flag whether or not a coefficient of the block undergone adjustment. As described previously, to maintain low levels of distortion, the labelled process

is subsequently conducted in accordance with the following rules:

$$\tilde{c}_{ij} = \begin{cases} \hat{c}_{ij} - (2^k - 1)\beta, & \text{if } \hat{c}_{ij} \le -\beta \\ \hat{c}_{ij} + (2^k - 1)\beta, & \text{if } \hat{c}_{ij} \ge -\beta, \end{cases} \tag{2}$$

where $\tilde{c}_{ij}$ denotes the labelled coeficients. That is, no data bits would be carried by the the labelled coeficients. After the adjustments have been made, the data bits bs are embedded into the blocks. The coefficients $c_r \in C$ which satisfy $0 \le c_r < \beta$ are multiplied by 2^k to obtain $\hat{c}_r$. The data bits b_s are then added to $\hat{c}_r$. Following this, the coefficients $c_l \in C$ which satisfy $-\beta < c_l < 0$ are multiplied by 2^k to obtain $\hat{c}_l$, and b_s is than substracted from $\hat{c}_l$. This procedure is repeated until all data bits have been processed.

Figures 1-2 present examples of bit embedding. The figures illustrate the cases of n^2-bit and non-n^2-bit hidden, respectively. The k used here is 1. Both control parameters β and γ are set to be 3 and 2, respectively. A host IWT-block was shown in Fig. 1(a). Figure 1(b) illustrates a shifted block, which obtained by computing (1). Note that each of the shifted coefficients was marked by a rectangle. Since all of the coefficients in the shifted block can be used to hide bits, the labelled process was skipped here. Figure 1 (c) shows the bit-hidden block. The mean square error (MSE) computed from Figs. 1(a) and 1(c) is 2.375. Another example of hiding 12-bit (or non-n^2-bit) in a IWT-block was shown in Fig. 2. According the rules listed in (1) and (2), a shifted block and a labelled block were obtained, as shown in Figs. 2(b) and 2(c), repectively. Notice as well the labelled coefficients were denoted by a gray highlighted number. The resulting hidden block was depicted in Fig. 2(d). In this case, the MSE for the bit-hidden block is 1.875.

1	1	2	0
4	2	3	-1
1	-2	-4	-1
-2	-1	0	-1

(a)

1	1	2	0
2	2	1	-1
1	-2	-2	-1
-2	-1	0	-1

(b)

3	3	5	0
4	4	3	-2
2	-4	-5	-2
-4	-2	0	-3

(c)

FIGURE 1. Example of 16-bit embedding with a bit-stream of 1110-0010-0010-0001. (a) The original IWT-block, (b) shifted block, and (c) bit-hidden block.

5	-2	-6	-1
-1	1	3	3
-5	0	0	6
0	2	-4	0

(a)

-3	-2	-4	-1
-1	1	1	1
-3	0	0	4
0	2	-2	0

(b)

6	-2	-7	-1
-1	1	1	1
-6	0	0	7
0	2	-2	0

(c)

6	-4	-7	-2
-3	3	3	2
-6	1	0	7
0	5	-4	1

(d)

FIGURE 2. Example of 12-bit embedding with a bit-stream of 0011-1010-0101. (a) The IWT-block, (b) shifted block, (c) labelled block, and (d) bit-hidden block.

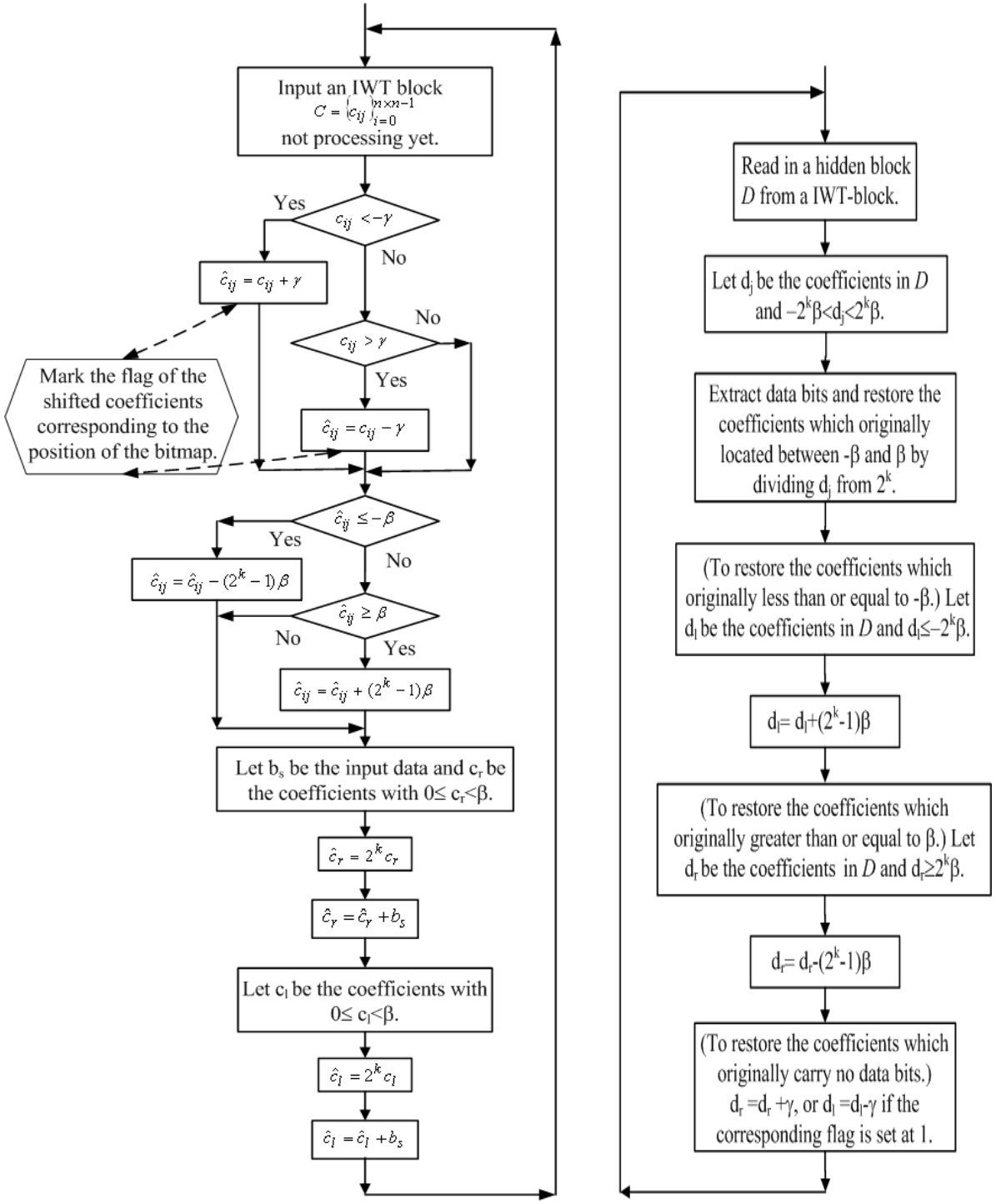
2.2. **Data extraction.** Firstly, a marked image is decomposed into the IWT domain. It is then read in a block D of size $n \times n$ from the LH, LH, and HH sub-bands of the IWT. If a coefficient $d_j \in D$, exists which satisfies $-2^k\beta < d_j < 2^k\beta$, the coefficient d_j is divided by 2^k. It is quite obvious that the hidden bits can then be obtained from the residual. At the same time, the coefficients which were originally located between $-\beta$ and β can be restored from the quotient. The coefficients $d_l \in D$, which satisfy $d_l \leq -2^k\beta$ (which were originally less than or equal to $-\beta$) can be restored by adding $(2^k-1)\beta$ to d_l. In addition, the coefficients $d_r \in D$, which satisfy $d_r \geq 2^k\beta$ (which were originally greater than or equal to β) can be restored by subtracting (2^k-1) from d_r. Moreover, to restore the coefficients which originally contained no data bits, γ is added to d_r if the corresponding flag on the bitmap was set to 1. Conversely, γ subtracted from the coefficients d_l if the corresponding flag was marked as 1. As a result, data bits are extracted perfectly and the original host block is completely recovered. This procedure is repeated until all of the data bits have been extracted. The schematic overview of the proposed method is summarized in Fig. 3.

2.3. **Overhead information analysis.** The number of bits for the overhead information which used to signify whether or not a coefficient of the block underwent adjustment for the proposed method is $\left(\frac{M}{2}/n\right) \times \left(\frac{N}{2}/n\right) \times n^2 \times 3 = \frac{3MN}{4}$, where the image size is $M \times N$ and the block size is $n \times n$. To assist the decoder in extracting the secret bits, the overhead information can be compressed losslessly using the arithmetic encoder and the resulting bits stream can be sent to the receiver by out-of-band transmission. From the point of view of data security, the proposed method provides a more secure manner than the methods which embed message in combination with the overhead information into a host medium.

To overcome the issue of overflow or underflow, a pixel-shift approach can be performed in the spatial domain before embedding. Namely, if a pixel p in a host image satisfies either $p < \phi_1$ or $p > \phi_2$, p is adjusted to a new value by adding to or subtracting from an integer offset δ. Both ϕ_1 and ϕ_2 are two predetermined threshold values. However, an extra location map is required for the proposed to record whether or not a pixel has undergone pixel adjustment.

3. **Experimental Results.** Several greyscale images of size 512×512 were used as host images. A quarter of the host image *Lena* was used as the test data. An integer k used here is set to 1 and 2, respectively. To provide a variety of bit rate, the values of two control parameters β and γ are not fixed. The marked images generated by embedding test data in the host images via the proposed method are shown in Fig. 4. The block size is 4×4. It can be seen from Fig. 4 that the perceived quality is acceptable. Their average PSNR and bit rate are 30.97 dB and 1.235 bits per pixel (bpp), respectively. Moreover, the relationship between PSNR and bit rate for the proposed method is depicted in Fig. 5. From the figure we can see that the maximum PSNR of value 48.30 dB can be achieved at the bit rate of 0.257 by the proposed method. On the other hand, the maximum hiding rate is 1.427 bpp with the PSNR of value 29.98 dB.

The payload size and PSNR (around 30 dB) comparisons between the proposed method and the reported techniques [9, 12-14] are listed in Table 1. The average hiding capacity and distortion of these methods is also included. Table 1 indicates that the proposed method provides the best hiding capacity on all test images except *Jet*. Although the payload size of the proposed method is less than that of Zeng et al.'s algorithm [13] and Yang et al.'s approach [14] on image *Jet*, the proposed method resulted in a better PSNR value. Notably, the proposed method has the best performance of the average payload



(a) Data embedding (b) Data extraction

FIGURE 3. The schematic overview of the proposed method. (a) Data embedding and (b) data exteaction.

size and PSNR among these methods. In addition, a comparison of the capacity against distortion for the various methods [9-10, 12-13] on image *Lena* is provided in Fig. 6. As shown in Fig. 6, the proposed method outperforms the other four methods.

Furthermore, neither a watermark nor host image was extracted or recovered successfully using the other four methods [9-10, 12-13] when the marked images were manipulated

(a) Lena (32.47/1.293) (b) Jet (31.18/1.147)

(c) Peppers (31.77/1.273) (d) Goldhill (30.29/1.229)

FIGURE 4. The marked images (with PSNR and bit rate) generated by the proposed method. (a) Lena, (b) Jet, (c) Peppers, and (d) Goldhill.

by the third parties. To reveal the robust performance of the proposed method, examples of extracted watermarks (size of 210×210 with 8 bits/pixel, 2 colours) after various manipulations of the image are depicted in Fig. 7. The bit correct ratio (BCR) is also included. The BCR is defined by

$$BCR = \left(\sum_{i=0}^{MN-1} \overline{w_i \oplus w_i'} \Big/ M \times N \right) \times 100\%, \tag{3}$$

where w_i and w_i' represent the values of the original watermark and the extracted watermark respectively. Although the BCR in Figs. 7(b), 7(c), and 7(e) are not high, the extracted watermarks are identifiable. Figures 7(d) and 7(f) also confirm that the watermarks extracted from the manipulated images were recognizable.

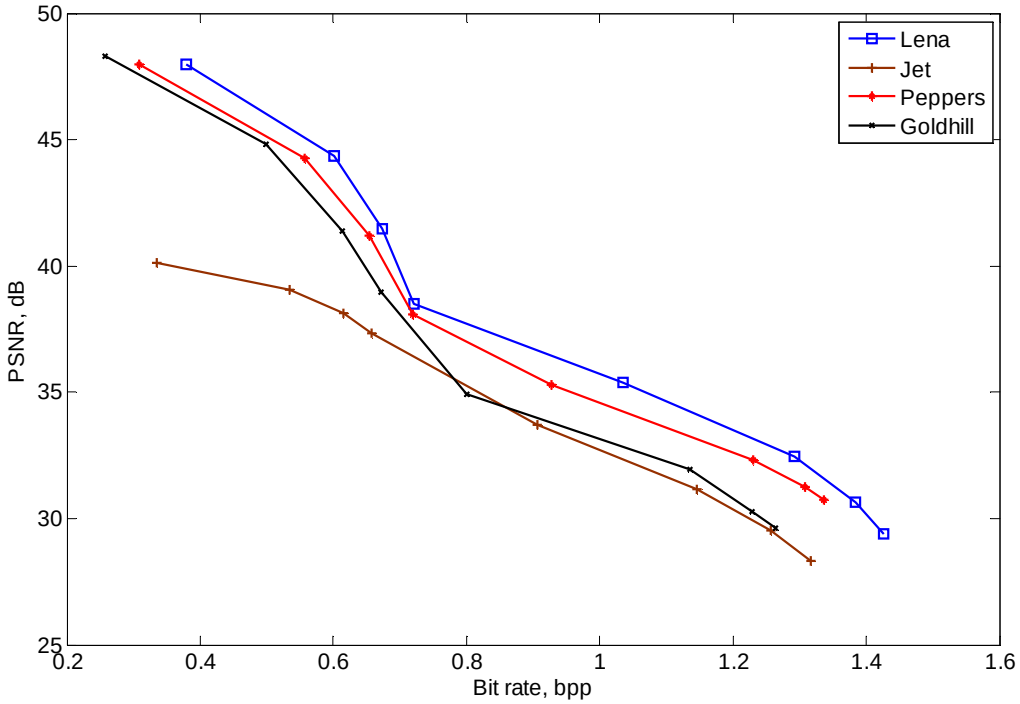


FIGURE 5. Trade-off between PSNR and bit rate for the proposed method on several images.

TABLE 1. Payload size and PSNR comparison between the proposed method and other methods (with PSNR around 30 dB).

Methods	Images				
	Lena	*Jet*	*Peppers*	*Goldhill*	Average
Lin et al.'s Technique [9]	231,971/ 30.2	289,877/ 30.1	268,042/ 30.2	234,160/ 30.1	256,013/ 30.15
Hsiao et al.'s Scheme [12]	303,700/ 30.00	286,488/ 30.00	303,736/ 30.00	245,370/ 30.00	284,824/ 30.00
Zenget al.'s Algorithm [13]	282,147/ 30.12	338,492/ 30.08	317,194/ 29.66	-	310,681/ 30.30
Yang et al.'s Approach [14]	314,573/ 30.00	311,404/ 30.71	317,194/ 29.66	246,415/ 29.65	297,397/ 30.01
Proposed method	362,840/ 30.64	300,608 31.18	333,622/ 31.77	322,190/ 30.29	329,815 30.97

4. **Conclusions.** A simple but effective lossless data hiding method is proposed in this paper. Using the adaptive IWT-coefficient adjustment, the proposed method embeds a large number of data bits into the three high sub-bands of the IWT domain while maintaining low levels of distortion. Experiments also verify that the marked images generated by the proposed method can tolerate attacks from JPEG2000, JPEG, brightness adjustment, cropping, and inversion. Our future work will focus on the reduction of overhead bits and the promotion of robustness.

REFERENCES

[1] J. S. Pan, H. C. Huang, and L. C. Jain (Eds.), *Intelligent Watermarking Techniques*, Singapore: World Scientific, 2004.

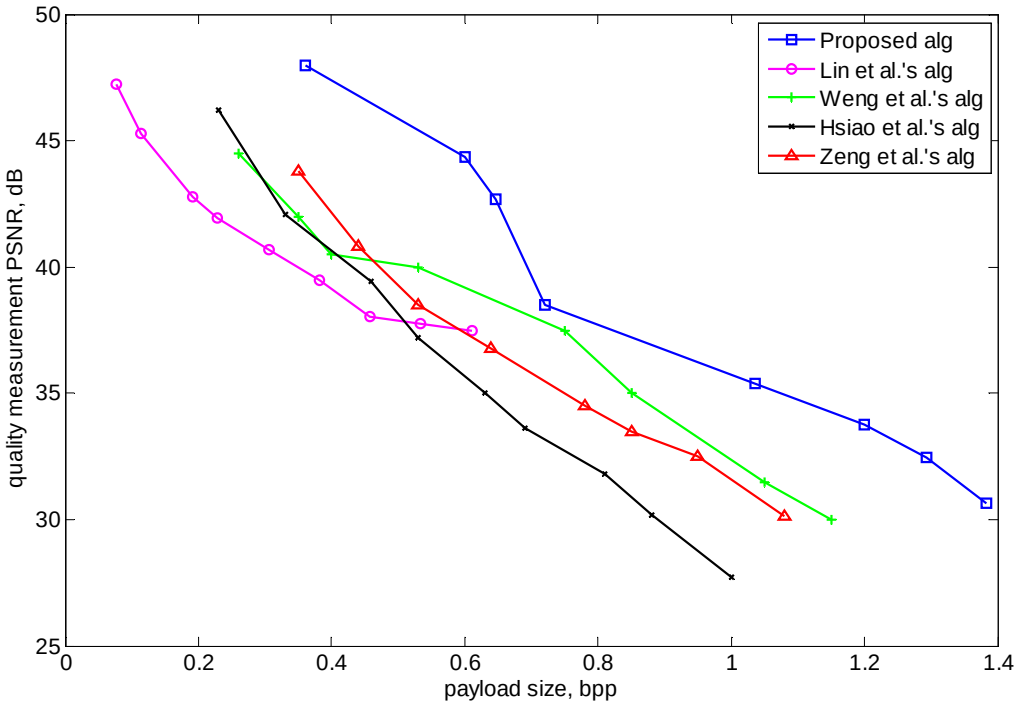
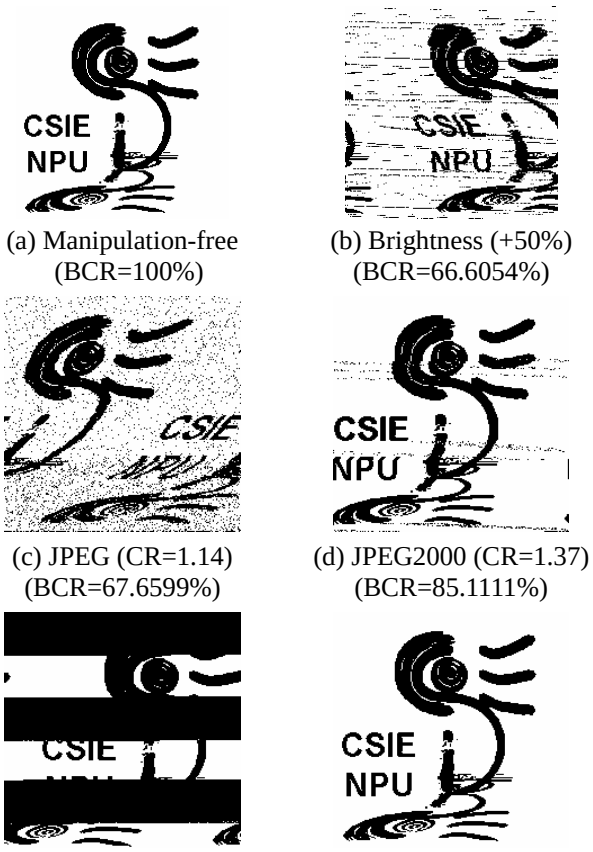


FIGURE 6. Capacity against distortion comparison on image *Lena*.



(a) Manipulation-free (BCR=100%)

(b) Brightness (+50%) (BCR=66.6054%)

(c) JPEG (CR=1.14) (BCR=67.6599%)

(d) JPEG2000 (CR=1.37) (BCR=85.1111%)

(e) Cropping (50%) (BCR=41.0113%)

(f) Inversion (BCR=100%)

FIGURE 7. Examples of extracted watermarks after various manipulations.

[2] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*, CRC Press., FL, 2008.

[3] T. H. Chen and T. H. Hung, Multiple watermarking based on visual secret sharing, *International Journal of Innovative Computing Information and Control*, vol. 4, no. 11, pp. 3005-3026, 2008.
[4] S. Wang, B. Yang, and X. Niu, Secure steganography method based on genetic algorithm, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 28-35, 2010.
[5] M. C. Hu, D. C. Lou, and M. C. Chang, Dual-wrapped digital watermarking scheme for image copyright protection *Computers & Security*, vol. 26, no. 4, pp. 319-330, 2007.
[6] C. Y. Yang, W. C. Hu, W. Y. Hwang, and Y. F. Cheng, A simple digital watermarking by the adaptive bit-labeling scheme, *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 3, pp. 1401V1410, 2010.
[7] J. Tian, Reversible data mbeddedding using a difference expansion, *Proc. of IEEE T. Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.
[8] C. C. Chang, T. Lu, Y. F. Chang, and C. T. Lee, Reversible data hiding schemes for deoxyribonucleic acid (DNA) medium, *International Journal of Innovative Computing Information and Control*, vol. 3, no. 5, pp. 1145-1160, 2007.
[9] C. C. Lin, N. L. Hsueh, and W. H. Shen, High-performance reversible data hiding, *Fundamenta Informaticae*, vol. 82, no. 1-2, pp. 155-169, 2007.
[10] S. Weng, Y. Zhao, J. S. Pan, and R. Ni, Reversible watermarking based on invariability and adjustment on pixel pairs, *Proceeding of IEEE Signal Processing Letters*, vol. 15, pp. 721-724, 2008.
[11] C. C. Chen, and D. S. Kao, DCT-based zero replacement reversible image watermarking approach, *Proc. of International Journal of Innovative Computing Information and Control*, vol. 4, no. 11, pp. 3027-3036, 2008.
[12] J. Y. Hsiao, K. F. Chan, and J. M. Chang, Block-based reversible data embedding, *Signal Processing*, vol. 89, no. 4, pp. 556-569, 2009.
[13] X. Zeng, L. Ping, and Z. Li, Lossless data hiding scheme using adjacent pixel difference based on scan path, *Journal of Multimedia*, vol. 4, no. 3, pp. 145-152, 2009.
[14] C. Y. Yang, W. C. Hu, and C. H. Lin, Reversible data hiding by coefficient-bias algorithm, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 2, pp. 100-109, 2010.