24

Robust Lossless Data Hiding by Feature-Based Bit Embedding Algorithm

Ching-Yu Yang
Department of Computer Science and Information Engineering
National Penghu University of Science and Technology
Taiwan

1. Introduction

Recently, data hiding, or information hiding, plays an important role in data assurance. Generally speaking, data hiding techniques can be classified into steganography and digital watermarking (Cox et al., 2008; Shih, 2008). The marked images generated by the steganographic methods (Gu & Gao, 2009; Liu & Shih, 2008; Qu et al., 2010; Wang et al., 2010; Zhou et al., 2010; Fan et al., 2011) were prone to catch damage (by manipulations) and resulted in a failure extraction of the message. However, based on the spatial domain, the steganographic methods often provide a large payload with a good perceived quality. Major applications of the techniques can be found in private data saving, image tagging and authentication, and covert communications. On the other hand, the robustness performance with a limited payload is a key feature of digital watermarking approaches (Lai et al., 2009; Al-Qaheri et al., 2010; Lin & Shiu, 2010; Yamamoto & Iwakiri, 2010; Yang et al., 2010; Martinez-Noriega et al., 2011). Most of the robust watermarking approaches which based on the transform domain such as discrete cosine transform (DCT), integer wavelet transform (IWT), and discrete Fourier transform (DFT) can be tolerant of common image processing operations. Their usages can be found in owner identification, proof of ownership, and copy control. Note that conventional data hiding techniques were irreversible, namely, the host media can not be recovered after data extraction. To preserve or protect the originality of the valuable (or priceless) host media, for example, military or medical images, and law enforcement, the reversible data hiding schemes, also known as lossless data hiding schemes were suggested to achieve the goal. For some applications, it requires to completely recover the host media if the marked images remain intact, and to extract the hidden message when the marked images were intentionally (or unintentionally) manipulated by the third parties. But, most of reversible data hiding schemes (Tian, 2003; Alattar, 2004; Hsio et al., 2009; Hu et al., 2009; Tai et al., 2009; Wu et al., 2009; Lee et al., 2010; Xiao & Shih, 2010; Yang & Tsai, 2010; Yang et al., 2010, 2011) were fragile in the sense that the hidden message can be unsuccessfully extract even if a slight alteration to the marked images, not to mention the recovery of the host media. Several authors (Zou et al., 2006; Ni et al., 2008; Zeng et al., 2010) therefore proposed robust reversible data hiding algorithms to overcome the issue.

Zou et al. (Zou et al., 2006) presented a semi-fragile lossless watermarking scheme based on integer wavelet transform (IWT). To obtain a good perceptual quality, they only embed data

bits into the low-high (LH) and high-low (HL) of the IWT coefficients. During bit embedding, the IWT blocks remain intact if an input bit is 0, otherwise, the proposed embedding process were applied to the blocks. Simulations showed that the hidden message was robust against lossy compression to a certain degree. Ni et al. (Ni et al., 2008) presented a robust lossless data hiding technique based on the patchwork theory, the distribution features of pixel groups, error codes, and the permutation scheme. The marked images generated by the technique contained no salt-and-pepper noise with a limited payload size. In addition, the marked images were robust against to JPEG/JPEG2000 compression. Zeng et al. (Zeng et al., 2010) adjusted the mathematical difference values of a block and designed a robust lossless data hiding scheme. A cover image was first divided into a number of blocks and the arithmetic difference of each block was calculated. Data bits were then embedded into the blocks by shifting the arithmetic difference values. Due to the separation of the bit-0-zone and the bit-1-zone, as well as the particularity of mathematical difference, a major merit of the method was tolerant of JPEG compression to some extent. Compared with Ni et al.'s work (Ni et al., 2008), the performance of Zeng et al.'s scheme (Zeng et al., 2010) was significantly improved.

Currently there are a few robust lossless data hiding techniques published in the literature. Since the payload provided by the above techniques (Zou et al., 2006; Ni et al., 2008; Zeng et al., 2010) was not good enough, we therefore propose the FBBE algorithm so that to introduce an effective robust lossless data hiding method. Moreover, to provide a high-capacity version of lossless data hiding scheme that based on IWT domain, we use a smart allocation of the coefficients in an IWT block to achieve the goal. The scheme not only provides a high payload but also generates a good perceived quality.

This chapter is organized as follows. In section 2, a robust lossless data hiding via the feature-based bit embedding (FBBE) algorithm is introduced followed by a high-performance lossless data hiding scheme. Section 3 provides both test results and performance comparisons. We conclude this chapter in section 4.

2. Proposed method

Based on the integer wavelet transform (IWT), we propose two lossless data hiding methods, namely, a robust version and a high-capacity one. First, a robust lossless data hiding via the feature-based bit embedding (FBBE) algorithm is specified. Instead of embedding data bits directly into the IWT coefficient blocks, we use the FBBE algorithm to encode a block so that it can carry data bits and can be successfully identified later at the receiver. Then, a high-performance lossless data hiding scheme is presented to provide a large hiding storage by adjusting the location of each IWT coefficient in the host block. More specifically, the FBBE algorithm can be used to generate a robust lossless data hiding method. Whereas, the proposed smart adjustment of the IWT coefficients can be used to generate a high-performance lossless data hiding scheme.

2.1 FBBE algorithm

To achieve a robust lossless data hiding method, we embed a secret message into transform domain via the FBBE algorithm. An input image was first decomposed to the IWT domain. The IWT coefficients can be acquired by using the following two formulas:

$$d_{1,k} = s_{0,2k+1} - s_{0,2k} \tag{1}$$

and

$$s_{1,k} = s_{0,2k} + \left\lfloor \frac{d_{1,k}}{2} \right\rfloor, \tag{2}$$

where $s_{j,k}$ and $d_{j,k}$ are the kth low-frequency and high-frequency wavelet coefficients at the jth level, respectively (Calderbank et al., 1998). The $\lfloor x \rfloor$ is a floor function. Then, data bits were embedded into the blocks which derived from the LH and HL sub-bands of the IWT coefficients, respectively. The FBBE algorithm consists of four parts, namely, Up-U (UU) sampling, Down-U (DU) sampling, Up-Down (UD) sampling, and Left-Right (LR) sampling. Each sampling is allowed to carry a single data bit. For each host block, the above four samplings is conducted according to the sequence of UU, DU, UD, and LR samplings. The details are specified in the following sections.

2.1.1 Bit embedding

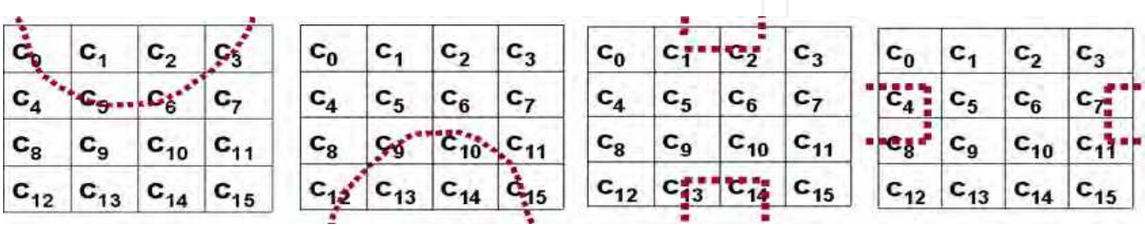
Let $C_j = \{c_{jk}\}_{k=0}^{n^2-1}$ be the jth block of size $n \times n$ taken from the LH (or HL) sub-bands of IWT domain. Also let $C_j = \{\hat{C} \cup \tilde{C} \cup C' \cup C''\}$ with $\hat{C} = \{\hat{c}_i \mid i = 0,3,5,6\}$, $\tilde{C} = \{\tilde{c}_u \mid u = 9,10,12,15\}$, $C' = \{c'_v \mid v = 1,2,13,14\}$, and $C'' = \{c''_w \mid w = 4,7,8,11\}$ be the UU, DU, UD, and LR samplings coefficients, respectively, as shown in Fig. 1 if n=4. In addition, let

$$C_{jp} = \{\hat{c}_i \mid \beta \le \hat{c}_i < 2\beta\} \tag{3}$$

and

$$C_{jm} = \{\hat{c}_i \mid -2\beta \le \hat{c}_i < -\beta\} \tag{4}$$

be the two focal groups being used to 'carry' data bits. The β used here is a robustness parameter.



(a) (b) (c) (d)

Fig. 1. A 4×4 IWT coefficients block. (a) UU, (b) DU, (c) UD, and (b) LR sampling coefficients.

The main steps of UU (or DU, UD, LR) samplings are specified as follows:

Step 1. Input a block C_j not processing yet.

Step 2. If an input bit ϕ=0 and $|C_{jp}|\geq|C_{jm}|$ then do nothing, which means a bit 0 can be carried by the UU (or DU, UD, LR) sampling coefficients without alteration of their value, and go to Step 8.

Step 3. If ϕ=0 and $|C_{jp}|<|C_{jm}|$ then add β to the coefficients c_{jk} in C_j with $0 \leq c_{jk} < \beta$, respectively, mark a flag to the shifted coefficient, and go to Step 8.

Step 4. If ϕ=0 and $|C_{jp}|<|C_{jm}|$ then add β to the coefficients in C_{jm}, respectively, mark a flag to the shifted coefficient, and go to Step 8.

Step 5. If ϕ=1 and $|C_{jp}|<|C_{jm}|$ then do nothing, which means the UU (or DU, UD, LR) samplings coefficients carry a bit 1, and go to Step 8.

Step 6. If ϕ=1 and $|C_{jp}|\geq|C_{jm}|$ then subtract β from the coefficients c_{jk} in C_j with $-\beta \leq c_{jk} < 0$, respectively, mark a flag to the shifted coefficient, and go to Step 8.

Step 7. If ϕ=1 and $|C_{jp}|\geq|C_{jm}|$ then subtract β from the coefficients in C_{jp}, respectively, mark a flag to the shifted coefficient.

Step 8. Repeat Step 1 until all IWT coefficients blocks have been processed.

Notice that the coefficients $\hat{c}_i$ which belong to either C_{jp} or C_{jm} have to be changed to $\tilde{c}_u$, c'_v, or c''_w, respectively, when the DU, UD, or LR samplings was employed. From the above procedures we can see that each block can carry at most four data bits. This resulted in a total payload of $\lfloor M/2n \rfloor \times \lfloor N/2n \rfloor \times 2 \times 4 \leq \frac{2MN}{n^2}$ bits provided by the proposed method, where *M* and *N* is the size of a host image.

2.1.2 Bit extraction

Let $D_j = \{d_{jk}\}_{k=0}^{n^2-1}$ be the *j*th hidden block of size $n \times n$ taken from the LH (or HL) sub-bands of IWT domain derived from a marked image, and $D_j = \{\hat{D} \cup \tilde{D} \cup D' \cup D''\}$ with $\hat{D} = \{\hat{d}_i \mid i = 0,3,5,6\}$, $\tilde{D} = \{\tilde{d}_u \mid u = 9,10,12,15\}$, $D' = \{d'_v \mid v = 1,2,13,14\}$, and $D'' = \{d''_w \mid w = 4,7,8,11\}$. Also let

$$D_{jp} = \{\hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w) \mid \beta \leq \hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w) < 2\beta\} \tag{5}$$

and

$$D_{jm} = \{\hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w) \mid -2\beta \leq \hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w) < -\beta\} \tag{6}$$

be the two subsets of D_j. The procedure of bits extraction for the UU (or DU, UD, LR) sampling can be summarized in the following steps.

Step 1. Input a hidden block D_j not processing yet.

Step 2. If $|D_{jp}| > |D_{jm}|$ then a bit 0 can be identified. Subtract β from either the coefficients d_{jk} in D_j with $-\beta \le d_{jk} < 0$ or the coefficients $\hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w)$ in D_{jp} when the corresponding flag was set at 1, and go to Step 6.

Step 3. If $|D_{jp}| < |D_{jm}|$ then a bit 1 can be extracted. Add β to either d_{jk} in D_j with $0 \le d_{jk} < \beta$ or the coefficients $\hat{d}_i (\text{or } \tilde{d}_u, d'_v, d''_w)$ in D_{jm} when the corresponding flag was set at 1, go to Step 6.

Step 4. If $|D_{jp}| = |D_{jm}|$ and the flag of the coefficients d_{jk} in D_j with $-\beta \le d_{jk} < 0$ was set at 1, a bit 0 can be identified, and go to Step 6.

Step 5. If $|D_{jp}| = |D_{jm}|$ and the flag of the coefficients d_{jk} in D_j with $0 \le d_{jk} < \beta$ was set at 1, a bit 1 can be identified.

Step 6. Repeat Step 1 until all hidden bits have been extracted.

The number of bits for the overhead information which used to signify whether or not a coefficient of the block undergone adjustment is $\left\lfloor \frac{M}{2} \Big/ n \right\rfloor \times \left\lfloor \frac{N}{2} \Big/ n \right\rfloor \times n^2 \times 2 \le \frac{MN}{2}$.

2.2 High-performance lossless data hiding scheme

To provide a high-capacity with a good perceived quality, the proposed scheme, which based on the adjustment of the locations of the coefficients in a host block, embeds a secret message into the three high sub-bands of IWT domain. The details are described in the following subsections.

2.2.1 Data embedment

Let $C_j = \{c_{jk}\}_{k=0}^{n^2-1}$ be the jth block of size $n \times n$ taken from the LH (or HL, HH) sub-band of IWT domain. Also let $C_{jp} = \{c_p \mid \beta \le c_p < 2\beta\}$ and $C_{jm} = \{c_m \mid -2\beta \le c_m < -\beta\}$ be two subsets of C_j. The main steps of bit embedding are specified as follows:

Step 1. Input a block C_j not processing yet.

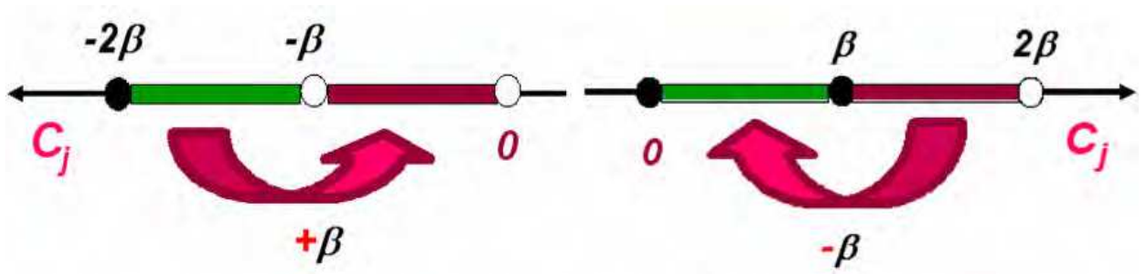
Step 2. If $|C_{jp}| \ne \varnothing$ then subtract β from each coefficient of C_{jp} and mark a flag to the modified coefficient.

Step 3. If $|C_{jm}| \ne \varnothing$ then add β to each coefficient of C_{jm} and mark a flag to the modified coefficient.

Step 4. After adjustment, for a coefficient $c_i \in C_j$ with $0 \le c_i < \beta$ (or $-\beta \le c_i < 0$), multiply c_i by 2 to obtain $\hat{c}_i$, and add an input bit to $\hat{c}_i$.

Step 5. Repeat to Step 1 until all blocks have been processed.

The purpose of steps 3 and 4 are tried to further dig out hiding space from the selected coefficients. The schema of the adjustment of the coefficients values for the above two steps can be illustrated in Fig. 2.



(a) (b)

Fig. 2. The schema of the coefficients adjustment. (a) The positive part and (b) the negative part.

To increase payload size, multiple bits can be hidden in each IWT coefficient. In this case, the above steps 2-4 are rewritten as follows:

Step 2a. For a coefficient $c_t \in C_j$ with $-\beta < c_t < \beta$, multiply c_t by 2^k to obtain $\hat{c}_t$, and mark a flag to the modified coefficient.

Step 3a. For each $\hat{c}_t$, add data bits ϕ to $\hat{c}_t$ if $\hat{c}_t \geq 0$, otherwise, subtract ϕ from $\hat{c}_t$.

The parameter *k* is an integer. To maintain a good resulting perceived quality, the value of *k* is no more than 2. From the above procedure we can see that the number of bits used for recording the indices of the modified coefficients is $\lfloor M/2n \rfloor \times \lfloor N/2n \rfloor \times n^2 \times 3 < {3MN}/{4}$.

2.2.2 Data extraction

To extract the hidden message, the overhead information can be losslessly compressed by using either the run-length coding algorithm or JBIG2. The resulting bit stream can then sent by an out-of-band transmission to the receiver. Without loss of generality, let D_j be the *j*th hidden block of size $n \times n$ taken from the LH (or HL, HH) sub-band of IWT domain which derived from a marked image, and $\hat{D}_j = \{\hat{d}_j \mid -2\beta \leq \hat{d}_j < 2\beta\}$ with $\hat{D}_j \subseteq D_j$. The procedure of bits extraction can be summarized in the following steps.

Step 1. Input a block D_j not processing yet.

Step 2. A data bit can be extracted by performing modulus-2 to $\hat{d}_j$.

Step 3. The IWT coefficients $\tilde{d}_j$ which hid data bit can be restored by performing either $\tilde{d}_j = \lfloor \hat{d}_j / 2 \rfloor$ if $\hat{d}_j \geq 0$ or $\tilde{d}_j = \lceil (\hat{d}_j / 2) - 0.5 \rceil$ if $\hat{d}_j < 0$.

Step 4. The original IWT coefficients can be recovered by adding (or subtracting) β to (or from) $\tilde{d}_j$ if $\tilde{d}_j \geq 0$ (or $\tilde{d}_j < 0$) while the flag of $\tilde{d}_j$ was marked.

Step 5. Repeat to Step 1 until all data bits have been extracted.

Note that $\lfloor x \rfloor$ and $\lceil x \rceil$ in step 3 denote the floor and ceiling functions, respectively. To perform multiple bits extraction for each coefficient, the above steps 2-4 are rewritten as follows:

Step 2b. A data bit can be extracted by performing modulus-2k to d'_j with $-2^k \beta \le d'_j < 2^k \beta$.

Step 3b. The IWT coefficients $\tilde{d}_j$ which hid data bits can be restored by performing $\tilde{d}_j = \lfloor \hat{d}_j / 2^k \rfloor$ if the flag of $\tilde{d}_j$ was marked.

Step 4b. The original IWT coefficients can be recovered by adding (or subtracting) $(2^k - 1)\beta$ to (or from) $\tilde{d}_j$ if $\tilde{d}_j \ge 0$ (or $\tilde{d}_j < 0$).

To specify the idea of data embedding, two examples were presented in Figs. 3-4. The figures illustrate the cases of full-bit ($n \times n$ bits) and partial-bit hidden, respectively. The k used here is 1. The control parameter β is set to be 4. A host IWT-block was shown in Fig. 3(a). Figure 3(b) illustrates a shifted block, which obtained by according to the steps 2-3 of Sec. 2.2.1. Note that each of the shifted coefficients was marked by a rectangle. According to the step 4 of Sec. 2.2.1, we can see that all of the coefficients in the shifted block can be used to hide bits. Namely, a full-bit (or 16-bit) can be embedded in Fig. 3(b). Figure 3 (c) shows the hidden block. The mean square error (MSE) computed from Figs. 3(a) and 3(c) is 7.667. Another example of hiding partial-bit (or 12-bit) in an IWT-block was shown in Fig. 4(a). A shifted block was shown in Fig. 4(b). Notice as well there are 4 coefficients (in bold type) containing null bits. The resulting hidden block was depicted in Fig. 4(c). In this case, the MSE for the hidden block is 6.444. To recover the original block, a similar reverse process (with a bitmap) can be performed to Figs. 3(c) and 4(c), respectively.

-5	-8	-3	-2
3	-7	-7	-2
6	-3	-8	-5
5	0	-6	-8

(a)

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

(b)

-2	-7	-5	-4
6	-5	-6	-4
4	-5	-8	-1
3	1	-4	-8

(c)

Fig. 3. Example of 16-bit embedding with a bit-stream of 0110 0100 0101 1100. (a) The original IWT-block, (b) shifted block, and (c) hidden block.

8	17	0	11
0	1	-15	2
-5	1	-6	-7
6	5	1	4

(a)

8	**17**	0	**11**
0	1	**-15**	2
-1	1	-2	-3
2	1	1	0

(b)

8	17	0	11
1	3	-15	4
-2	3	-3	-6
4	2	3	1

(c)

Fig. 4. Example of 12-bit embedding with a bit-stream of 0110 0110 0011. (a) The IWT-block, (b) shifted block, and (c) hidden block.

2.2.3 Overflow/underflow issues

An overflow/underflow can be occurred during bit embedding if a pixel value of the host image is a little either less than 255 or larger than 0. To overcome the overflow/underflow issues, a pixel-shifting approach can be performed in the spatial domain before data embedment. Namely, if a pixel value p in a host image satisfied either $p < \phi_1$ or $p > \phi_2$, p can be adjusted to a new value by adding to ϕ_1 or subtracting from ϕ_2. Both ϕ_1 and ϕ_2 are two predetermined threshold values.

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. To provide a variety of embedding rate, the value of the control parameter β is not fixed. Simulations generated by the proposed FBBE algorithm were first shown in the following subsection. Subsequently, a high-performance hiding scheme was examined.

3.1 Simulations of the FBBE algorithm

Figure 5 depicts the relationship between peak signal-to-noise ratio (PSNR) and robustness parameter β that generated by the proposed FBBE algorithm. The size of the block was 4×4. The figure indicated that the optimal PSNR value of 57.45 dB is achieved with β=1.

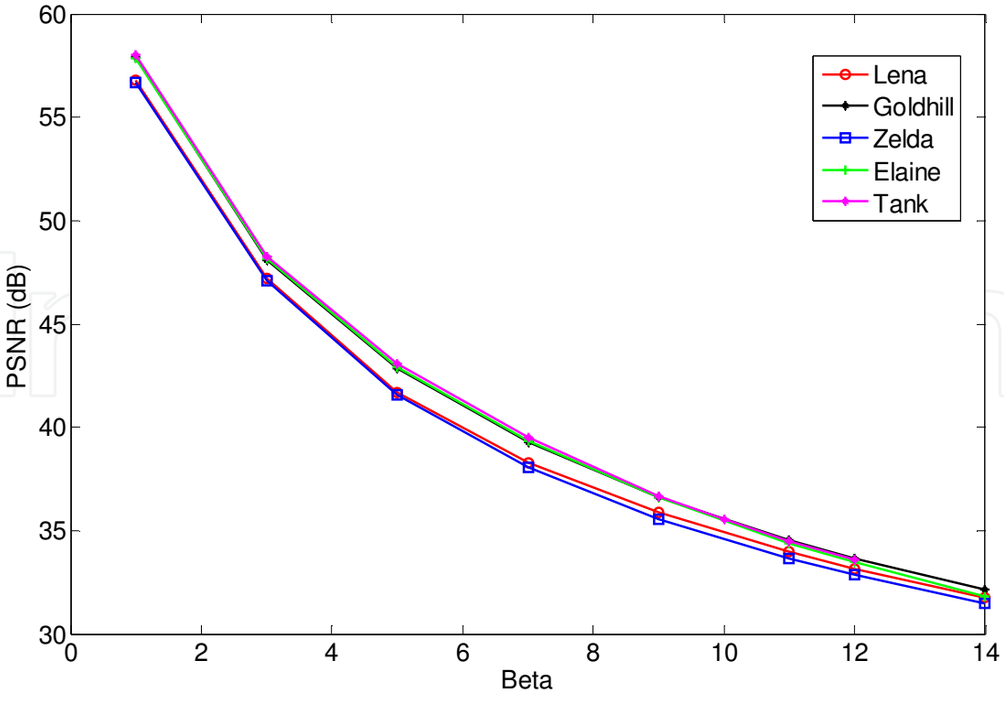


Fig. 5. The relationship between PSNR and β.

The PSNR value is approximately linear decreased as β increased. Actually, the larger the value of β, the more robust performance can be obtained by the proposed method. The PSNR is defined by

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}, \tag{7}$$

where $MSE = \frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{M} (\hat{x}(i,j) - x(i,j))^2$. Here $x(i,j)$ and $\hat{x}(i,j)$ denote the pixel values of the original image and the marked image. Figure 6 shows the marked images generated by the proposed method with β=12. Their average PSNR value was 33.35 dB with an embedding rate of 0.125 bits per pixel (bpp). It can be seen that the perceptual quality was acceptable.

(a) (b) (c)

(d) (e)

Fig. 6. The marked images generated by the proposed FBBE algorithm. (a) Lena, (b) Goldhill, (c) Zelda, (d) Elaine, and (e) Tank.

For comparison, two graceful schemes, namely, Ni et al.'s algorithm (Ni et al., 2008) and Zeng et al.'s approach (Zeng et al., 2010) are compared with our method. Table 1 indicates the performance comparison of these methods on three test images. From Fig. 5 and Table 1 we can see that the proposed method with β =5 (or β of which value being less than 6) provides the largest payload among these methods while the PSNR for the proposed method is superior to that for the other two techniques. Moreover, Table 1 shows that the average hiding capacity provided by the proposed method is two times that achieved by Zeng et al.'s approach (Zeng et al., 2010), and five times larger than that achieved by Ni et al.'s algorithm (Ni et al., 2008).

Methods	Images			
	Lena	*Zelda*	*Goldhill*	Average
Ni et al.'s algorithm	6,336/ 40.19	4,480/ 40.47	6,336/ 40.18	5,717/ 40.28
Zeng et al.'s approach	16,384/ 38.07	16,384/ 38.09	16,384/ 38.10	16,384/ 38.09
Proposed Method	32,768/ 41.71	32,768/ 41.56	32,768/ 42.84	32,768/ 42.04

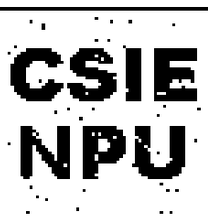
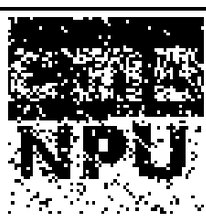
Table 1. Hiding performance (Payload/ PSNR) comparison between various methods.

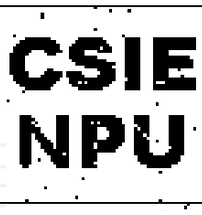
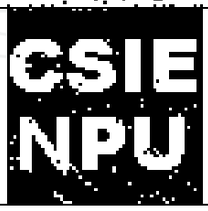
To demonstrate the robustness performance of the proposed method, examples of extracted watermarks after various manipulations of the image are given in Table 2. A logo of size 63×63 with 8 bits/pixel 2 colours was used as the test watermark, as shown in Fig. 7. The bit correct ratio (BCR) is also included. The BCR is defined by

$$BCR = \left(\sum_{i=0}^{ab-1} \overline{w_i \oplus \tilde{w}_i} \Big/ a \times b \right) \times 100\%, \tag{8}$$

Fig. 7. The test watermark.

where w_i and $\tilde{w}_i$ represent the values of the original watermark and the extracted watermark respectively, as well as the size of a watermark is $a \times b$. Note that a majority-vote decision was employed during bits extraction. Although the BCR for those watermarks, which extracted from the images that gone through attacks such as JPEG2000, JPEG, equalized, interleaved, and inversion are not high, they are identifiable. Although the BCR for the watermark extracted from an image which manipulated by inversion attack is only 1.99%, it is recognizable. Furthermore, Fig. 8 shows the BCR performance of the survived watermarks under a variety of degree of Uniform/Gaussian noise additions attacks. From the figure we can see that the proposed method is more robust against Uniform than Gaussian noise additions attacks. Similarly, Fig. 9 indicates the proposed method has the better performance in resisting JPEG200 than JPEG attacks. Figure 10 shows that the proposed method is nearly free from brightness attacks. Finally, Fig. 11 indicates that the extracted watermarks are tolerant of colour quantization attack even if the number of level of pixel-value in a marked image is reduced to 8.

Attacks	Survived Watermarks	Attacks	Survived watermarks
Cropping (50%) BCR =87.88 %		Brightness (+90%) BCR = 87.45%	
JPEG2000 (CR*=8.33) BCR=71.89%		Brightness (-100%) BCR = 89.65%	
JPEG (CR=5.54) BCR=75.36%		Contrast (40%) BCR = 87.48%	
Uniform noise (5%) BCR = 78.94%		Contrast (-15%) BCR = 78.18%	
Gaussian noise (4%) BCR = 74.38%		Posterized (8-level) BCR = 85.26%	
Edge sharpening BCR = 98.92%		Equalized BCR = 80.78%	
Mean filtering (3×3) BCR = 98.34%		Interleaved (Odd) BCR = 54.14%	

Attacks	Survived Watermarks	Attacks	Survived watermarks
Median filtering (3×3) BCR = 98.76%		Interleaved (Even) BCR = 53.87%	
Quantization† BCR = 95.67%		Inversion BCR = 1.99%	

*CR stands for compression ratio, which is defined as the ratio of the size of a host image to that of a compressed image.
†The last four bits of the pixel in the marked image were truncated.

Table 2. Examples of watermarks extracted from image *Lena*. (β=12)

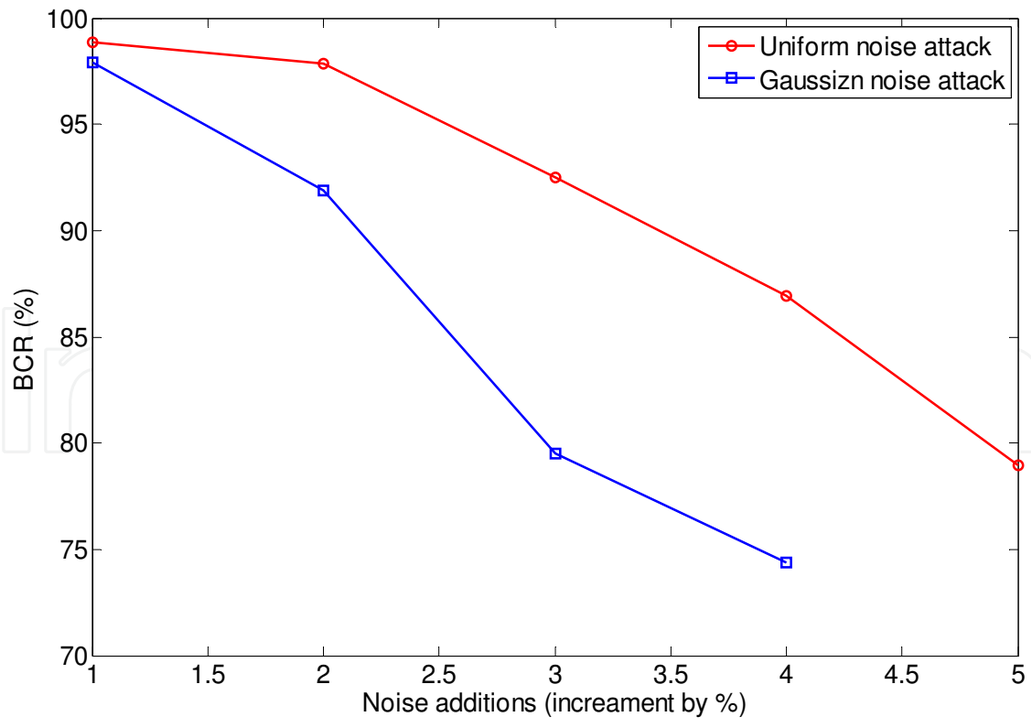


Fig. 8. The BCR for the proposed method under Uniform/Gaussian noise additions attacks, respectively.

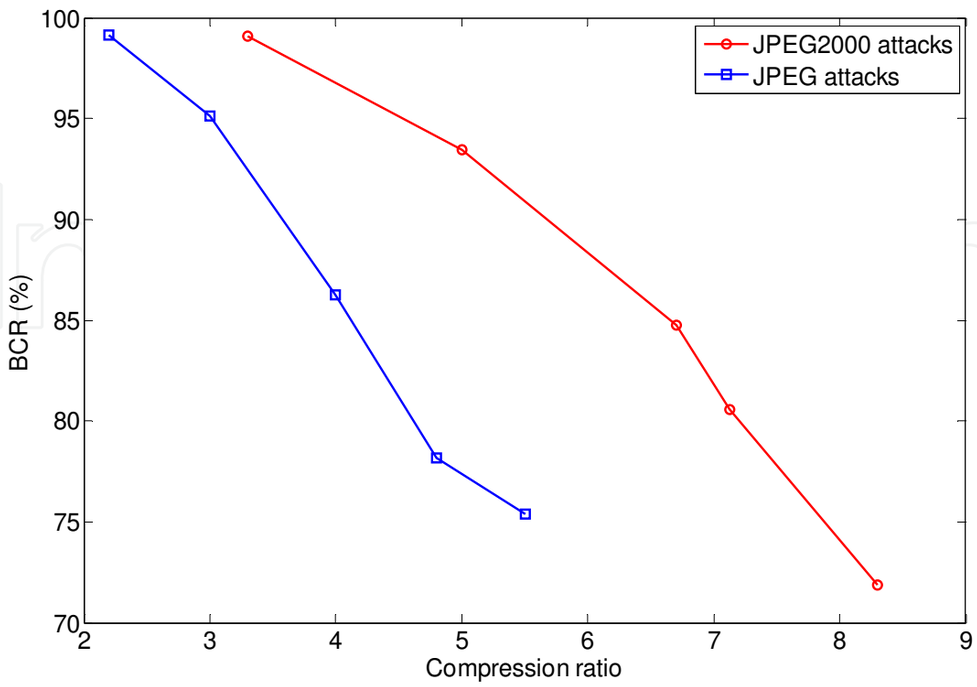


Fig. 9. The BCR for the proposed method under JPEG2000/JPEG attacks, respectively.

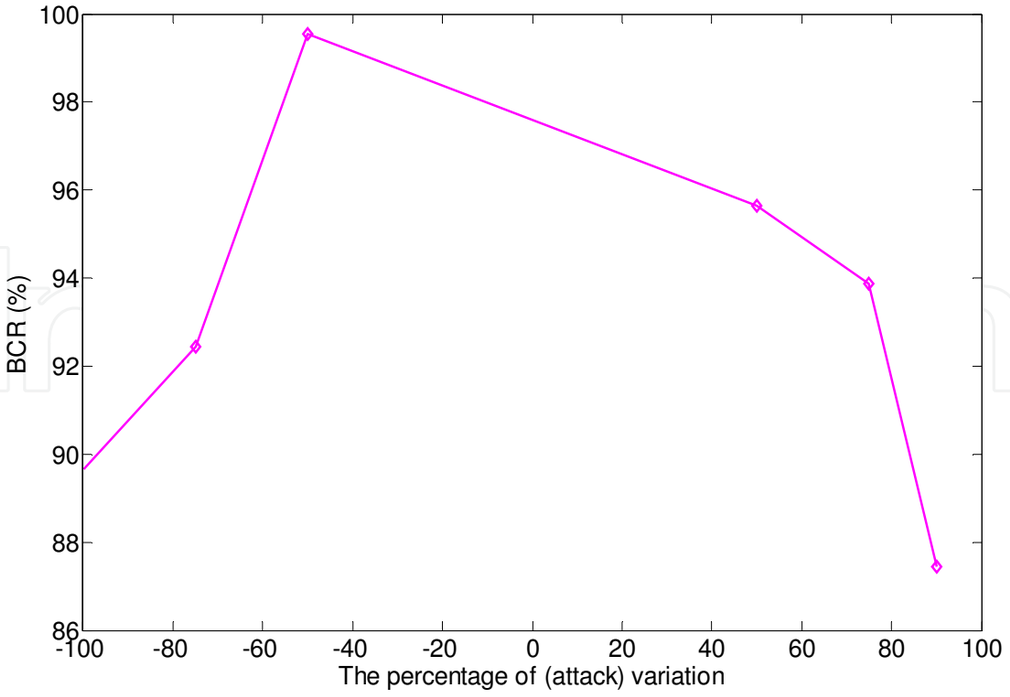


Fig. 10. The BCR for the proposed method under Brightness attacks.

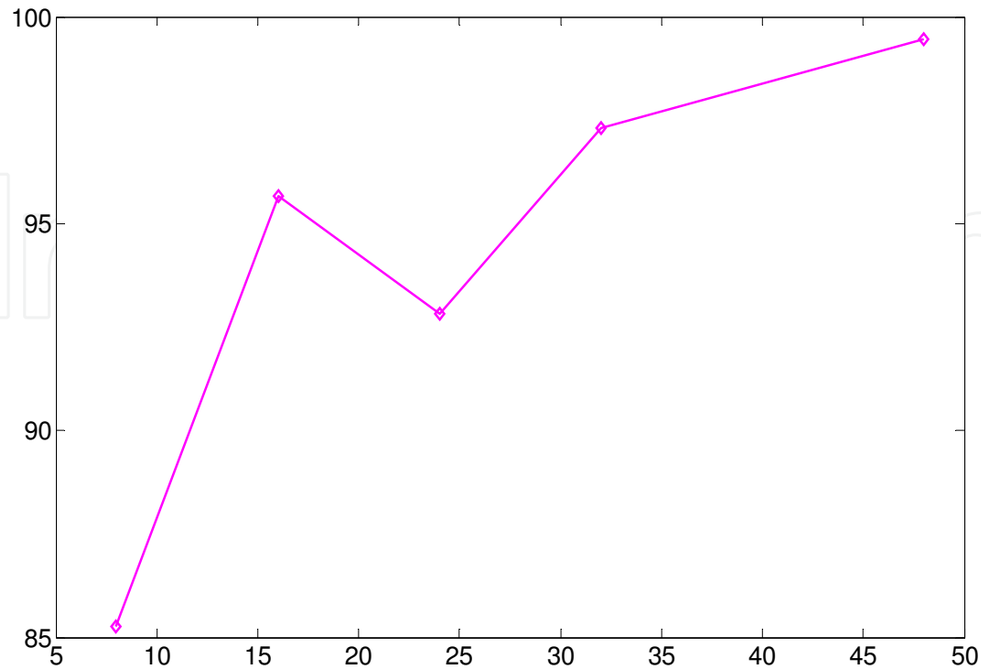


Fig. 11. The BCR for the proposed method under (color) quantization attacks.

3.2 Simulations of high-performance hiding scheme

The trade-off between PSNR and payload for the proposed scheme was depicted in Figure 12. The figure indicated that the average PSNR achieved by the proposed scheme was approximately 55 dB at a bit rate of 0.236 bpp. Whereas, the optimal PSNR value of 37.76 dB can be achieved in image *Zelda* with bit rate of 0.747 bpp. In addition, the relationship between payload (or embedding rate) and robustness parameter β was drawn in Fig. 13. From the figure we can see that the larger the value of β, the higher the bit rate was achieved.

For comparison, three outstanding approaches: Wu et al.'s scheme (Wu et al. 2009), Lee et al.'s algorithm (Lee et al., 2010), and Yang & Tsai's technique (Yang & Tsai, 2010) were compared with our method. Performance comparison between these methods was given in Table 3. It is obvious that the proposed method provides the largest payload among these methods while the PSNR for the proposed method is superior to that for the other three algorithms. Moreover, Table 3 implies that the hiding capacity provided by the proposed method is approximately two times that achieved by the Wu *et al.*'s scheme (Wu et al. 2009), and is two times that achieved by Lee et al.'s algorithm (Lee et al., 2010). Moreover, Table 4 revealed the superiority of our scheme when the PSNR value around 43 dB. The average embedding rate for the proposed scheme was two times larger than that for the Wu et al.'s technique (Wu et al. 2009).

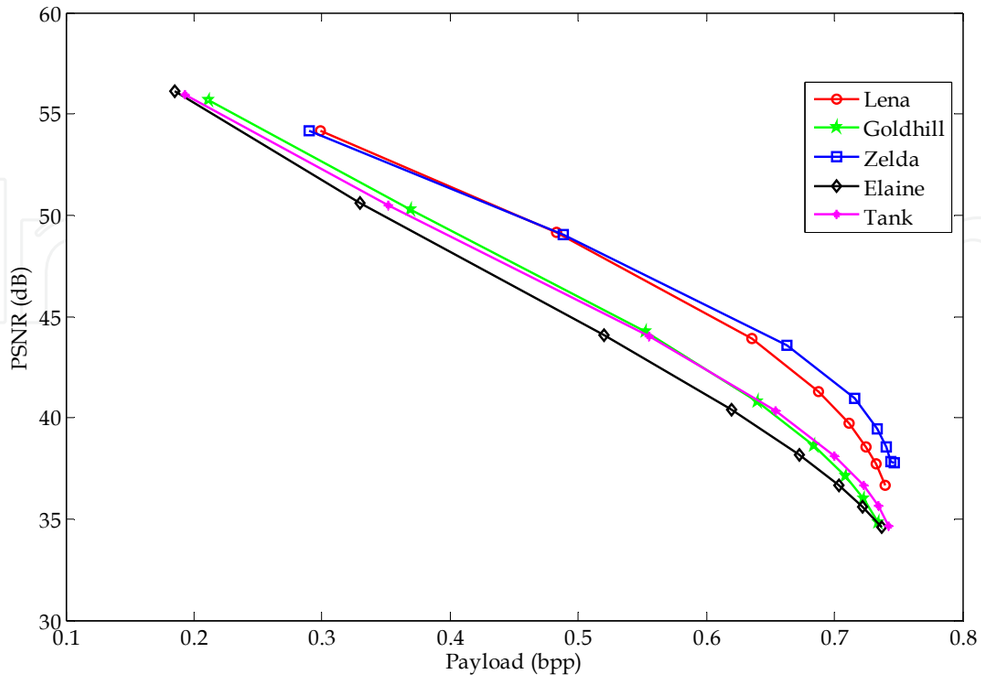


Fig. 12. The trade-off between payload and PSNR for the proposed scheme.

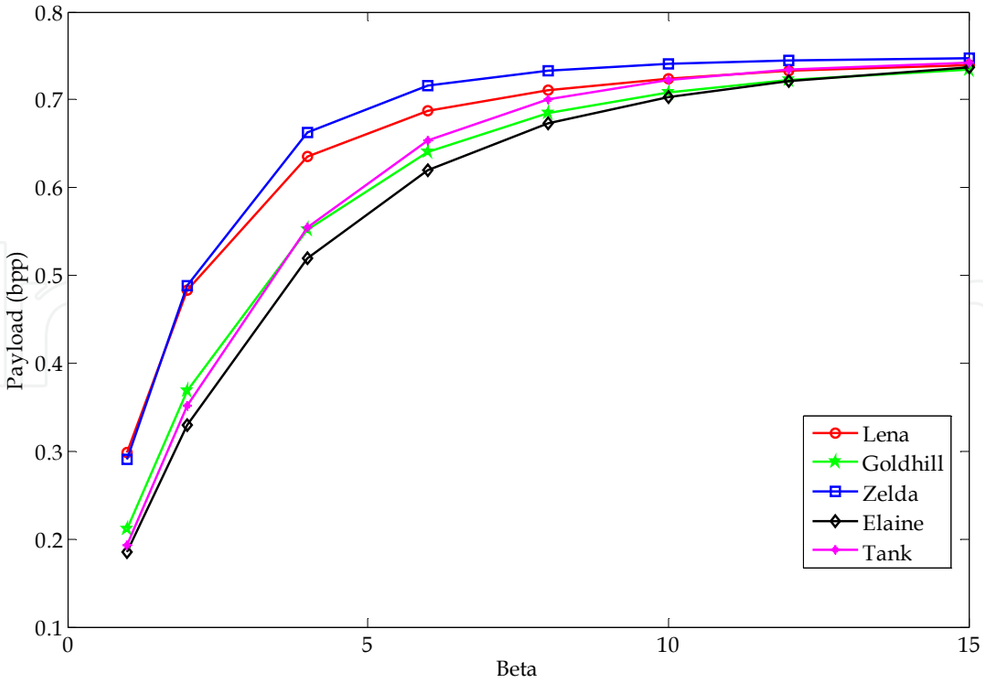


Fig. 13. The relationship between payload and β.

Methods	Images				
	Lena	*Zelda*	*Goldhill*	*Peppers*	Average
Wu et al.'s scheme	0.20/ 47.55	0.19/ 47.75	0.15/ 48.25	0.37/ 48.25	0.23/ 47.95
Lee et al.'s algorithm	0.23/ 48.25	0.18/ 48.25	-	0.17/ 48.25	0.20/ 48.25
Yang & Tsai's technique	0.38/ 48.81	-	0.26/ 48.81	0.33/ 48.81	0.33/ 48.81
Proposed method	0.48/ 49.14	0.49/ 49.02	0.40/ 50.27	0.43/ 49.37	0.45/ 49.45

Table 3. Embedding rate and PSNR performance comparison between various methods when PSNR value was approximately 48 dB.

Methods	Images				
	Lena	*Zelda*	*Goldhill*	*Peppers*	Average
Wu et al.'s scheme	0.24/ 43.60	0.40/ 43.60	0.28/ 43.60	0.23/ 43.60	0.29/ 43.60
Lee et al.'s algorithm	0.53/ 43.15	0.42/ 43.15	-	0.41/ 43.15	0.46/ 43.15
Yang & Tsai's technique	0.62/ 43.84	-	0.45/ 43.84	0.55/ 43.84	0.54/ 43.84
Proposed method	0.64/ 43.94	0.66/ 43.56	0.55/ 44.24	0.60/ 43.75	0.61/ 43.87

Table 4. Embedding rate and PSNR performance comparison between various methods when PSNR value was approximately 43 dB.

4. Conclusion

In this chapter, we first propose a robust lossless data hiding via the feature-based bit embedding (FBBE) algorithm based on integer wavelet transform (IWT). Data bits can be effectively carried by the IWT blocks via the FBBE algorithm and the hidden message can be successfully identified later at the receiver. Moreover, the FBBE algorithm can completely recover the host media if the marked image remains intact, and extract (most part of) the hidden message if manipulations were intentionally (or unintentionally) altered to the marked images. In addition, we employ a smart arrangement of the IWT coefficients so as to provide a high-capacity lossless data hiding scheme. Simulations validate that the marked images generated by the proposed FBBE algorithm are robust to a variety of attacks such as JPEG2000, JPEG, cropping, noise additions, (colour) quantization, bits truncation,

brightness/contrast, mean/median filtering, and inversion. Furthermore, the payload and PSNR provided by the proposed two methods outperform those provided by existing schemes.

The proposed two methods can be extended to color images by embedding data bits in the RGB system separately. In addition, to further enlarge the hiding storage of the FBBE algorithm, an extra one (or two) data bits could be hidden in each IWT coefficients block during data embedment. However, a tradeoff between PSNR and payload size may be a problem with this algorithm. These issues will be discussed in detail in future work. Furthermore, to reduce memory space and transmission delay, the decreasing of the overhead bits will be our future study.

5. References

Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE T. Image Processing*, Vol. 13, No. 8, pp. 1147-1156.

Al-Qaheri, H.; Mustafi, A. & Banerjee, S. (2010). Digital Watermarking using Ant Colony Optimization in Fractional Fourier Domain. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 1, No. 3, pp. 179-189.

Calderbank, A.R.; Daubechies, I.; Sweldens, W. & Yeo, B.L. (1998). Wavelet transforms that map integers to integers. *Applied & Computational Harmonics Analysis*, Vol. 5, No. 3, pp.332-369.

Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J. & Kalker T. (Ed(s.)) (2008). *Digital Watermarking and Steganography*, 2nd Ed., Morgan Kaufmann., MA.

Fan, L.; Gao, T. & Yang Q. (2011). A novel watermarking scheme for copyright protection based on adaptive joint image feature and visual secret sharing. *International Journal of Innovative Computing, Information and Control,* Vol. 7, No. 7(A), pp. 3679-3694.

Gu, Q. & Gao, T. (2009). A novel reversible watermarking algorithm based on wavelet lifting scheme. *ICIC Express Letters*, Vol. 3, No. 3 (A), pp. 397-402.

Hu, Y., Lee; H. K. & Li, J. (2009). DE-based reversible data hiding with improved overflow location map. *IEEE T. Circuits and Systems for Video Technology*. Vol. 19, No. 2, pp. 250-260.

Hsiao, J. Y.; Chan, K.F. & Chang, J.M. (2009). Block-based reversible data embedding. *Signal Processing*, Vol. 89, pp. 556-569.

Lai, C.C.; Huang, H.C. & Tsai, C.C. (2010). A digital watermarking scheme based on singular value decomposition and micro-genetic algorithm. *International Journal of Innovative Computing Information and Control*, Vol. 5, No. 7, pp. 1867-1873.

Lee, C.F.; Chen, H.L. & Tso, H.K. (2010). Embedding capacity raising in reversible data hiding based on prediction of different expansion. *The Journal of Systems and Software*, Vol. 83, pp. 1864-1872.

Lin, C.C. & Shiu, P.F. (2010). High capacity data hiding scheme for DCT-based images. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 1, No. 3, pp. 220-240.

Liu, J. C. & Shih, M. H. (2008). Generalization of pixel-value differencing staganography for data hiding in images. *Fundamenta Informaticate*, Vol. 83, pp. 319-335.

Martinez-Noriega, R.; Nakano, M.; Kurkoski, B. & Yamaguchi, K. (2011). High Payload Audio Watermarking: toward Channel Characterization of MP3 Compression. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, No. 2, pp. 91-107.

Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W.; Sun, Q. & Lin, X. (2008). Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE T. Circuits and Systems for Video Technology*, Vol. 18, No. 4, pp. 497-509, 2008.

Qu, Z.G.; Chen, X.B.; Zhou, X.J.; Niu, X.X. & Yang, Y.X. (2010). Novel quantum steganography with large payload. *Optics Communications*, Vol. 283, No. 23, pp. 4782-4786.

Shih, F.Y. (2008). *Digital watermarking and steganography: fundamentals and techniques*. CRC Press, FL.

Tai, W.L.; Yeh, C.M. & Chang, C.C. (2009). Reversible data hiding based on histogram modification of pixel differences. *IEEE T. Circuits and Systems for Video Technology*, Vol. 19, No. 6, pp. 906-910.

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE T. Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896.

Wang, S., Yang, B. & Niu, X. (2010). A secure steganography method based on genetic algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, Vo1. 1, No. 1.

Wu, H.C.; Lee, C.C.; Tsai, C.S.; Chu, Y.P. & Chen, H.R. (2009). A high capacity reversible data hiding scheme with edge prediction and difference expansion. *The Journal of Systems and Software*, Vol. 82, pp. 1966-1973

Xiao, D. & Shih, F.Y. (2010). A reversible image authentication scheme based on chaotic fragile watermark. *International Journal of Innovative Computing, Information and Control,* Vol. 6 No. 10, pp. 4731-4742.

Yamamoto, K. & Iwakiri M. (2010). Real-time audio watermarking based on characteristics of PCM in digital instrument. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 1, No. 2, pp. 59-71.

Yang, C.H. & Tsai, M.H. (2010). Improving histogram-based reversible data hiding by interleaving predictors. *IET Image Processing*, Vol. 4, No. 4, pp. 223-234.

Yang, C.Y.; Hu, W.C. & Lin, C.H. (2010). Reversible data hiding by coefficient-bias algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 1, No. 2, pp. 91-100.

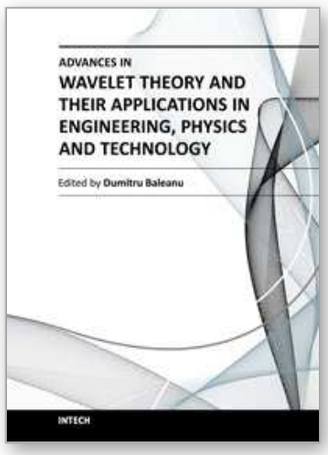
Yang, C.Y.; Hu, W.C.; Hwang, W.Y. & Cheng, Y.F. (2010). A simple digital watermarking by the adaptive bit-labeling scheme. *Int. Journal of Innovative Computing, Information and Control, Vol. 6, No. 3,* pp. 1401-1410.

Yang, C.Y.; Lin, C.H. & Hu, W.C. (2011). Block-based reversible data hiding," *ICIC Express Letters*, Vol. 5, No. 7, pp. 2251-2256.

Zeng, X.T.; Ping, L.D. & Pan, X.Z. (2010). A lossless robust data hiding scheme. *Pattern Recognition*, Vol. 43, pp. 1656-1667.

Zhou, S.; Zhang, Q. & Wei, X. (2010). An image encryption algorithm based on dual DNA sequences for image hiding. *ICIC Express Letters*, Vol. 4, No. 4, pp. 1393-1398.

Zou, D.; Shi, Y.Q.; Ni, Z. & Su, W.A. (2006). A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. *IEEE T. Circuits and Systems for Video Technology*, Vol. 16, No. 10, pp. 1294-1300.



Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology

Edited by Dr. Dumitru Baleanu

ISBN 978-953-51-0494-0
Hard cover, 634 pages
Publisher InTech
Published online 04, April, 2012
Published in print edition April, 2012

The use of the wavelet transform to analyze the behaviour of the complex systems from various fields started to be widely recognized and applied successfully during the last few decades. In this book some advances in wavelet theory and their applications in engineering, physics and technology are presented. The applications were carefully selected and grouped in five main sections - Signal Processing, Electrical Systems, Fault Diagnosis and Monitoring, Image Processing and Applications in Engineering. One of the key features of this book is that the wavelet concepts have been described from a point of view that is familiar to researchers from various branches of science and engineering. The content of the book is accessible to a large number of readers.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen