Hindawi Publishing Corporation
Advances in Multimedia
Volume 2012, Article ID 473896, 9 pages
doi:10.1155/2012/473896

Research Article

Reversible Data Hiding Using Two Marked Images Based on Adaptive Coefficient-Shifting Algorithm

Ching-Yu Yang

Deptartment of Computer Science and Information Engineering, National Penghu University of Science and Technology, No. 300, Liu-Ho Road, Magong 880, Taiwan

Correspondence should be addressed to Ching-Yu Yang, chingyu@npu.edu.tw

Received 30 April 2012; Revised 8 September 2012; Accepted 20 September 2012

Academic Editor: Dimitrios Tzovaras

This paper proposes a novel form of reversible data hiding using two marked images by employing the adaptive coefficient-shifting (ACS) algorithm. The proposed ACS algorithm consists of three parts: the minimum-preserved scheme, the minimum-preserved with squeezing scheme, and the base-value embedding scheme. More specifically, each input block of a host image can be encoded to two stego-blocks according to three predetermined rules by the above three schemes. Simulations validate that the proposed method not only completely recovers the host medium but also losslessly extracts the hidden message. The proposed method can handle various kinds of images without any occurrence of overflow/underflow. Moreover, the payload and peak signal-to-noise ratio (PSNR) performance of the proposed method is superior to that of the conventional invertible data hiding schemes. Furthermore, the number of shadows required by the proposed method is less than that required by the approaches which are based upon secret image sharing with reversible steganography.

1. Introduction

Due to ubiquitous broadband services and high-speed networks provided by Internet service providers (ISPs), along with mass production of high-capacity and low-cost multimedia devices, individuals and organizations can easily share their information on the Internet. Moreover, thanks to the portability and mobility provided by such wireless communications as intelligent mobile systems, wireless fidelity (Wi-Fi), and worldwide interoperability microaccess (WiMax), people can exchange/retrieve resources anywhere and anytime. Preventing data from being eavesdropped, tampered with, and falsified during transmission has become an important goal. In addition to the use of cryptographic systems, one can use data hiding to achieve this result. Primary applications of data hiding can be found in proof of ownership, content authentication, copyright protection, and covert communications. In general, data hiding can be divided into two categories: digital watermarking and steganography [1, 2]. In digital watermarking, the embedded message (or watermark) is often related to the medium and conveys additional information about the medium. Robust performance is a key feature of the watermarking schemes [3–5]. In steganography, the hidden message often has nothing to do with the host media; however, both hiding capacity and perceived quality are the two areas of concern pursued by the authors [6–8]. One of the major issues of the steganographic approach is that the marked images are susceptible to manipulation. In this scenario, the embedded message cannot be extracted if even a slight alteration is imposed on the marked images. Note that the two above mentioned data hiding techniques are irreversible. Since host media such as medical and military images, geographic systems, and satellite resources can be valuable or even priceless, it is undesirable that the host media be at all damaged after data extraction. Recently, several researchers [9–15] have presented lossless data hiding in an effort to address this issue.

Tian [9] used a difference expansion (DE) technique to derive a high-capacity and low-distortion form of reversible watermarking. An image was first divided into pairs of pixels. A secret message was then embedded into the difference of the pixels in each of the pairs that were not expected to cause

Table 1: Three rules of data embedment for each host block.

Input block	Output (two) blocks		
	Rule 1* (BV $< \tau/3$)	Rule 2+ ($\tau/3 \leq$ BV $\leq \tau$)	Rule 3† (BV $> \tau$)
H	S1-A	S1-A	S1-C
	S2-A	S2-B	S2-C

*Both S1 and S2 were introduced by embedding data bits into H via the minimum-preserved scheme (A).
+S1 was introduced by embedding a secret message into H via the minimum-preserved scheme, and S2 was introduced by the BV embedding scheme (B).
†Both S1 and S2 were introduced by embedding data bits into H via the minimum-preserved with squeezing scheme (C).

an overflow or an underflow. For a single-layer embedding, the payload size of the technique was less than 0.5 bits per pixel (bpp). Alattar [10] extended Tian's algorithm using a DE of vectors, instead of pairs, to improve the performance of the algorithm. In a single pass, Alattar's algorithm can embed several bits in every vector. In addition to grayscale images, the algorithm can effectively be applied to color systems. Lin et al. [11] proposed a multilayer scheme for reversible data hiding based on the modification of the difference histogram. By combining the peak point of a difference image with a multilevel hiding strategy, the scheme maintained high capacity while keeping distortion low. In the fifteenth-level embedding, the optimal payload surpassed 5×10^5 bits with a peak signal-to-noise ratio (PSNR) value of 25.39 dB. To obtain a reversible watermarking technique, Zeng et al. [12] used adjacent pixel difference and multilayer embedding techniques on a scan path. Specifically, they employed nine predetermined scan paths to dig out space for hiding bits. The multilayer embedding technique did increase the hiding capacity. To improve the performance of the conventional difference expansion methods, Wu et al. [13] presented a high-capacity reversible data hiding scheme based on the JPEG-LS predictive technique and the multiple-base notational system. In using the JPEG-LS predictive technique, the distortion of the marked images can be significantly reduced. Moreover, the multiple-base notational system can effectively increase the hiding storage capacity. Simulations indicate that their method can provide a high embedding capacity while preserving the quality of the perceived results. Yang and Tsai [14] suggested a reversible (multilevel) data hiding method based upon an interleaving prediction. All predictive values were transformed into a histogram to generate high peak values and improve the hiding capacity. For each pixel, the difference in value between the original image and the marked one remained within ± 1. This guaranteed that the PSNR of the marked image was around 48 dB. Moreover, in the twelfth-level embedding, the optimal payload surpassed 3.5×10^5 bits with a PSNR value of 29.26 dB. Yang and Hu [15] proposed a lossless data hiding method based on the minimum/maximum preserved with overflow/underflow avoidance (MMPOUA) algorithm. First, the MMPOUA algorithm kept the minimum (or maximum) pixel of a host block unchanged. A difference block was introduced by subtracting the pixels remaining in the block from the minimum (or maximum) one. Following pixel adjustment, data bits were embedded in the difference blocks. Simulations showed that the MMPOUA algorithm not only generated good hiding capacity but also high perceived quality, especially at a moderate rate of embedding.

To enlarge the hiding storage, the idea of a secret sharing scheme, namely, the (t, n) threshold scheme invented by Shamir [16], was employed and extended to image hiding and authentication [17–23]. Moreover, to fully recover the host image and losslessly extract the hidden message, researchers [24, 25] presented reversible secret image sharing with steganography. However, a (t, n) threshold of secret image sharing with steganography often requires $t \leq n$ and $n \geq 3$. As result, a large size of storage is an inevitable requirement.

In this paper, we present the adaptive coefficient-shifting (ACS) algorithm to losslessly embed a secret message into a host image. The ACS algorithm requires less number of shadows than the techniques based upon reversible secret image sharing with steganography. In addition, both the payload and the PSNR for the ACS algorithm are far larger than that of the existing invertible data hiding schemes. The rest of the paper is organized as follows. Section 2 describes the ACS algorithm, including the minimum-preserved scheme, the minimum-preserved with squeezing scheme, the base-value (BV) embedding scheme, and the prevention of overflow/underflow. Section 3 presents the simulation results and also includes performance comparisons. Section 4 offers the conclusions.

2. Proposed AdaptiveCoefficient-Shifting (ACS) Algorithm

The proposed ACS algorithm consists of three parts: the minimum-preserved scheme, the minimum-preserved with squeezing scheme, and the base-value embedding scheme. Namely, each input (host) block can be encoded to two stego-blocks according to the three predetermined rules listed in Table 1. For example, the two blocks stego-block 1 (S1) and stego-block 2 (S2) can be generated by embedding data bits into a host block (H) via the minimum-preserved scheme, when the BV of the block is less than $\tau/3$. The term τ is a control parameter. The details of the ACS algorithm are specified in the following subsections. In addition, the BV of the block will be defined later in Section 2.3.

2.1. The Minimum-Preserved Scheme. Table 1 indicates that both S1 and S2 can be generated by the minimum-preserved scheme when the BV of the host block is less than $\tau/3$. In addition, a stego-block S1 can be generated by the minimum-preserved scheme if the BV of the host block satsifies $\tau/3 \leq$ BV $\leq \tau$. The details of the minimum-preserved scheme are described in the following sections.

2.1.1. Bit Embedding. Let $P = \{p_{ij}\}_{i=0}^{n\times n-1}$ be the jth non-overlapping block of size $n \times n$ that is divided from an input image. A difference block $\{\hat{p}_{ij}\}_{i=0}^{n\times n-1}$ can be obtained by

$$\left\{\hat{p}_{ij}\right\}_{i=0}^{n\times n-1} = \left\{p_{ij}\right\}_{i=0}^{n\times n-1} - m_j, \tag{1}$$

where $m_j = \text{Min}\{p_{ij}\}_{i=0}^{n\times n-1}$ indicates the minimum pixel value of the jth block. To maintain low levels of distortion, an isolation process can be subsequently conducted to $\hat{p}_{ij}$ to obtain a new value $\widehat{p}_{ij}$ according to the following criteria:

$$\widehat{p}_{ij} = \hat{p}_{ij} + \left(2^k - 1\right)\beta \quad \text{if } \hat{p}_{ij} \geq \beta. \tag{2}$$

The term β is a control parameter and k is an integer. Namely, no data bits would be carried by the isolated coefficients. After adjustment, data bits are ready to be embedded into $\hat{p}_{ij}$ with $0 \leq \hat{p}_{ij} < \beta$, by multiplying $\hat{p}_{ij}$ by 2^k to obtain $\breve{p}_{ij}$ and adding an input data to $\breve{p}_{ij}$. Finally, a stego-block is formed by adding m_j to $\widehat{p}_{ij}$ and $\breve{p}_{ij}$, respectively.

2.1.2. Bit Extraction. Let $Q = \{q_{ij}\}_{i=0}^{n\times n-1}$ be the jth hidden block of the stego-image and $m_j = \text{Min}\{q_{ij}\}_{i=0}^{n\times n-1}$ the minimum pixel value of the block. The coefficients of the jth difference block $\{\hat{q}_{ij}\}_{i=0}^{n\times n-1}$are acquired using $\{\hat{q}_{ij}\}_{i=0}^{n\times n-1} = \{q_{ij}\}_{i=0}^{n\times n-1} - m_j$. Then, data bits can be extracted from a difference block. If $0 \leq \hat{q}_{ij} < 2^k\beta$, then the data bits are obtained by applying modulo-2^k operation. Subsequently, the pixels $\hat{q}_{ij}$ which hid the data bit can be restored by computing $\hat{q}_{ij} = \lfloor \hat{q}_{ij}/2^k \rfloor$. The pixels $\hat{q}_{ij}$ which satisfy $\hat{q}_{ij} \geq 2^k\beta$ were subtracted from $(2^k - 1)\beta$ in order to recover the pixels which contained no data bits. Notice that $\lfloor x \rfloor$ is the floor function. Finally, a host block can be restored by adding m_j to all the coefficients except the minimum pixel of the difference block.

2.2. The Minimum-Preserved with Squeezing Scheme. To provide even further capacity, the minimum-preserved with squeezing scheme can be used to embed data bits into the blocks classified by Rule 3 of Table 1. A major distinction between the minimum-preserved scheme and the minimum-preserved with squeezing scheme is that the latter scheme employs a squeezing technique which can effectively dig out extra hiding space. The minimum-preserved with squeezing scheme is summarized in the following subsections.

2.2.1. Bit Embedding and Extraction. As a difference block was obtained by $\{\hat{p}_{ij}\}_{i=0}^{n\times n-1} = \{p_{ij}\}_{i=0}^{n\times n-1} - m_j$, the squeezing process adjusted $\hat{p}_{ij}$ to a new value $\widetilde{p}_{ij} = \hat{p}_{ij} - \gamma$ if $\hat{p}_{ij} > \gamma$, where γ is a control parameter. Note that a bitmap was used here to flag whether or not a coefficient of the block had undergone adjustment. To help the decoder to later extract the data bits, overhead information can be losslessly compressed and sent by an out-of-band transmission to the receiver. After the squeezing process, the isolation process and bit embedding mentioned in Section 2.1.1 can be sequentially performed on the difference block.

The bit extraction of the minimum-preserved with squeezing scheme that uses the bitmap as a look-up table is similar to that of the minimum-preserved scheme (see Section 2.1.2). After bit extraction, to restore the original difference coefficients which had undergone adjustment, the term γ has to be added to the temporary difference block if the corresponding flag in the bitmap was set at 1. Subsequently, the original pixels can be recovered by adding m_j to all the coefficients except the minimum pixel of the difference block.

2.2.2. Overhead Information Analysis. The number of bits for the bitmap is $s \times n^2$ with s denoting the occurrence of the blocks encoded by the minimum-preserved with squeezing scheme. The overhead information can be significantly reduced if $(s/\lfloor M/n \rfloor \times \lfloor N/n \rfloor) \times 100\% \leq 40\%$, where the image size is $M \times N$. This can be achieved by adjusting the value of τ during data embedding.

2.3. BV Embedding Scheme. According to Rule 2 of Table 1, the minimum-preserved scheme and the BV embedding scheme can be used to generate stego-blocks 1 and 2, respectively, when the BV of the host block satisfies $\tau/3 \leq \text{BV} \leq \tau$. Let b_j be the BV of the jth block. The term b_j is defined by

$$b_j = C_{\max} - C_{\min} + 1, \tag{3}$$

where $C_{\min} = \text{Min}\{p_{ij}\}_{i=0}^{n\times n-1}$ and $C_{\max} = \text{Max}\{p_{ij}\}_{i=0}^{n\times n-1}$ represent the minimum and maximum pixel value of the block. A difference block $\{\hat{p}_{ij}\}_{i=0}^{n\times n-3}$ can be obtained by

$$\left\{\hat{p}_{ij}\right\}_{i=0}^{n\times n-3} = \left\{p_{ij}\right\}_{i=0}^{n\times n-3} - C_{\min}. \tag{4}$$

Note that the minimum and the maximum pixel values of the block remain intact. The main idea of the BV embedding scheme is the addition of the difference block $\{\hat{p}_{ij}\}_{i=0}^{n\times n-3}$ to an input bit stream. More specifically, let the binary bit stream with the length of L to be embedded into $\{\hat{p}_{ij}\}_{i=0}^{n\times n-3}$ be $B = \{\phi_i\}_{i=0}^{L-1} = \sum_{i=0}^{L-1}\phi_i 2^i$. Transform B into $B = \sum_{i=0}^{n^2-3}\eta_i b_j^i = (\eta_{n^2-3}, \ldots, \eta_1, \eta_0)_{b_j}$ with BV of b_j. The resulting jth stego-block $\{\widetilde{p}_{ij}\}_{i=0}^{n^2-3}$ is obtained by

$$\left\{\widetilde{p}_{ij}\right\}_{i=0}^{n^2-3} = \left\{\hat{p}_{ij} + \eta_i + C_{\min}\right\}_{i=0}^{n^2-3}. \tag{5}$$

Notice that the locations of both the minimum and the maximum pixels must be adjusted to the top-left of the block before the addition of data (η_i) and restored to their original locations after the addition of the minimum pixel ($C_{\min}$).

At the receiver, instead of retrieving the BV from the stego-block 2, we compute the BV $b'_j = D_{\max} - D_{\min} + 1$, where $D_{\max}$ and $D_{\min}$ represent the maximum and minimum pixel values of the host block. These values have been previously restored by the minimum-preserved scheme from the stego-block 1. Let $Q = \{q_{ij}\}_{i=0}^{n\times n-1}$ be the jth hidden block which is derived from stego-image 2. The difference pixels of the jth block can be acquired using

$$\left\{\hat{q}_{ij}\right\}_{i=0}^{n\times n-3} = \left\{q_{ij}\right\}_{i=0}^{n\times n-3} - D_{\min}. \tag{6}$$

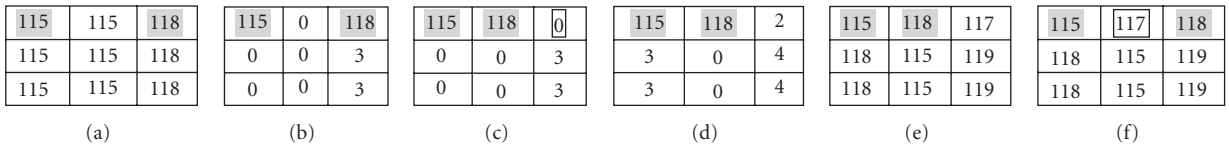


Figure 1: Example of data embedment with an input data digits of $(103\ 103\ 2)_4$. (a) A host block, (b) a difference block; (c) adjust the maximum pixel value (118) to the top-left of the block; (d) add each data digit to the coefficients of the block in reverse order, (e) a hidden block, and (f) the resultant stego-block 2.

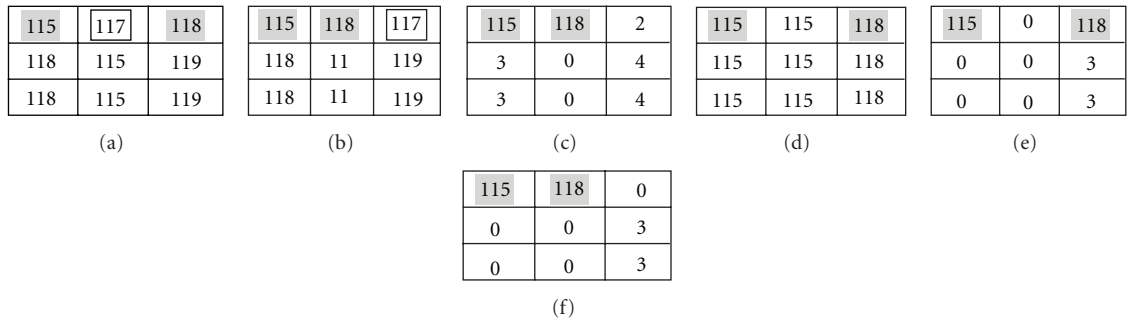


Figure 2: Example of data extraction. (a) The stego-block 2, (b) after the adjustment of the maximum pixel value, (c) the difference block, (d) the host block restored from the stego-block 1, (e) the difference block of (d), and (f) after adjustment the maximum pixel value. The hidden digits can be extracted by subtracting the coefficients in (c) from those in (f); respectively, the extracted digits was $(103\ \ 103\ \ 2)_4$.

Then treat the n^2-3 digit number

$$\left\{\eta'_{ij}\right\}_{i=0}^{n^2-3} = \left\{\hat{q}_{ij} - \hat{p}_{ij}\right\}_{i=0}^{n^2-3} \tag{7}$$

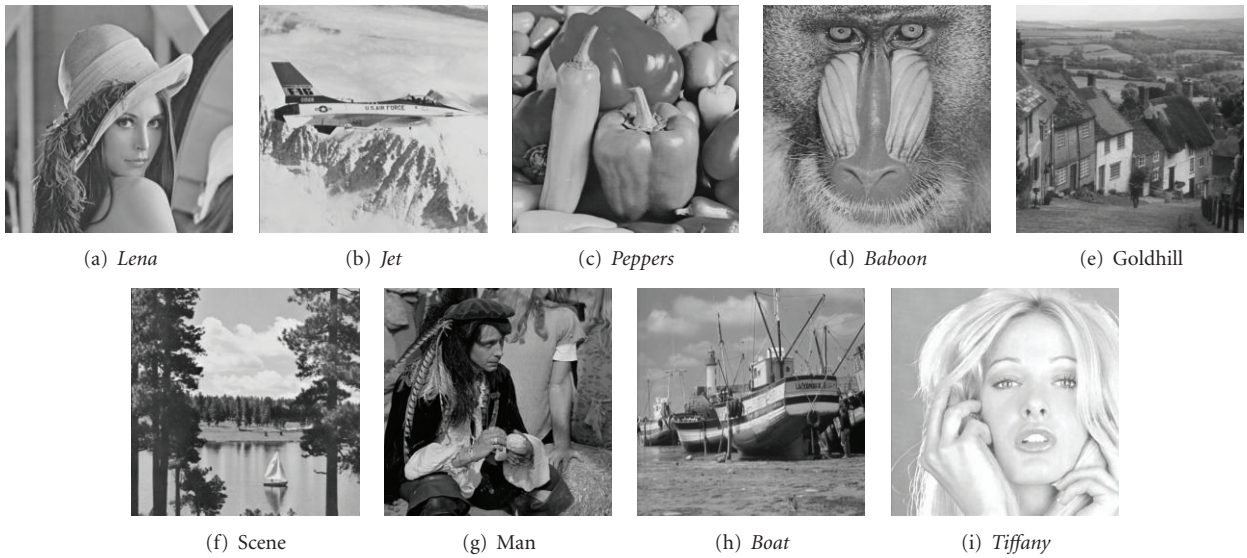
as a BV of b'_j number, and convert the number $\{\eta'_{ij}\}_{i=0}^{n^2-3}$ to the expected number with BV of 2. Note that the coefficients $\{\hat{p}_{ij}\}_{i=0}^{n^2-3}$ have been previously obtained from the stego-block 1 by the minimum-preserved scheme. Notice as well that the number of bits hidden in the block is $L = \lfloor (n^2 - 2)\log_2 b_j \rfloor$. This implies that the length of bits to be embedded into a host block is determined by the BV of b_j.

Figures 1 and 2 present examples of data embedding and extraction by the BV embedding scheme. A host block was shown in Figure 1(a) with the minimum and maximum pixel value of the block denoted by the gray highlighted numbers. The BV of the block is 118 − 115 + 1 = 4. Figure 1(b) shows the difference block which was introduced by subtracting all the pixels except the minimum and maximum ones in Figure 1(a) from 115. Figure 1(c) was obtained by adjusting the maximum pixel value of 118 to the top-left of the block. Note that the corresponding adjusted coefficient in Figure 1(c) was marked by a rectangle. Assume that the secret bit stream $(0100110\ 1001101)_2$ is the 14-bit stream to be embedded in Figure 1(c). Figure 1(d) was acquired by adding the input digits $(0100110\ \ 1001101)_2 = (4942)_{10} = (1031032)_4$ to the cofficients in Figure 1(c) in a raster scan with a reverse order. The hidden block, as shown in Figure 1(e), was generated by adding 115 to each of the coefficients in Figure 1(d). Finally, the stego-block 2 in which the maximum pixel was restored, is shown in Figure 1(f). The mean square error (MSE) computed from Figures 1(a) and 1(f) was 2.67. To extract the hidden data and recover the host block, a similar reverse procedure can be conducted to Figure 1(f). An example of data extraction is given in Figure 2.

2.4. Overflow/Underflow Discussion. Since the minimum pixel value of the block is preserved by the minimum-preserved (with squeezing) scheme, an underflow issue can be prevented. As for the blocks encoded by the BV embedding scheme, the underflow issue could be avoided by adjusting the value of parameter τ. However, if there is a pixel of the block where the value is equal to (or a little less than) 255, an overflow issue can occur during bit embedding. A block skipped policy can be used to solve the issue. Alternatively, the maximum-preserved (with squeezing) scheme, which preserves the maximum pixel value of the block, can be employed in the proposed ACS algorithm to overcome the overflow issue; more precisely, the minimum-preserved (with squeezing) scheme can be replaced by the maximum-preserved (with squeezing) scheme when (1) the host images were incapable of recovering from the stego-images by the former scheme or (2) the number of skipped blocks lies beyond a predefined threshold. Since the process of data embedment and the extraction procedure for the maximum-preserved (with squeezing) scheme is similar to that of the minimum-preserved (with squeezing) scheme, they are skipped here.

3. Experimental Results

Several 512 × 512 gray-scale images, as shown in Figure 3, are used as the host images. One of the host images, *Baboon*, is used as the test data. The size of block is 3 × 3, and the



(a) *Lena* (b) *Jet* (c) *Peppers* (d) *Baboon* (e) Goldhill

(f) Scene (g) Man (h) *Boat* (i) *Tiffany*

FIGURE 3: The host images.

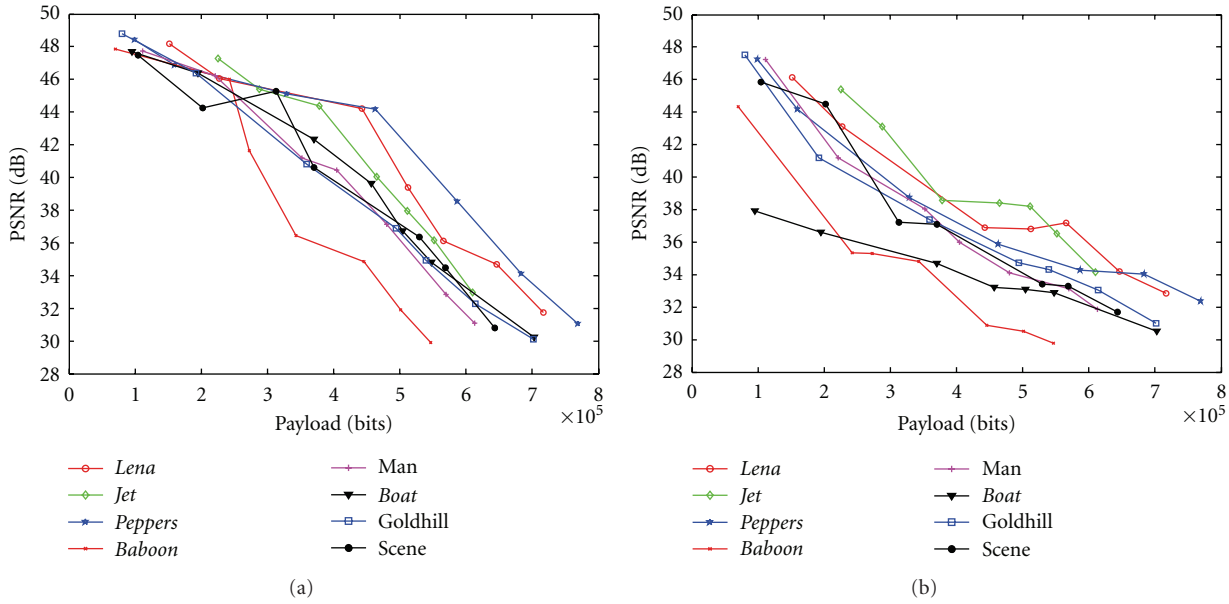


FIGURE 4: The relationship between PSNR and payload for the proposed method on test images. (a) Stego-image 1 and (b) stego-image 2.

integer k is set to 1. A tradeoff between the PSNR (dB) and the payload (in bits) for the stego-images 1 and 2 generated by the proposed method using various β is drawn in Figure 4. Figure 4(a) shows that the payload exceeds 6×10^5 bits for all images except *Baboon*. The optimal PSNRs for the stego-image 1 (Figure 4(a)) and stego-image 2 (Figure 4(b)) are 30.98 dB and 31.78 dB, respectively, with an average payload size of 662,861 bits. Moreover, Figure 4 reveals that the average PSNR value of stego-image 2 is nearly 2 dB below that of stego-image 1 if the payload size is less than 5×10^5 bits. Notice that a block skipped policy was employed on the image *Boat*; however, only 5 blocks were skipped. In addition, two stego-images generated by the proposed method from the images *Lena* and *Baboon*, respectively, are depicted in Figure 5. It can be seen that the perceived quality of these images is acceptable. The average PSNR/payload for the images *Lena* and *Baboon* are 33.73 dB/690,233 bits and 30.36 dB/546,688 bits, respectively. The PSNR is defined by

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}}, \tag{8}$$

where $\text{MSE} = (1/MN) \sum_{i=1}^{N} \sum_{j=1}^{M} (\hat{x}(i,j) - x(i,j))^2$ if the image size is $M \times N$. Here $x(i,j)$ and $\hat{x}(i,j)$ denote the pixel values of the original image and the marked image, respectively. Notice as well that the relation between two

(a) (b)

(c) (d)

Figure 5: Two stego-images generated by the proposed method. (a) Stego-image 1 of *Lena* (33.19 dB), (b) stego-image 2 of *Lena* (34.25 dB), (c) stego-image 1 of *Baboon* (30.41 dB), and (d) stego-image 2 of *Baboon* (30.78 dB).

control parameters β and γ is $\gamma = \beta - 1$. Figure 6 indicates that the payload size varied by a different combination of the parameters β, γ, and τ on the images *Lena* and *Baboon*. The payload is gradually increased as β (or τ) is enlarged. Figure 6 also reveals that the maximum hiding storage provided by the image *Lena* is approximately 2×10^5 bits larger than that provided by the image *Baboon*. To demonstrate the capability of handling the overflow issue, the proposed maximum-preserved (with squeezing) scheme was applied to the image *Tiffany*, which is a typical image often used to test the occurrence of overflow by several existing methods. Simulations confirm not only that the proposed method can losslessly extract the secret message but also that the host image can be fully recovered. Figure 7 presents the experimental results. Figure 7(a) displays the relationship between PSNR and payload. We can see that the performance of stego-image 1 is better than that of stego-image 2 when the payload size is lower than 6.5×10^5 bits. Moreover, Figure 7(b) shows the variations of payload versus the parameters of β, γ, and τ. It presents a similar performance to that of Figure 6(a).

To evaluate our scheme's performance, this subsection compares our scheme with various approaches [11, 13, 14, 20, 22, 24]. Since the PSNR value of Yang and Tsai [14] is better than those of Zeng et al. [12] and Yang and Hu [15] when the payload approaches 1 bpp, the performance comparison does not include both methods. Figure 8 illustrates the comparison between various methods in two test images, *Lena* and *Boat*. Figure 8(a) shows that our method provides the best PSNR with the largest hiding capacity when the payload is larger than 1.70×10^5 bits. Note that the larger the payload, the larger the leading gap. Similarly, Figure 8(b) reveals the superiority of the proposed method when the payload is larger than 1.25×10^5 bits. Table 2 compares our method with the conventional reversible data hiding techniques [11, 13, 14] when the average payload size is larger than 3×10^5 bits with the PSNR around 30 dB. Table 2 indicates that the payload generated by the proposed method is far larger than that generated by the rest of the techniques, while our PSNR is the best among them. Table 2 also implies that it is difficult for the reversible data hiding techniques [11–15] to provide

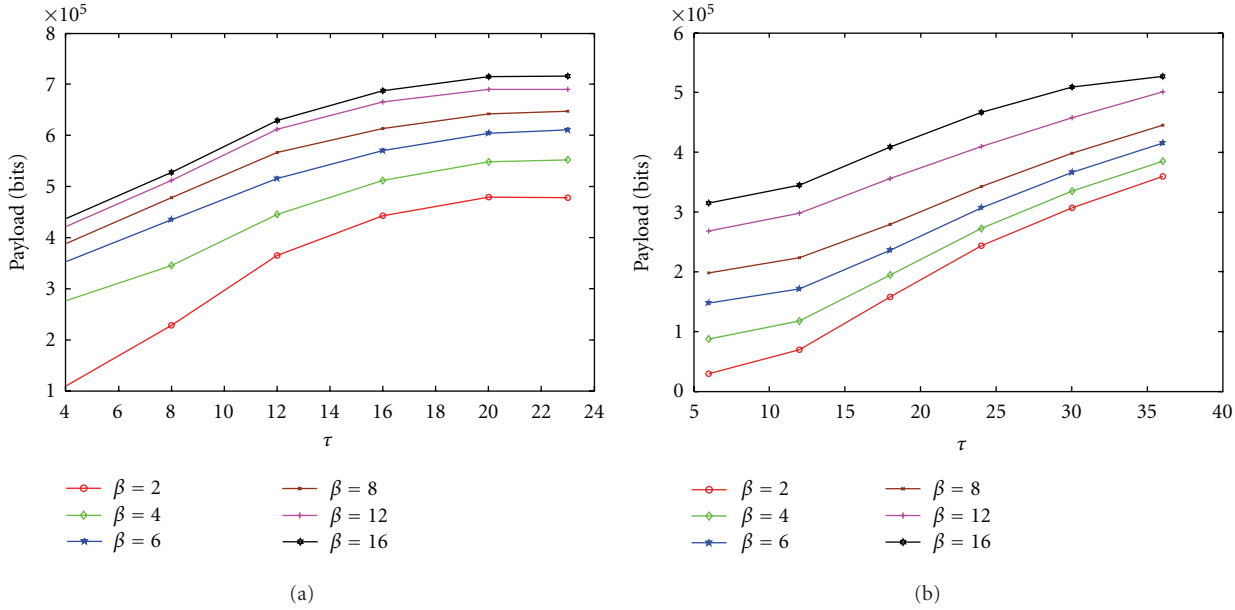


Figure 6: Relationship between the payload and the control parameters β (with $\gamma - 1$) and τ for the proposed method on the test images. (a) *Lena* and (b) *Baboon*.

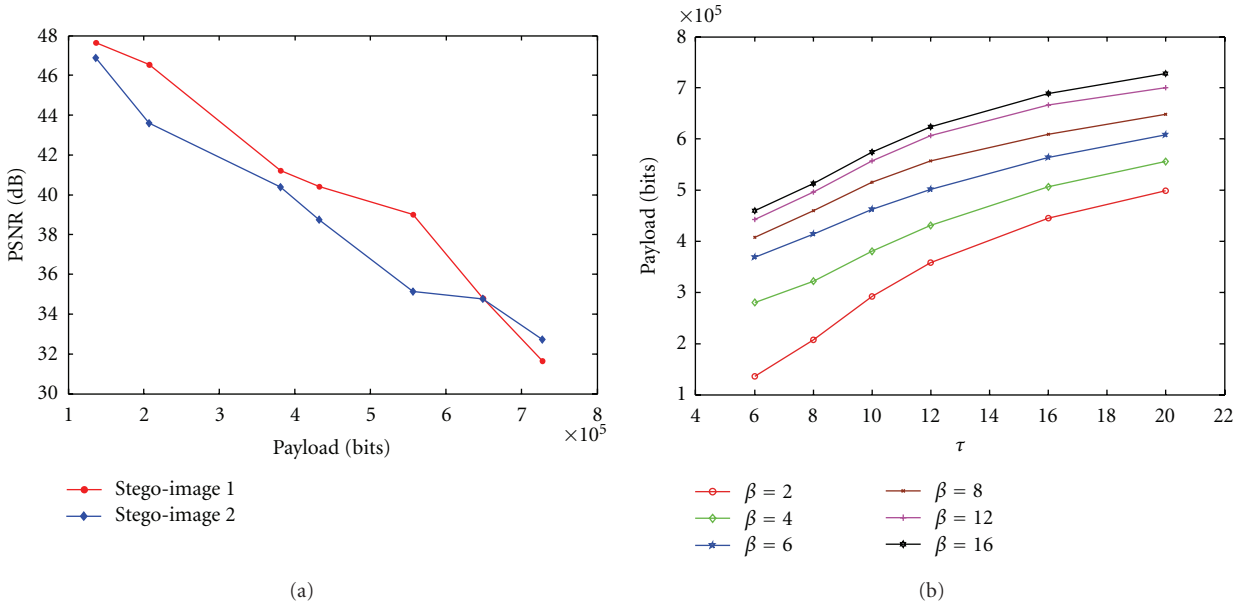


Figure 7: Simulations of the image *Tiffany*. (a) Tradeoff between PSNR and payload and (b) the relationship between the payload and the parameters β (with $\gamma - 1$) and τ.

Table 2: Payload/PSNR performance comparison between various methods (under PSNR value above 30 dB).

Methods	Images				
	Lena	*Jet*	*Peppers*	*Boat*	Average
Lin et al. [11]	346,568/30.19	362,847/30.19	342,175/30.19	314,196/30.19	341,447/30.19
Wu et al. [13]	319,816/30.30	411,566/31.35	322,437/31.54	306,708/31.01	340,132/31.05
Yang and Tsai [14]	385,519/31.65	364,951/31.65	341,202/31.65	280,285/31.65	342,989/31.65
Our method†	716,596/32.29	610,269/33.58	769,364/31.71	702,811/30.60	699,760/32.05

†The average PSNR of stego-image 1 and stego-image 2 was displayed here.

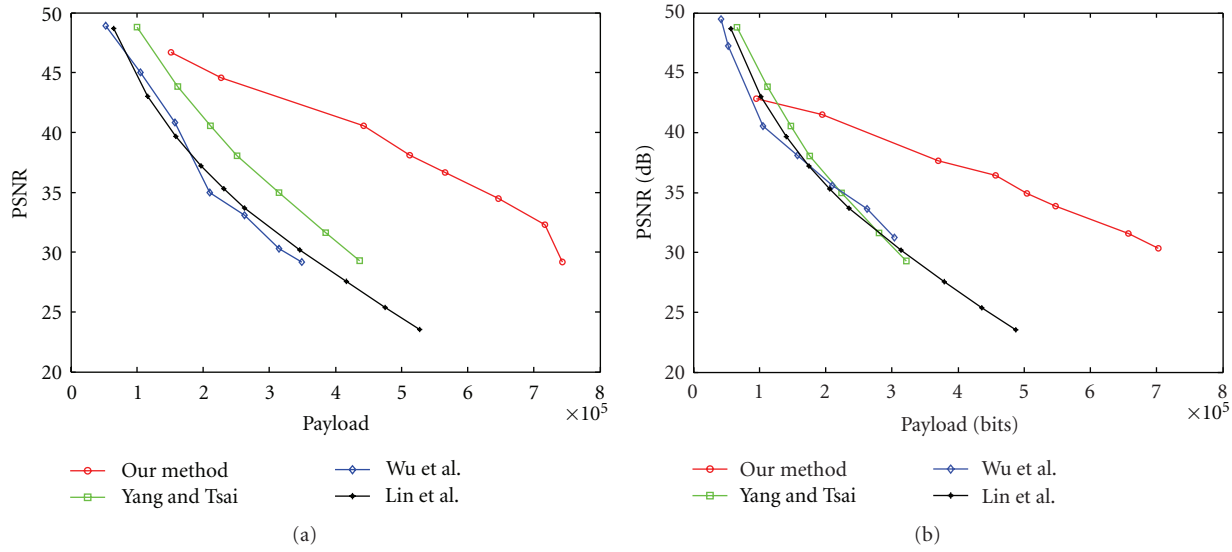


Figure 8: Performance comparison between various methods on two test images. (a) *Lena* and (b) *Boat*.

Table 3: Comparisons of the related secret image sharing schemes.

Functionality	Methods				
	Yang et al. [20]	Chang et al. [21]	Chang et al. [22]	Lin et al. [24]	Our method
Meaningful shadows	Yes	Yes	No	Yes	Yes
PSNR	40 dB	40 dB	~34 dB	43 dB	~35 dB
Lossless secret image	Yes	Yes	Yes	Yes	Yes
Lossless cover image	No	No	No	Yes	Yes
Max. payload (bytes)	$(M \times N)/4$	$(M \times N)/4$	$(M \times N)/8 \leq$	$((t-3)M \times N)/3$	$>(M \times N)/4$
Number of shadows	3	3	2	>3	2

a payload of a size approaching 7×10^5 bits with a PSNR value above 32 dB. For example, if one tried to embed a secret message of the above size into two host images using one of the other approaches, the PSNR value would be around 31 dB. Since a secret message can be separately embedded into two stego-images using the proposed method, third parties (or malicious users) would be incapable of extracting the hidden message (and recovering the original host image) when they are only dealing with one of the stego-images.

Table 3 compares our method with the secret image sharing schemes. All of the methods except for Chang et al.'s technique [22] have the capability of generating meaningful stego-images, which can be an important feature for a secret image sharing (with steganography). In addition, however, the three schemes, Yang et al. [20], Chang et al. [21], and Chang et al. [22], are incapable of recovering the host image without distortion. Although the PSNR of our method is not better than that of the other schemes [20, 21, 24], the maximum capacity provided by our method is larger than that provided by Yang et al. [20] and Chang et al. [21]. However, both the PSNR and the payload of our method are superior to that of Chang et al. [22]. Finally, the last row of Table 3 reveals that the number of shadows needed to implement the proposed method is less than that required by the other three schemes [20, 21, 24].

4. Conclusions

This paper presents an effective reversible data hiding method using two marked images via the adaptive coefficient-shifting (ACS) algorithm. According to the three predetermined rules, two target blocks, stego-block 1 (S1) and stego-block 2 (S2), are generated by embedding secret digits into the host block via the ACS algorithm. More specifically, both S1 and S2 are generated by either the minimum-preserved scheme (or the minimum-preserved with squeezing scheme) when Rule 1 (or Rule 3) is satisfied. S1 and S2 are generated by the minimum-preserved scheme and the BV embedding scheme, respectively, if Rule 2 fits the case. Simulations validate that the ACS algorithm not only completely recovers a host medium but is also able to obtain a distortion-free extracted message. The ACS algorithm is capable of handling various kinds of images without any occurrence of overflow/underflow. Moreover, the payload and PSNR performance of the proposed method is superior to that of the conventional invertible data hiding schemes. Since a secret message is spread into two stego-images by the proposed method, third parties with one stego-image cannot extract the hidden message nor can the original host image be recovered. Furthermore, the number of shadows required by the proposed method is less than that required by

the existing (t, n)-threshold schemes of secret image sharing with steganography.

Acknowledgment

The author would like to thank the editors and anonymous reviewers for providing valuable comments that helped to improve the content of the paper.

References

[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, Massachusetts, Mass, USA, 2nd edition, 2008.

[2] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, CRC Press, Florida, Fla, USA, 2008.

[3] 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. 1401–1410, 2010.

[4] C. C. Lin and P. F. Shiu, "High capacity data hiding scheme for DCT-based images," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 3, pp. 220–240, 2010.

[5] K. Yamamoto and M. Iwakiri, "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, 2010.

[6] S. Zhou, Q. Zhang, and X. Wei, "An image encryption algorithm based on dual DNA sequences for image hiding," *ICIC Express Letters*, vol. 4, no. 4, pp. 1393–1398, 2010.

[7] 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.

[8] Z. G. Qu, X. B. Chen, X. J. Zhou, X. X. Niu, and Y. X. Yang, "Novel quantum steganography with large payload," *Optics Communications*, vol. 283, no. 23, pp. 4782–4786, 2010.

[9] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[10] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[11] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 12, pp. 3582–3591, 2008.

[12] 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.

[13] H. C. Wu, C. C. Lee, C. S. Tsai, Y. P. Chu, and H. R. Chen, "A high capacity reversible data hiding scheme with edge prediction and difference expansion," *Journal of Systems and Software*, vol. 82, no. 12, pp. 1966–1973, 2009.

[14] C. H. Yang and M. H. Tsai, "Improving histogram-based reversible data hiding by interleaving predictions," *IET Image Processing*, vol. 4, no. 4, pp. 223–234, 2010.

[15] C. Y. Yang and W. C. Hu, "High-performance reversible data hiding with overflow/underflow avoidance," *ETRI Journal*, vol. 33, no. 4, pp. 580–588, 2011.

[16] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[17] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology, Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '94)*, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Perugia, Italy, May 1994.

[18] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414, 2004.

[19] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377–1385, 2004.

[20] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076, 2007.

[21] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.

[22] C. C. Chang, C. C. Lin, T. H. N. Le, and H. B. Le, "Sharing a verifiable secret image using two shadows," *Pattern Recognition*, vol. 42, no. 11, pp. 3097–3114, 2009.

[23] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognition*, vol. 43, no. 1, pp. 397–404, 2010.

[24] P. Y. Lin, J. S. Lee, and C. C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886–895, 2009.

[25] P. Y. Lin and C. S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.