Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2010, Article ID 249826, 13 pages
doi:10.1155/2010/249826

Research Article

Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function

Jeong-Chun Joo,[1] Hae-Yeoun Lee,[2] and Heung-Kyu Lee[1]

[1] *Department of Computer Science, Korea Advanced Institute of Science and Technology, 335 Gwahangno, Yuseong-Gu, Daejeon 305-701, Republic of Korea*
[2] *School of Computer and Software Engineering, Kumoh National Institute of Technology, Yangho-Dong, Gumi, Gyeongbuk 730-701, Republic of Korea*

Correspondence should be addressed to Heung-Kyu Lee, hklee@mmc.kaist.ac.kr

Received 20 August 2009; Revised 4 February 2010; Accepted 20 March 2010

Academic Editor: Bulent Sankur

We herein advance a secure steganographic algorithm that uses a turnover policy and a novel adjusting process. Although the method of Wang et al. uses Pixel-Value Differencing (PVD) and their modulus function provides high capacity and good image quality, the embedding process causes a number of artifacts, such as abnormal increases and fluctuations in the PVD histogram, which may reveal the existence of the hidden message. In order to enhance the security of the algorithm, a turnover policy is used that prevents abnormal increases in the histogram values and a novel adjusting process is devised to remove the fluctuations at the border of the subrange in the PVD histogram. The proposed method therefore eliminates all the weaknesses of the PVD steganographic methods thus far proposed and guarantees secure communication. In the experiments described herein, the proposed algorithm is compared with other PVD steganographic algorithms by using well-known steganalysis techniques, such as RS-analysis, steganalysis for LSB matching, and histogram-based attacks. The results support our contention that the proposed method enhances security by keeping the PVD histogram similar to the cover, while also providing high embedding capacity and good imperceptibility to the naked eye.

1. Introduction

Steganography is a method of secret communication in which a message is embedded in a cover, such as text or an image. Message embedding is performed in spatial or frequency domain. One of the representative data hiding methods in spatial domain is to use the least significant bit (LSB), such as LSB replacement or LSB matching. Transform domain steganographic methods employ the well-known transformation techniques such as Discrete Cosine Transform (DCT), Fourier Transform (FT), or Discrete Wavelet Transform (DWT). Spatial domain methods are simpler and have a large capacity while transform domain methods are more robust compared to spatial domain method. The key factors for the secure communication are high security, high embedding capacity, and good imperceptibility to the naked eye. In order to satisfy these requirements, a number of different steganographic algorithms have been developed with the primary aim of maintaining the characteristics of the cover image such as histogram to avoid any statistical attack [1–3].

Steganalysis schemes can be classified into two categories: specific and universal steganalysis. Due to the fact that specific steganalysis attempts to detect a specific target steganography [4, 5], it has high performance when tested only on that precise embedding method. Universal steganalysis is designed to reveal a hidden message regardless of the steganographic algorithm used [6–8]. Although universal steganalysis performs slightly worse than specific steganalysis techniques where the stego method is assumed known, it nevertheless yields acceptable results. Universal steganalysis therefore appears to be the more practical solution.

In order to resist detection by well-known steganalytic techniques, such as RS-analysis [4], and to take account of the properties of the human visual system, Wu and Tsai [9] proposed a Pixel-Value Differencing (PVD) steganography that embeds more bits into pairs that have large PVD values, such as those found in edge areas. Although this method provides high embedding capacity and invisibility, it creates step effects in the PVD histogram and embedded messages may be detected. A modified version of PVD steganography was presented by Zhang and Wang [10], which removed the step effects by varying the lower and upper bounds of the subrange using a pseudorandom parameter $\beta(\in [0,1])$. Since the random expansion of the subrange allowed fewer bits to be embedded for the same difference values and decreased the changing quantity of the pixel value, Zhang and Wang's method had lower embedding capacity but better quality than Wu and Tsai's. Though it made the histogram smooth, it was still detected by Sabeti et al. by the use of one-more-time embedding and neural networks [11]. Although a hybrid steganography was proposed using LSB steganography at flat areas and PVD steganography at edge areas in order to increase the embedding capacity [12], it still contained step effects and was detected by applying a χ^2-attack on the PVD histogram [13]. More recently, a steganographic algorithm using PVD and the modulus function was presented by Wang et al. [14], in which the remainder of two consecutive pixels was changed to match the decimal value of the message bits. However, the embedding process created fluctuations and abnormal increases, which destroyed the symmetry of the PVD histogram. Wang et al.'s method was therefore detected using a PVD histogram-based attack [15]. Yang et al. suggested the adaptive LSB steganographic method using PVD to determine the length of the message bits [16], which divides the range of difference values into lower, middle, and higher levels.

In our assessment of all the previous PVD steganographic techniques described herein, we found that detection occurred because the embedding process changed the PVD histogram too severely. In order to achieve the required level of security, the embedding process must avoid those attacks that exploit modifications to the PVD histogram and eliminate all artifacts generated by the embedding process. In view of these assessments, the aim of this paper is to introduce improvements on Wang et al.'s method in terms of higher capacity and lower detectability, while being secure against well-known steganalytic methods. The use of the modulus function improves capacity by overcoming the falling-off-boundary problem and provides good image quality by minimizing the changes in pixel values [17, 18]. The proposed method makes two main contributions to steganographic technique: a turnover policy and a novel adjusting process. The turnover policy yields histograms close to those of the cover image and maintains the symmetry of the PVD histogram. The novel adjusting process helps to remove fluctuations around the border of the subrange. The proposed method therefore maintains the PVD histogram similar to that of the cover and is secure against RS-analysis [4], steganalysis for LSB matching [5], and histogram-based steganalysis that focuses on PVD steganographic methods [10, 15]. Furthermore, high capacity and good imperceptibility are achieved.

The remainder of the paper is organized as follows. Section 2 provides a review of Wang et al.'s steganographic algorithm and describes its weaknesses in the face of steganalytic measures. In Section 3, we present our secure steganographic algorithm, including a turnover policy and a novel adjusting process. Experimental results are presented in Section 4 and Section 5 concludes.

2. Review of Wang et al.'s Method

2.1. Wang et al.'s Steganographic Algorithm. For high embedding capacity and good image quality, Wang et al. proposed steganography using PVD and a modulus function [14]. It modifies the remainder of two consecutive pixels instead of the difference between them.

In order to embed the message bits, five parameters are obtained for each subblock F_i, each of which is composed of two consecutive pixels $(P_{(i,x)}, P_{(i,y)})$ using Wu and Tsai's scheme [9], namely, the difference $d_i = P_{(i,y)} - P_{(i,x)}$, the subrange R_k such that $R_k \in [l_k, u_k]$ and $l_k \leq d_i \leq u_k$, the width $w_k = u_k - l_k + 1$, the embedding capacity t_i (bits), and the decimal value t_i' of t_i message bits. The remainder values $F_{\text{rem}(i)}$ are then calculated by dividing $(P_{(i,x)} + P_{(i,y)})$ by 2^{t_i}. A range table R provides data on the embedding capacity of each sub-block F_i and is composed of n contiguous subranges R_k $(0 \leq k < n)$. t_i bits of secret data S are embedded into F_i by altering $P_{(i,x)}$ and $P_{(i,y)}$ such that $F_{\text{rem}(i)} = t_i'$, using the approach that achieves the minimum distortion. When the stego pixel values $(P'_{(i,x)}, P'_{(i,y)})$ do not overflow the boundary of the grayscale pixel value ([0 255]), the embedding process is completed following the replacement of $(P_{(i,x)}, P_{(i,y)})$ by $(P'_{(i,x)}, P'_{(i,y)})$ in the cover image. When $P'_{(i,x)}$ or $P'_{(i,y)}$ overflows, $P'_{(i,x)}$ and $P'_{(i,y)}$ are revised by adding $2^{(t_i-1)}$, subtracting $2^{(t_i-1)}$, or shifting the overflowing values. Since $(P'_{(i,x)}, P'_{(i,y)})$ can be corrected, the range of the revised stego pixel values $(P''_{(i,x)}, P''_{(i,y)})$ may neither fall below 0 nor rise above 255. Finally, the embedding process is completed by replacing $(P_{(i,x)}, P_{(i,y)})$ in the cover image by $(P''_{(i,x)}, P''_{(i,y)})$.

In order to extract the message bits, the receiver obtains the difference d_i between two consecutive pixels $(P_{(i,x)}, P_{(i,y)})$. d_i determines the subrange index k, the width w_k of the subrange by $w_k = u_k - l_k + 1$ and the length t_i of the message bits. After computing the remainder value using $F_{\text{rem}(i)} = (P_{(i,x)} + P_{(i,y)}) \mod 2^{t_i}$, the extraction algorithm is completed by transforming the remainder value $F_{\text{rem}(i)}$ into a binary string of length t_i.

2.2. Steganalytical Weaknesses of Wang et al.'s Method. In [15], we presented three steganalytic measures to detect a message that was embedded using Wang et al.'s method. Although Wang et al.'s method achieves high embedding capacity and good imperceptibility, the significant changes in the PVD histogram reveal the existence of the messages.

Let h and h' be the PVD histogram of the cover and the stego images, respectively. In addition, the estimated histogram is denoted by h_e. d $(-255 \leq d \leq 255, d \in N)$ is the difference between the two pixels. Table 1 shows an example of how the pixel pair changes when the message value is embedded using Wang et al.'s method. After embedding the messages, the difference of two stego pixels is changed by 1, at most. For example, if the cover pixel pair is (9, 8), its original difference is -1 and the difference of the stego pixel pair becomes -1 or 0. In general, in a negative area ($d < 0$), d is changed to d or $(d+1)$, while in a positive area ($d > 0$), d is changed to d or $(d-1)$. This means that the absolute value of the difference between two pixels is unchanged or decreased by 1 after embedding. However, since there are no absolute values smaller than 0, a change of $h(0)$ violates the general modification rule. We therefore model the changes in the PVD histogram from the cover as per (1):

$$h'(d) = \begin{cases} \left(1-\dfrac{\alpha}{2}\right)\cdot h(d)+\dfrac{\alpha}{2} \\ \quad\cdot h(d-1), & \text{if } d<0; \\ \dfrac{\alpha}{2}\cdot h(d-1)+\left(1-\dfrac{\alpha}{2}\right) \\ \quad\cdot h(d)+\dfrac{\alpha}{2}\cdot h(d+1), & \text{if } d=0 \text{ or } 1; \\ \left(1-\dfrac{\alpha}{2}\right)\cdot h(d)+\dfrac{\alpha}{2} \\ \quad\cdot h(d+1), & \text{if } d>1, \end{cases} \tag{1}$$

where α is the embedding rate.

The weaknesses of Wang et al.'s method are caused by these changes in the PVD histogram. Since there are some special cases that do not follow the general modification rule of (1), h' around the lower and upper bound of the subrange are computed using (2):

$$h'(u_{k-1}) = \left(1-\frac{\alpha}{2}\right)\cdot h(u_{k-1});$$

$$h'(l_k+1) = \frac{\alpha}{2}\cdot h(l_k)+\left(1-\frac{\alpha}{2}\right)\cdot h(l_k+1)+\frac{\alpha}{2}\cdot h(l_k+2), \tag{2}$$

where u_k and l_k are the upper and lower bound of the kth subrange. $h'(u_{k-1})$ decreases and $h'(l_k+1)$ increases after the message is embedded. The first steganalytic measure ($SM1$) checks the fluctuation using (3):

$$SM1 = \frac{h'(-9)-h'(-7)}{h'(-7)}\times 100. \tag{3}$$

Because the width of each subrange is taken to be a power of 2, -8 is the common border in the various range tables. Since the PVD histogram value $h(d)$ decreases by increasing $|d|$ in a macroscopically smooth fashion [9], two points $(-7,-9)$ adjacent to the common border (-8) are used to obtain the maximum difference. In order to normalize and maximize the effects of the message embedding, $h'(-7)$ is used as the divisor.

Due to the fact that the difference histogram for natural images without embedding the message follows a Gaussian distribution [19], the PVD histogram has bilateral symmetry about zero. The second steganalytic measure ($SM2$) therefore checks the asymmetry using (4).

$$SM2 = \frac{h'(1)-h'(-1)}{h'(-1)}\times 100. \tag{4}$$

As shown in (1), since $h'(1)$ and $h'(-1)$ is obtained from 3 bins $(h(0), h(1), h(2))$ and 2 bins $(h(-1), h(-2))$ of the original PVD histogram, respectively, $h'(1)$ is higher than $h'(-1)$. Therefore, $SM2$ of the cover image is close to 0 and $SM2$ of the stego image is very much higher than 0.

After the message has been embedded using Wang et al.'s method, $h'(0)$ is generated from 3 bins $(h(-1), h(0), h(1))$ and increases significantly. The third steganalytic measure ($SM3$) checks for the abnormal increase of $h'(0)$ using the following equation:

$$SM3 = \frac{h'(0)-h_e(0)}{h_e(0)}\times 100, \tag{5}$$

where $h_e(0)$ is estimated close to the original value using the curve-fitting methods of three well-known models described in [15]. Thus, $SM3$ of the cover image is close to 0. However, Wang et al.'s embedding process increases both $h'(0)$ and $SM3$.

The values of the three steganalytic measures for the cover and stego images can be separated from each other and can hence reveal the existence of the hidden messages embedded using Wang et al.'s method without the cover images. The performance of the steganalytic measures used is described and verified by experiment (see Figure 7).

3. Proposed Steganography Preserving the PVD Histogram

To achieve secure steganography, the PVD histogram of the stego image should preserve the statistical properties of the cover image as well as possessing good visual quality. This section presents an improvement to Wang et al.'s method that generates no artifacts in the PVD histogram after embedding the message and is not detected using well-known steganalytic techniques or PVD histogram-based attacks. Firstly, the improved embedding algorithm with the turnover policy and the novel adjusting process is explained and then the extraction algorithm is presented without the cover images.

3.1. Embedding Algorithm. In order to provide high embedding capacity, good imperceptibility to the naked eye, and improved security, the modulus function is adopted and the weaknesses of Wang et al.'s method are eliminated through a turnover policy and a novel adjusting process. When embedding the message bits into two consecutive pixels $(P_{(i,x)}, P_{(i,y)})$, m is the difference between the remainder of two pixels' sum and the message value. If the modifying value m is odd, the two pixels are modified by $\lfloor m/2 \rfloor$ and $\lfloor m/2 \rfloor + 1$, respectively. The turnover policy allocates the significant distortion $(\lfloor m/2 \rfloor + 1)$ to $P_{(i,x)}$ or

Table 1: Changes in pixel values when embedding the message value using Wang et al.'s method. The difference d_i between two stego pixels remains intact or is modified by ±1.

$(P_{(i,x)}, P_{(i,y)})$	Decimal message value 0	1	2	3	4	5	6	7	Changes of difference d_i
(10, 8)	(9, 7)	(9, 8)	(10, 8)	(10, 9)	(11, 9)	(11, 10)	(12, 10)	(8, 7)	$-2 \Rightarrow -2, -1$
(9, 8)	(8, 8)	(9, 8)	(9, 9)	(10, 9)	(10, 10)	(11, 10)	(7, 7)	(8, 7)	$-1 \Rightarrow -1, 0$
(8, 8)	(8, 8)	(8, 9)	(9, 9)	(9, 10)	(10, 10)	(6, 7)	(7, 7)	(7, 8)	$0 \Rightarrow 0, 1$
(8, 9)	(8, 8)	(8, 9)	(9, 9)	(9, 10)	(10, 10)	(10, 11)	(7, 7)	(7, 8)	$1 \Rightarrow 1, 0$
(8, 10)	(7, 9)	(8, 9)	(8, 10)	(9, 10)	(9, 11)	(10, 11)	(10, 12)	(7, 8)	$2 \Rightarrow 2, 1$

$P_{(i,y)}$ in turn. Therefore, the absolute value of the difference between two pixels can be decreased or increased. Since the difference between two pixels may be altered in a positive or negative way, the new histogram $h'(d)$ of the stego image is obtained from 3 bins $(h(d-1), h(d), h(d+1))$ of the original histogram (refer to Table 2). Consequently, the turnover policy prevents $h'(0)$ and $h'(1)$ from increasing abnormally and helps to make the PVD histogram symmetric about zero in a similar way to the cover. As a result, *SM*2 and *SM*3, as described in Section 2.2, are no longer effective. Our novel adjusting process is applied to solve the out-of-subrange problem, which opens the algorithm to possible detection by *SM*1. Whereas Wang et al.'s method creates fluctuations around the border of the subrange, the proposed adjusting process eliminates these. Therefore, the proposed method is secure against detection by *SM*1.

The overall embedding process is shown in Figure 1. The proposed steganographic algorithm consists of four steps, namely, the pixel pairing step, the embedding step, the adjusting step, and the overcoming step. The pixel pairing step vectorizes the pixel pairs and permutates the sub-blocks. At the embedding step, the message bits are embedded into the pixel pair using the modulus function and turnover policy. The adjusting step employs our novel adjusting process when the difference in the new pixel pair is below or above the subrange. Finally, the falling-off-boundary problem is solved at the overcoming step. The embedding process is repeated until no messages or pixel pairs remain.

Firstly, in the pixel pairing step, the cover image is partitioned into nonoverlapping sub-blocks composed of two consecutive pixels by Zigzag scan. To enhance the security, the sub-blocks are permutated.

In the embedding step, the remainder of two pixels is simply modified to match the message value. Given that the modulus function is used, the proposed method reduces or increases the pixel value to match the residue of the pixel pair to the decimal message value t'_i. m is a modifying value used to minimize the distortion as per Equation (6):

$$m = \begin{cases} t'_i - F_{\text{rem}(i)}, & \text{if } \left| t'_i - F_{\text{rem}(i)} \right| \le \dfrac{w_k}{2}; \\ t'_i - F_{\text{rem}(i)} - w_k, & \text{if } \left(t'_i - F_{\text{rem}(i)}\right) > \dfrac{w_k}{2}; \\ t'_i - F_{\text{rem}(i)} + w_k, & \text{if } \left(t'_i - F_{\text{rem}(i)}\right) < -\dfrac{w_k}{2}, \end{cases} \tag{6}$$

where $F_{rem(i)}$ is the remainder of the sum of the two pixels $(P_{(i,x)} + P_{(i,y)})$ divided by the width w_k of subrange R_k. In order to embed the message, the two pixels are modified using (7):

$$\begin{aligned} \left(P'_{(i,x)}, P'_{(i,y)}\right) &= f\left[\left(P_{(i,x)}, P_{(i,y)}\right), m\right] \\ &= \begin{cases} \left(P_{(i,x)}+r_c, P_{(i,y)} + r_f\right), \\ \quad \text{if } i \text{ is } \textit{odd} \text{ number;} \\ \left(p_{(i,x)}+r_f, p_{(i,y)} + r_c\right), \\ \quad \text{if } i \text{ is } \textit{even} \text{ number,} \end{cases} \end{aligned} \tag{7}$$

where m is the modifying value obtained from (6), $r_c = \lceil m/2 \rceil$, and $r_f = \lfloor m/2 \rfloor$. Since the turnover policy is employed in (7) to obtain the new stego pixels $(P'_{(i,x)}, P'_{(i,y)})$, the changing opportunities are distributed nearly equally over the two pixels in the sub-block. Each histogram value therefore has the same probability of being changed, and the proposed method preserves the shape of the PVD histogram more closely to that of the cover.

The third (adjusting) step is designed to eliminate the fluctuations in the PVD histogram. After modifying the pixel values according to the decimal message value t'_i, whether or not the out-of-subrange problem is present is checked by investigating whether the new difference of two stego pixels is in a different subrange. In order to solve the out-of-subrange problem by preserving the difference between two pixels, a novel adjusting process is devised using (8).

$$\left(P'_{(i,x)}, P'_{(i,y)}\right) = \begin{cases} \left(g(P_{(i,x)}, q_x), g(P_{(i,x)}, q_x) + d_i\right), \\ \qquad \text{if } i \text{ is } \textit{odd} \text{ number;} \\ \left(g\left(P_{(i,y)}, q_y\right) - d_i, g\left(P_{(i,y)}, q_y\right)\right), \\ \qquad \text{if } i \text{ is } \textit{even} \text{ number,} \end{cases} \tag{8}$$

where $d_i = P_{(i,y)} - P_{(i,x)}$, $g(p,q) = \{\lfloor p/w_k \rfloor - q\} \times w_k + t'_i (q \in \{-1, 0, 1\})$, $q_x = \arg\min_{q \in \{-1,0,1\}} |g(P_{(i,x)}, q) - P_{(i,x)}|$, $q_y = \arg\min_{q \in \{-1,0,1\}} |g(P_{(i,y)}, q) - P_{(i,y)}|$. In other words, $g(p,q)$ is the closest value to p among all the values that have a residue t'_i by w_k. When the new difference d'_i of the altered pixels $(P'_{(i,x)}, P'_{(i,y)})$ is not zero $(d'_i \neq 0)$ and is in the other subrange or at the border of the subrange $(d'_i \le l_k$ or $u_k \le d'_i)$, one pixel is modified to embed the message value and

Table 2: PVD changes after embedding, using Wang et al.'s method and the proposed method.

$d_i(P_{(i,y)} - P_{(i,x)})$	$d'_i(P'_{(i,y)} - P'_{(i,x)})$		
	Wang et al. [14]	Proposed method	
		i is *even* number	i is *odd* number
...	...	...	...
−2	(−2 or −1)	(−1 or −2)	(−2 or −3)
−1	(−1 or **0**)	(0 or −1)	(−1 or −2)
0	(**0** or **1**)	(1 or 0)	(0 or −1)
1	(**1** or **0**)	(0 or 1)	(1 or 2)
2	(2 or **1**)	(1 or 2)	(2 or 3)
3	(3 or 2)	(2 or 3)	(3 or 4)
4	(4 or 3)	(3 or 4)	(4 or 5)
5	(5 or 4)	(4 or 5)	(5 or 6)
6	(6 or 5)	(5 or 6)	(6 or 7)
7	(**7** or 6)	(6 or 7)	(7 or 7)
8	(8 or 9)	(8 or 8)	(8 or 9)
9	(9 or 8)	(8 or 9)	(9 or 10)
...	...	...	...

the other pixel is adjusted to maintain the PVD. Therefore, the proposed method can maintain $h'(u_k)$ and $h'(l_k + 1)$ similar to $h(u_k)$ and $h(l_k+1)$, respectively. There is no need to apply the proposed adjusting process at the subrange which is greater than 128 because the histogram value is very small (close to 0). Due to the fact that the proposed adjusting process is able to remove the fluctuations around the border of the subrange, this weakness of Wang et al.'s method is eliminated and secure communication can be guaranteed.

Table 2 shows how the difference value of the pixel pair is changed after the messages have been embedded. The changes of the difference value represent the weaknesses of Wang et al.'s method and the advantages of the proposed method. In Wang et al.'s method, the new difference value d'_i appears once (7), twice, or three times (0, 1). However, since the proposed method increases or decreases the difference value, every d'_i appears four times. Consequently, the proposed method ensures a balance of changing opportunity for the difference value through the turnover policy and the novel adjusting process. It avoids histogram-based attacks by keeping the PVD histogram of the cover.

The fourth (overcoming) step is carried out in order to deal with the falling-off-boundary problem. If the pixel value is out of boundary [0 255] after the adjusting step, the overcoming step revises the pixels as follows.

Case 1. $P'_{(i,x)} < 0$ and $P'_{(i,y)} \le (255 - z)$:

$$\left(P''_{(i,x)}, P''_{(i,y)}\right) = \left(P'_{(i,x)} + z, P'_{(i,y)} + z\right). \tag{9}$$

Case 2. $P'_{(i,x)} < 0$ and $P'_{(i,y)} > (255 - z)$:

$$\left(P''_{(i,x)}, P''_{(i,y)}\right) = \left(0, P'_{(i,y)} + \left(0 - P'_{(i,x)}\right)\right). \tag{10}$$

Case 3. $P'_{(i,x)} > 255$ and $P'_{(i,y)} \ge z$:

$$\left(P''_{(i,x)}, P''_{(i,y)}\right) = \left(P'_{(i,x)} - z, P'_{(i,y)} - z\right). \tag{11}$$

Case 4. $P'_{(i,x)} > 255$ and $P'_{(i,y)} < z$:

$$\left(P''_{(i,x)}, P''_{(i,y)}\right) = \left(255, P'_{(i,y)} + \left(P'_{(i,x)} - 255\right)\right). \tag{12}$$

where

$$z = \begin{cases} w_k, & \text{if } d'_i = l_k \text{ or } d'_i = u_k; \\ \dfrac{w_k}{2}, & \text{otherwise.} \end{cases} \tag{13}$$

This overcoming step was devised for $P'_{(i,x)}$. In case of $P'_{(i,y)}$, we apply the same technique by substituting $P'_{(i,x)}$ with $P'_{(i,y)}$. If the stego pixel pair is obtained without using the adjusting process, the overcoming value z is half of the width, in order to preserve the remainder of the summation of the values of the two pixels. However, if the difference of the stego pixel pair is equal to the lower or upper bound of the subrange, z is equal to the whole width of the subrange that is required, so as not to change the remainder of each pixel. Most falling-off-boundary problems may be categorized as Case 1 or Case 3. However, since the solution of Case 1 and Case 3 can make another falling-off-boundary problem when the difference is greater than 128, Case 2 and Case 4 are designed. For example, if the pixel pair of the cover is (255, 43) and message value is 66, the underflow problem occurs after solving the overflow problem by Case 3. To overcome this special case, Case 4 is applied and the new stego pixel pair is finally to be (255, 67).

After the overcoming step, the next pixel pair is selected and the embedding algorithm is applied repeatedly until no messages or pixel pairs remain.

3.2. Extracting Algorithm.

The embedded messages are simply extracted from the sum of two pixels or from one pixel. This extraction algorithm performs blind, without the cover. The sender and receiver must share the range table R. The difference d_i is computed from two consecutive pixels $(P_{(i,x)}, P_{(i,y)})$ and determines the subrange index k, width w_k, and message length t_i. If d_i is not zero and equal to l_k or u_k, the message value t'_i is extracted merely by computing the residue of $P_{(i,x)}$ or $P_{(i,y)}$ by w_k. If not, t'_i is the remainder value of the sum of two pixel values by w_k. The extracting process for two pixels is completed by transforming the message value t'_i into a binary stream of length t_i. The extracting algorithm is performed repeatedly until no messages or pixel pairs remain.

The message can be extracted correctly even though the proposed method tries to embed the message bits into the stego image again, that is, at double embedding. As shown in Figure 2, two pixel values are flexibly adjusted according to the message value. The receiver can extract the hidden message correctly, regardless of the original pixel pair. Therefore, the proposed method guarantees secure communication.

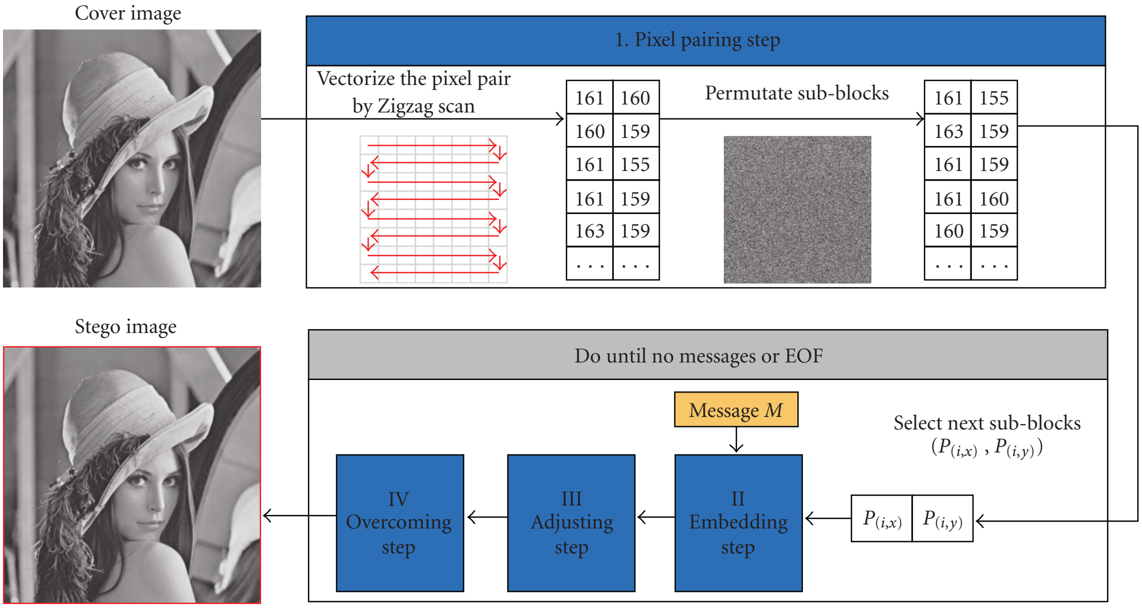
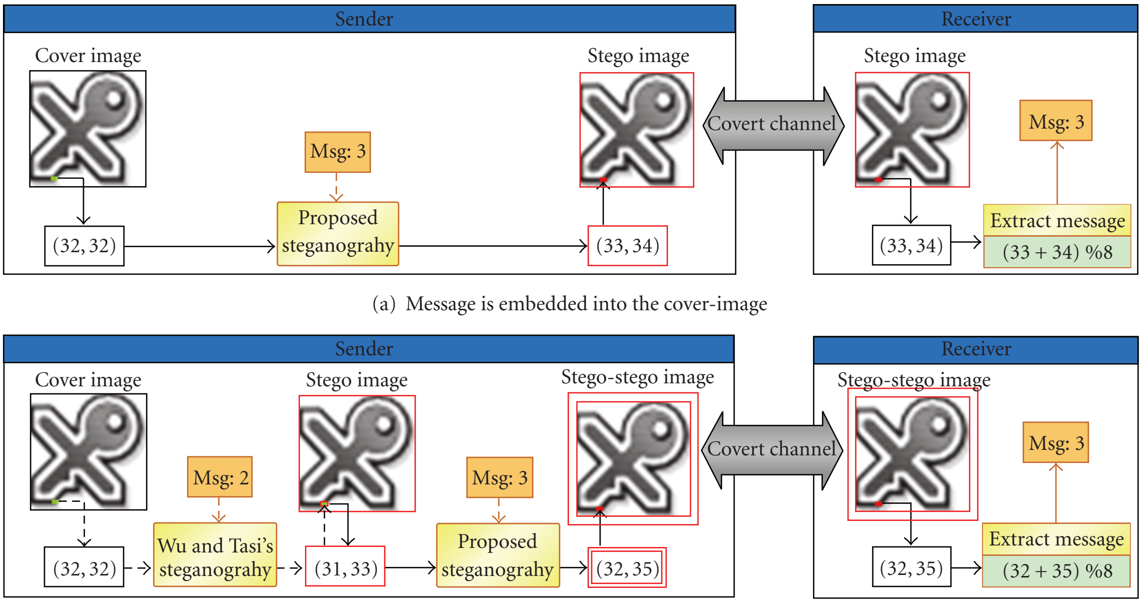


FIGURE 1: Overall message embedding process showing the pixel paring step, the embedding step, the adjusting step, and the overcoming step.



(a) Message is embedded into the cover-image

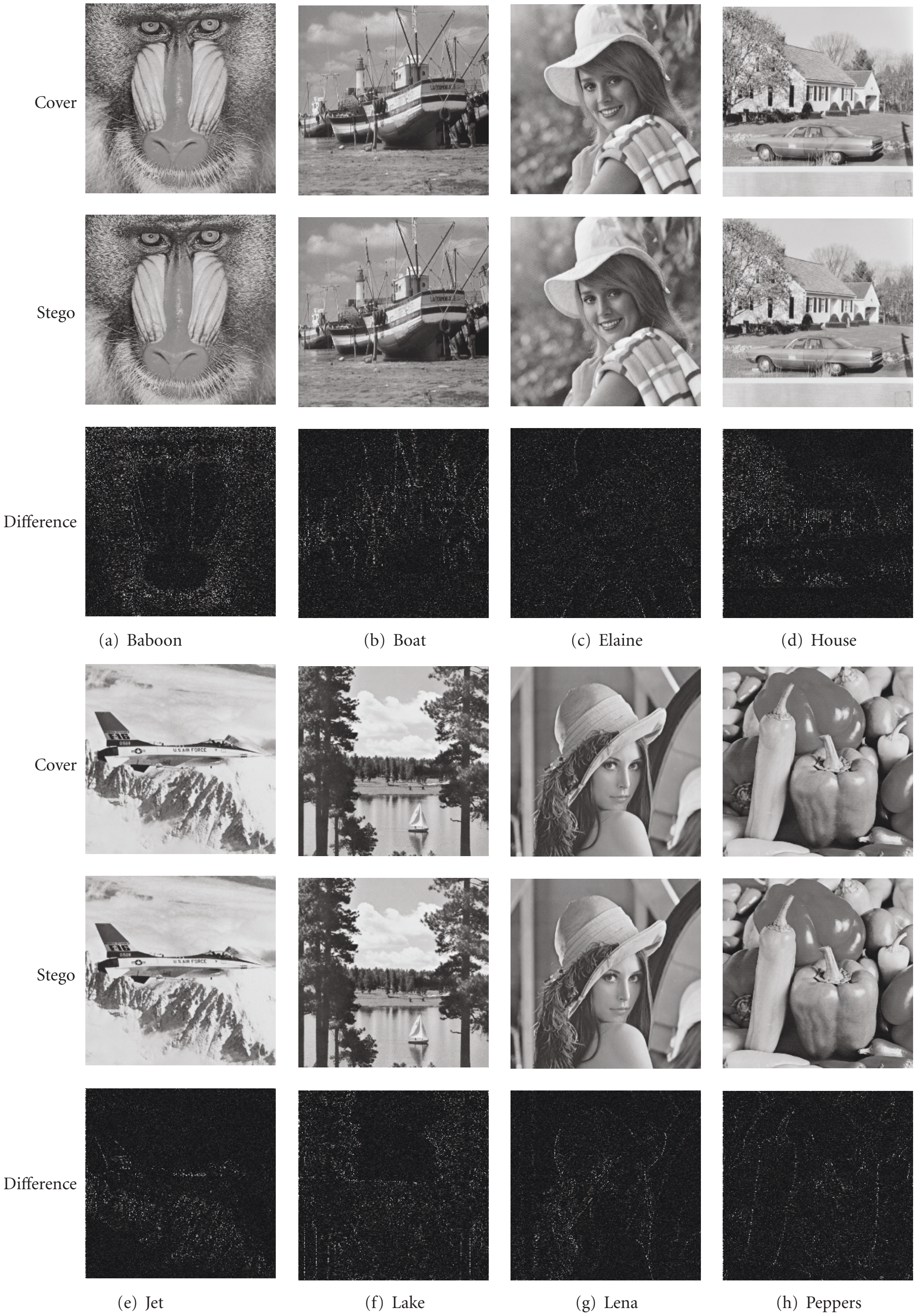
(b) Double embedding: Message is embedded into the stego image

FIGURE 2: Receiver can extract the hidden message correctly whether the message is embedded into the cover image (a) or stego image (b).

4. Experimental Results

In order to verify the minimum changes of the PVD histogram, the proposed method was compared with the methods of Wu and Tsai [9], Zhang and Wang [10], Wang et al. [14], and Yang et al. [16]. The stego images were generated using the range table R in Table 3. In Yang et al.'s method [16], the parameters for the lower, middle, and higher levels were set as (2-3-4). The security was tested using RS-analysis [4], steganalysis for LSB matching[5], and the histogram-based [10, 15]. Eight grayscale images of size 512 × 512 were tested: Baboon, Boat, Elaine, House, Jet, Lake, Lena, and Peppers. Figure 3 shows the cover images, the stego images generated by our method, and the difference images scaled thirty times between the cover and stego images. As shown in the figure, most of the distortions are found on the edge areas and no artifact can be distinguished by the human eye.

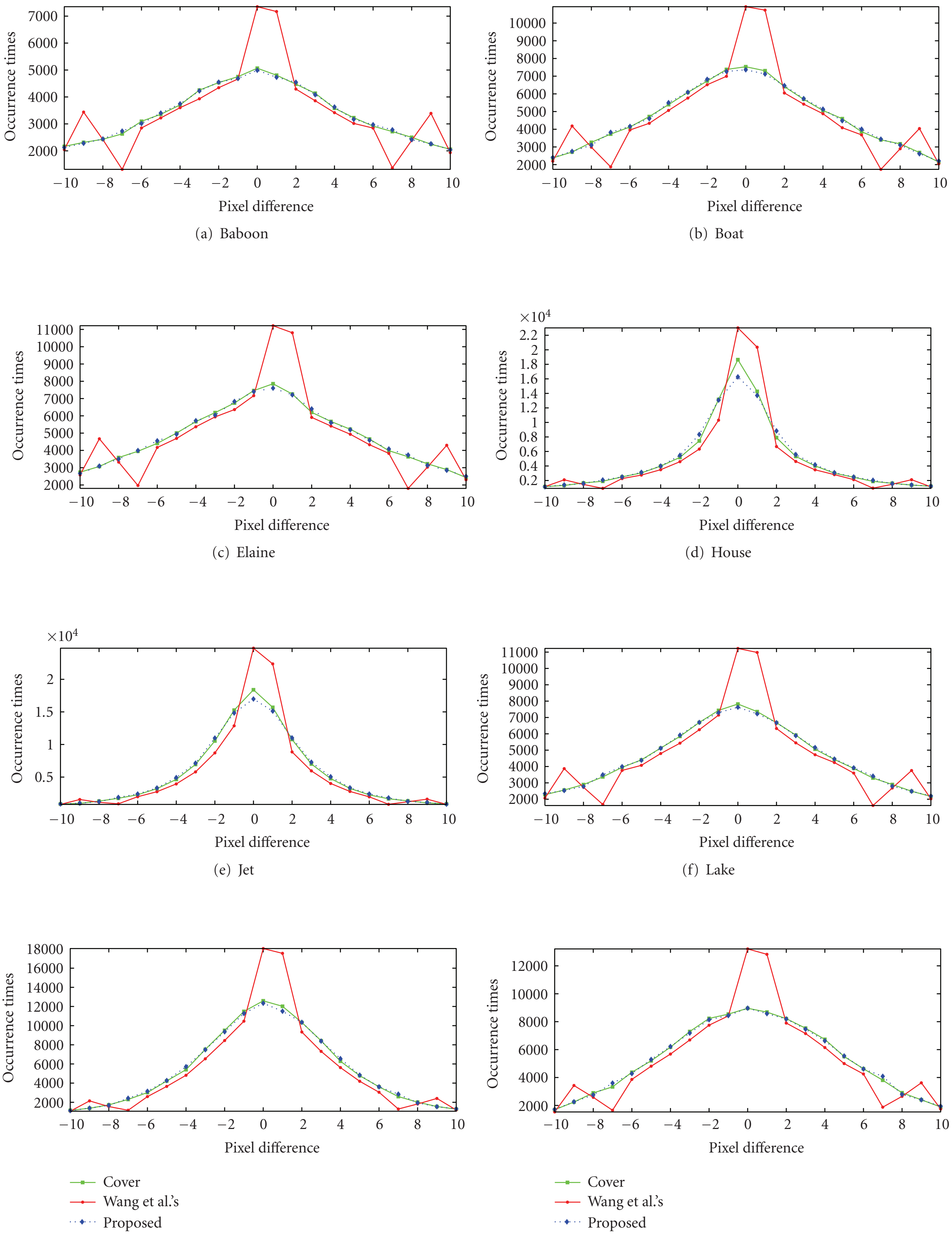
In Figure 4, the PVD histograms obtained for the cover and stego images are compared for our eight test images.



(a) Baboon (b) Boat (c) Elaine (d) House

(e) Jet (f) Lake (g) Lena (h) Peppers

Figure 3: The eight test images, the corresponding stego images obtained using the proposed method, and the difference images scaled 30 times between the cover and stego images.



(a) Baboon

(b) Boat

(c) Elaine

(d) House

(e) Jet

(f) Lake

(g) Lena

(h) Peppers

FIGURE 4: Comparison of the PVD histogram between the cover and the stego image.

Table 3: Range table R. l_k and u_k are the lower and upper bound of the subrange, respectively.

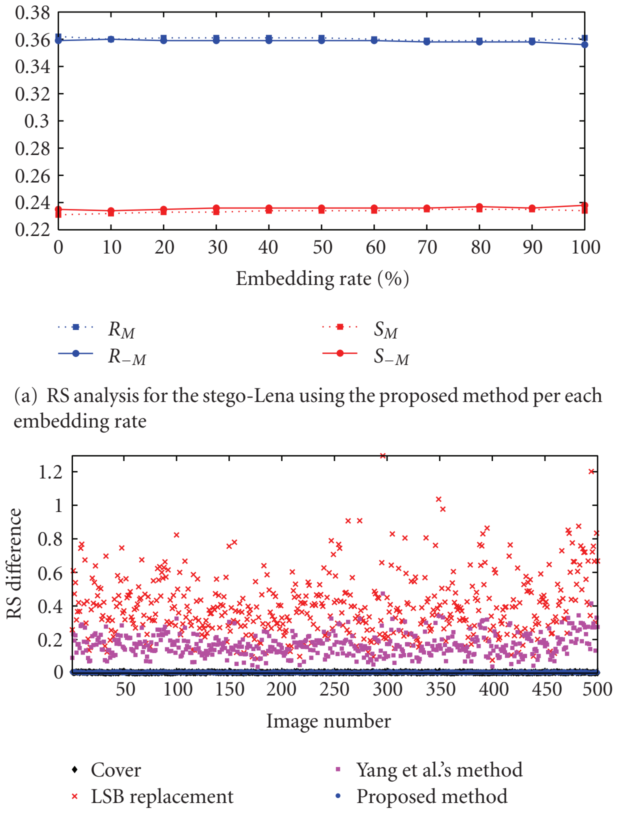
index (k)	0	1	2	3	4	5
$[l_k\ u_k]$	[0 7]	[8 15]	[16 31]	[32 63]	[64 127]	[128 255]
hiding bits (t_i)	3	3	4	5	6	7

Table 4: Mean of distance measures between the PVD histogram of the cover and that of the stego images for the eight test images.

	Manhattan dist. (L1)	Euclidean dist. (L2)	Chi-square dist.
Wu and Tsai [9]	45101.5	9747.3	6139.7
Zhang and Wang [10]	18056.0	4523.0	1257.6
Wang et al. [14]	23726.5	7088.8	1996.9
Yang et al. [16]	13870.5	3154.2	668.0
Proposed	4091.3	956.9	100.8

In Wang et al.'s method, the shapes of the PVD histograms of the stego images are clearly distinguished from those of the cover images because of the fluctuations and the abnormal increases. However, our proposed method kept the PVD histogram close to the cover and did not generate any artifacts.

4.1. Statistical Analysis of the PVD Histogram Difference. Table 4 summarizes the mean of the distance measures between the PVD histogram of the cover and that of the stego images which are obtained from the various PVD-based methods for the eight test images. This enables the similarity between the cover and stego images to be compared in a statistical way. Although Zhang and Wang's method maintained the symmetry, the PVD histogram was different from that of the cover because of the smoothness effects. Wu and Tsai's method and Wang et al.'s method had high values because of modifications such as step effects, fluctuations, and abnormal increases. However, the proposed method had the smallest value in statistical terms among all the PVD steganographic methods considered here.



(a) RS analysis for the stego-Lena using the proposed method per each embedding rate

(b) RS detection values for the massive images

Figure 5: (a) RS-analysis for the stego-Lena image using the proposed method and (b) RS detection values of the cover images, using the LSB replacement, the Yang et al.'s, and the proposed method for 500 randomly chosen images.

4.2. Security under RS-Steganalysis. The security of the proposed method under the well-known RS-analysis technique is shown in Figure 5. RS-analysis defines a discrimination function DF and flipping mask M. R_M is the proportion of blocks in which the magnitude of DF increases when DF_1 is applied to a part of each block, and S_M is the proportion of blocks with decreasing magnitude of DF. Similarly, two other parameters R_{-M} and S_{-M} are defined when DF_{-1} is applied to a part of each block. If the image does not contain secret data, $R_M \approx R_{-M} > S_M \approx S_{-M}$. When the messages are embedded into the least significant bits (LSBs) of the image, R_{-M} and S_M increase, whereas R_M and S_{-M} decrease, and the existence of the hidden message is therefore revealed. In the experiments, we used $\begin{bmatrix}0&1\\1&0\end{bmatrix}$ and $\begin{bmatrix}0&-1\\-1&0\end{bmatrix}$ as M and $-M$, respectively. As shown in Figure 5(a), since the proposed method changes the pixel values instead of the LSB to embed the message, R_M and S_M were similar to R_{-M} and S_{-M}, respectively. Figure 5(b) shows that the RS detection values $((|R_M - R_{-M}| + |S_M - S_{-M}|)/(R_M + S_M))$ for the cover and the proposed method were close to 0, whereas those of the LSB replacement method [20] and the Yang et al.'s method [16] were very much higher than 0. The proposed method is therefore also secure against RS-analysis, in common with other PVD methods.

4.3. Security Analysis under Steganalysis for LSB Matching. Since the pixel value is changed in order to embed the messages, the proposed method was tested under attack for LSB matching steganography. Steganalysis for LSB matching in grayscale images was presented in 2005 by Ker [5], who used the fact that the Histogram Characteristic Function-Center Of Mass (HCF-COM) of downsampled stego image $C'(H[k])$ would be greater than that of full-sized one $C(H[k])$. The Histogram Characteristic Function (HCF) $H[k]$ was obtained by calculating the Discrete Fourier Transform (DFT) of the histogram of the input image. The Center Of Mass (COM) of the HCF was calculated using

Table 5: Histogram-based attacks can be performed separately on the odd and even rows. The values of the proposed method are similar to the cover while those of the Wang et al.'s method are very higher than the cover.

	*SM*1						*SM*2					
	Even row			Odd row			Even row			Odd row		
	Cover	Wang	Proposed	Cover	Wang	Proposed	Cover	Wang	Proposed	Cover	Wang	Proposed
Baboon	−15.0	173.5	−14.8	−9.1	151.0	−16.3	2.9	54.7	4.0	−0.6	52.6	4.6
Boat	−27.2	123.9	−28.6	−27.3	122.2	−26.7	−4.5	52.5	−3.0	2.7	54.6	1.9
Elaine	−21.1	148.7	−19.2	−23.4	126.3	−26.5	−3.1	49.1	0.2	−2.2	52.5	−4.6
House	−32.6	128.3	−35.7	−28.3	127.6	−30.9	9.3	100.2	9.5	7.6	95.0	4.6
Jet	−42.4	77.3	−41.8	−47.6	69.8	−48.3	3.0	72.3	2.6	2.6	75.3	−0.6
Lake	−23.2	125.3	−29.7	−24.6	135.1	−28.7	−4.8	48.1	0.0	2.9	59.4	2.3
Lena	−41.2	79.2	−40.0	−39.2	89.3	−41.5	3.8	66.6	4.8	5.6	68.8	5.9
Peppers	−32.4	105.0	−34.6	−33.0	109.3	−34.6	1.0	53.7	−0.9	2.4	51.1	0.8

Table 6: Comparison of hiding capacity (bytes) and visual quality (dB).

	Wu [9]		Zhang [10]		Wang [14]		Yang [16]		Proposed	
	$L_{\max}$	PSNR	$L_{\max}$	PSNR	$L_{\max}$	PSNR	$L_{\max}$	PSNR	$L_{\max}$	PSNR
Baboon	57,028	37.0	53,586	40.4	57,043	40.2	80,688	39.6	57,043	39.2
Boat	52,320	39.6	50,926	42.4	52,490	41.1	71,788	42.1	52,490	41.0
Elaine	50,891	42.1	49,750	44.5	50,893	44.9	68,994	43.6	50,893	43.5
House	52,418	40.0	51,003	42.7	52,572	42.4	72,043	42.0	52,572	41.5
Jet	51,221	40.6	50,366	43.5	51,221	43.4	69,415	42.9	51,221	42.8
Lake	52,614	40.0	50,970	42.7	52,662	42.4	72,304	41.9	52,662	41.5
Lena	50,894	41.5	50,023	44.3	50,894	43.4	68,927	43.3	50,894	43.4
Peppers	50,657	41.5	49,968	43.9	50,815	43.4	68,632	43.4	50,815	42.5

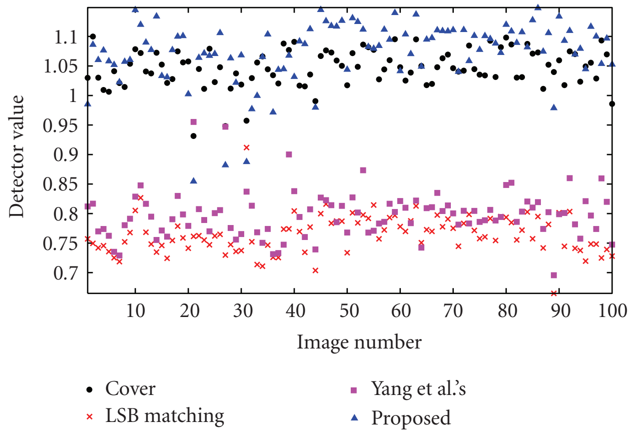
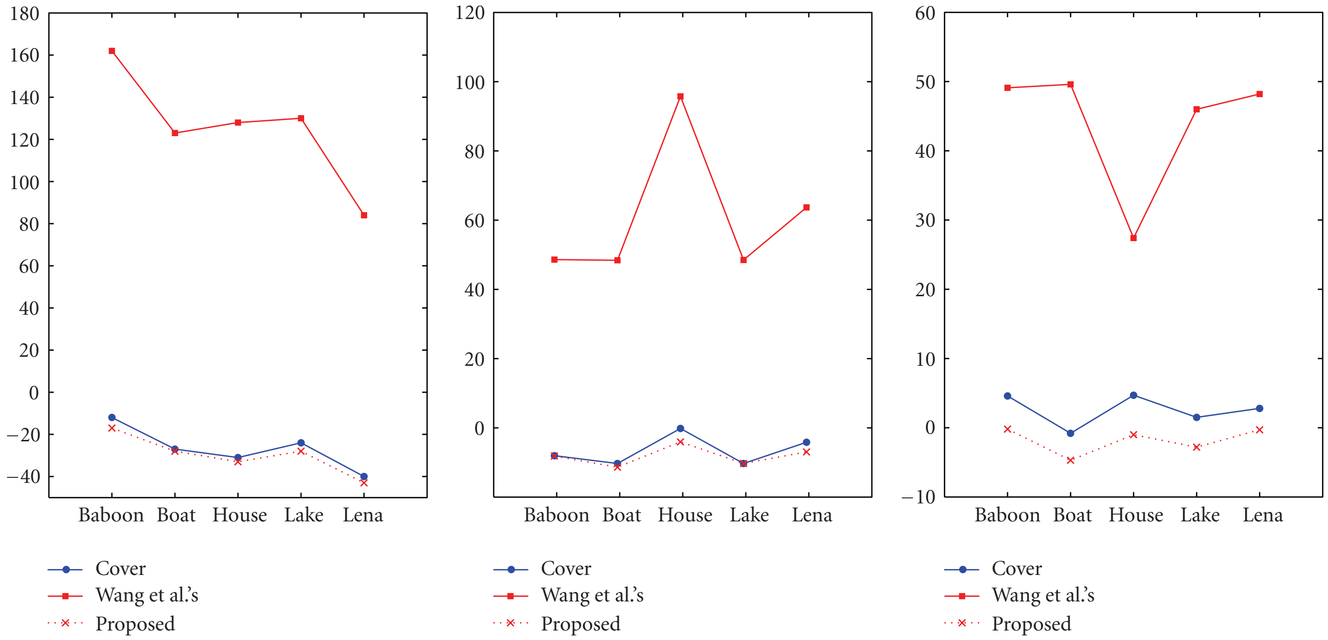


Figure 6: HCF-COM ratio of the full-sized images to the downsampled images for the cover images, obtained using the LSB matching, the Yang et al.'s, and the proposed method.

$C(H[k]) = \sum_{i=0}^{n} i|H[i]|/\sum_{i=0}^{n}|H[i]|$. This parameter gives general information about the energy distribution in the HCF. The discriminator used to differentiate stego images from cover images is $C(H[k])/C'(H[k])$. Figure 6 plots the detector values of the HCF-COM ratios for 100 randomly selected natural images from the NRCS image database [21] that satisfy $C(H[k]) \approx C'(H[k])$. The discriminator values of the stego images obtained using the proposed method were close to 1, similar to the cover images, while the values of the stego images obtained using the LSB matching method and the Yang et al.'s method were, on average, 0.76 and 0.80, respectively. This means that the proposed method is secure against calibrated HCF-COM attack of steganalysis for LSB matching.

4.4. Security Analysis under the PVD Histogram-Based Attacks. Zhang and Wang insisted that the steps at [7 8], [15 16], [31 64], and [127 128] in the PVD histograms clearly revealed the presence of the hidden message [10]. This assertion was based on the step effects generated by the embedding process used in Wu and Tsai's method. However, since our proposed method produces no step effects and the PVD histogram after embedding is very similar to the cover, as in Figure 4, it is impossible to detect the existence of the hidden message using Zhang and Wang's analysis.

Figure 7 shows the results for the three steganalytic measures described in Section 2.2. Wang et al.'s method produced very much higher values than the cover and was easily detected by our three steganalytic measures. However, the steganalytic measures of the stego images generated by the proposed method were very close to the cover. These results support our contention that the proposed method



(a) *SM1*

(b) *SM2*

(c) *SM3*

Figure 7: Three steganalytic measures of the cover, using Wang et al.'s and our proposed method.

removes all the weaknesses of Wang et al.'s method and is secure under PVD histogram-based attacks.

The histogram-based attack can be performed separately on the odd rows and even rows of the stego images. Because of the permutation of the sub-blocks in the first pixel pairing step of the proposed method, the *SM*1 and *SM*2 values of the stego image produced by the proposed scheme were similar to those of the cover image as shown in Table 5. Consequently, the proposed method is secure under the separate attack of the steganalytic measures described in Section 2.2.

4.5. Hiding Capacity and Perceptual Quality Analysis. As previously mentioned, effective steganography must possess high embedding capacity and good imperceptibility to the naked eye. Table 6 presents the maximum capacity ($L_{\max}$) and PSNR values for the PVD steganographic methods discussed herein. Although the PSNR values of our proposed method were slightly lower than those of Wang et al.'s method for the same capacity, our method nevertheless provides a good image quality for the human visual system because the human eye cannot see the decline in quality of stego images when PSNR values are over 38 dB [22]. In other words, a slightly lower PSNR than Wang et al.'s method is almost insignificant in terms of quality. Both Zhang and Wang's and Wang et al.'s method had already defeated, despite the high PSNR values. Even though Yang et al.'s method can provide the high capacity and good image quality, it is vulnerable under the LSB steganalysis such as RS-analysis (see Figure 5) and Ker's calibrated HCF-COM attack (see Figure 6). However, our proposed method achieved the high hiding capacity and security compared with the other PVD steganographic methods by sacrificing only a little visual quality.

5. Conclusion

In this paper, a secure steganographic method with a turnover policy and a novel adjusting process was proposed, in order to enhance the security of stego images. The method improves upon Wang et al.'s method. The turnover policy helps to minimize the distortion and remove abnormal increases in the PVD histogram. The novel adjusting process eliminates the fluctuations around the border of the sub-range. As a result, the proposed method can both maintain a PVD histogram similar to that of the cover and preserve the statistical properties of the PVD histogram, such as symmetry or a Gaussian-like shape. Therefore, compared with the methods of Wu and Tsai, Zhang and Wang, Wang et al., and Yang et al., our proposed method yields the least differences in the PVD histograms between the cover and stego images. Since the embedding process produces no artifacts for detection by steganalysis, and the steganalytic detector values are similar to those of the cover, our proposed method guarantees secure communication with a high embedding capacity and good imperceptibility to the naked eye. The experimental results support the contention that the proposed method shows the best similarity in the PVD histogram between the cover and the stego image and is secure against the various well-known steganalyses such as RS-analysis, steganalysis for LSB matching, and PVD histogram-based attacks.

List of Symbols

α:	Embedding rate
β:	Pseudo-random parameter
d:	Difference between two pixels of the sub-block
h:	PVD histogram of the cover image
h' :	PVD histogram of the stego image
h_e:	Estimated PVD histogram of the suspicious image
i:	Selecting sequence of the sub-blocks
k:	Index of the range table R
l_kv	Lower bound of the subrange R_k
m:	Modifying value to embed the message
t_i:	Length of embedding bits
t'_i:	Decimal value of t_i message bits
u_k:	Upper bound of the subrange R_k
w_k:	Width of the subrange R_k
z:	Overcoming value to solve the falling-off-boundary problem
$C(H[k])$:	Center Of Mass (COM) of the HCF of the full-sized image.
$C'(H[k])$:	Center Of Mass (COM) of the HCF of the down-sampled image
DF:	Discrimination function of the RS-steganalysis
F:	Cover image
F_i:	ith sub-block of the cover image
$F_{rem(i)}$:	Remainder value of F_i
$H[k]$:	Histogram Characteristic Function (HCF)
$L_{\max}$:	Maximum embedding capacity
M:	Flipping mask
$(P_{(i,x)}, P_{(i,y)})$:	Two pixels of F_i in the cover image
$(P'_{(i,x)}, P'_{(i,y)})$:	New stego pixel values of F_i
R:	Range table
R_M:	Proportion of blocks with increasing magnitude of DF under M
R_{-M}:	Proportion of blocks with increasing magnitude of DF under $-M$
S:	Secret data to be embedded
S_M:	Proportion of blocks with decreasing magnitude of DF under M
S_{-M}:	Proportion of blocks with decreasing magnitude of DF under $-M$

Acknowledgment

This research was supported by NRL (National Research Lab) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (no. R0A-2007-000-20023-0), and by Ministry of Culture, Sports and Tourism (MCST) and Korea Culture Content Agency (KOCCA) in the Culture Technology (CT) Research & Developement Program 2009.

References

[1] Z. Chen and W. Liu, "Improved LSB matching steganography with histogram characters reserved," in *Information Optics and Photonics Technologies II*, vol. 6837 of *Proceedings of SPIE*, p. 68370X, Beijing, China, November 2007.

[2] K. Solanki, A. Sarkar, and B. S. Manjunath, "YASS: yet another steganographic scheme that resists blind steganalysis," in *Proceedings of the 9th International Workshop on Information Hiding (IH '07)*, vol. 4567 of *Lecture Notes in Computer Science*, pp. 16–31, 2007.

[3] P. K. Amin, N. Liu, and K. P. Subbalakshmi, "Statistical attack resilient data hiding," *International Journal of Network Security*, vol. 5, no. 3, pp. 112–120, 2007.

[4] J. Fridrich and M. Goljan, "Practical steganalysis of digital images—state of the art," in *Security and Watermarking of Multimedia Contents IV*, vol. 4675 of *Proceedings of SPIE*, pp. 1–13, San Jose, Calif, USA, January 2002.

[5] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, 2005.

[6] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Security and Watermarking of Multimedia Contents V*, vol. 5020 of *Proceedings of SPIE*, pp. 131–142, 2003.

[7] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 111–119, 2006.

[8] I. Avcibaş, M. Kharrazi, N. Memon, and B. Sankur, "Image steganalysis with binary similarity measures," *EURASIP Journal on Applied Signal Processing*, vol. 2005, no. 17, pp. 2749–2757, 2005.

[9] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[10] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognition Letters*, vol. 25, no. 3, pp. 331–339, 2004.

[11] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis and payload estimation of embedding in pixel differences using neural networks," *Pattern Recognition*, vol. 43, no. 1, pp. 405–415, 2010.

[12] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proceedings: Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611–615, 2005.

[13] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis of pixel-value differencing steganographic method," in *Proceedings of IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing*, pp. 292–295, 2007.

[14] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *Journal of Systems and Software*, vol. 81, no. 1, pp. 150–158, 2008.

[15] J.-C. Joo, H.-Y. Lee, C. N. Bui, W.-Y. Yoo, and H.-K. Lee, "Steganalytic measures for the steganography using pixel-value differencing and modulus function," in *Proceedings of the 9th Pacific Rim Conference on Multimedia*, vol. 5353 of *Lecture Notes in Computer Science*, pp. 476–485, 2008.

[16] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, 2008.

[17] C.-C. Thien and J.-C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875–2881, 2003.

[18] S.-J. Wang, "Steganography of capacity required using modulo operator for embedding secret image," *Applied Mathematics and Computation*, vol. 164, no. 1, pp. 99–116, 2005.

[19] T. Zhang and X. Ping, "A new approach to reliable detection of LSB steganography in natural images," *Signal Processing*, vol. 83, no. 10, pp. 2085–2093, 2003.

[20] S. Walton, "Information authentication for a slippery new age," *Dr. Dobbs Journal*, vol. 20, no. 4, pp. 18–26, 1995.

[21] "NRCS Photo Gallery Home," http://photogallery.nrcs.usda.gov/.

[22] F. A. P. Petitcolas and R. J. Anderson, "Evaluation of copyright marking systems," in *Proceedings International Conference on Multimedia Computing and Systems (ICMCS '99)*, vol. 1, pp. 574–579, 1999.