Available online at www.sciencedirect.com

ScienceDirect

The Journal of Systems and Software 81 (2008) 150–158

The Journal of Systems and Software

www.elsevier.com/locate/jss

A high quality steganographic method with pixel-value differencing and modulus function

Chung-Ming Wang [a], Nan-I Wu [a], Chwei-Shyong Tsai [b], Min-Shiang Hwang [b,*]

[a] Institute of Computer Science, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan, ROC
[b] Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan, ROC

Received 18 February 2006; received in revised form 24 January 2007; accepted 24 January 2007
Available online 20 February 2007

Abstract

In this paper, we shall propose a new image steganographic technique capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. In addition, our new method avoids the falling-off-boundary problem by using pixel-value differencing and the modulus function. First, we derive a difference value from two consecutive pixels by utilizing the pixel-value differencing technique (PVD). The hiding capacity of the two consecutive pixels depends on the difference value. In other words, the smoother area is, the less secret data can be hidden; on the contrary, the more edges an area has, the more secret data can be embedded. This way, the stego-image quality degradation is more imperceptible to the human eye. Second, the remainder of the two consecutive pixels can be computed by using the modulus operation, and then secret data can be embedded into the two pixels by modifying their remainder. In our scheme, there is an optimal approach to alter the remainder so as to greatly reduce the image distortion caused by the hiding of the secret data. The values of the two consecutive pixels are scarcely changed after the embedding of the secret message by the proposed optimal alteration algorithm. Experimental results have also demonstrated that the proposed scheme is secure against the RS detection attack.

Keywords: Data hiding; Steganography; Cover image; Stego-image; Imperceptible; Modulus operation

1. Introduction

In recent years, enormous research efforts have been invested in the development of digital image steganographic techniques. The major goal of steganography is to enhance communication security by inserting secret message into the digital image, modifying the nonessential pixels of the image (Feng et al., 2006; Petitcolas et al., 1999). The image after the embedding of the secret message, so-called stego-image, is then sent to the receiver through a public channel.

In the transmission process, the public channel may be intentionally monitored by some opponent who tries to prevent the message from being successfully sent and received. The opponent may randomly attack the stego-image if he/she doubts the stego-image carries any secret message because the appearance of the stego-image shows obvious artifacts of hiding effect (Liao et al., 2007; Simmons, 1984). For this reason, an ideal steganography scheme, to keep the stego-image from drawing attention from the opponent, should maintain an imperceptible stego-image quality. That is to say, if there are more similarities between the cover image and the stego-image, it will be harder for an attacker to find out that the stego-image has important secret data hidden inside it (Wu and Hwang, 2007). This way, the secret data is more likely to travel from the sender to the receiver safe and sound.

For the past decade, many steganographic techniques for still images have been presented. A simple and well-known approach is directly hiding secret data into the least-significant bit (LSB) of each pixel in an image. Then,

[*] Corresponding author. Tel.: +886 4 22855401; fax: +886 4 22857173.
E-mail address: mshwang@nchu.edu.tw (M.-S. Hwang).

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.01.049

based on the LSB technique, a genetic algorithm of optimal LSB substitution is now also available to improve the stego-image quality of the simple LSB method (Wang et al., 2001). In addition, Chang et al. (2003) have also presented a fast and efficient optimal LSB method based on the dynamic programming strategy that improves the computation time of Wang et al.'s scheme (Wang et al., 2001). A novel simple LSB technique based on optimal pixel adjustment was presented to achieve the goal of improving the stego-image quality (Chan and Cheng, 2004). Besides, Thien and Lin also presented a simple LSB scheme based on the modulus function to improve the stego-image quality (Thien and Lin, 2003). In order to gain a higher payload than when the 4-LSBs method is used, Wang has proposed two new schemes based on the modulo operator (Wang, 2005). Wu et al. have also presented a combination scheme on the basis of pixel-value differencing and LSB replacement with a view to improving the hiding capacity while maintaining acceptable stego-image quality (Wu et al., 2005). In order to enhance the security, on the other hand, Lin and Tsai have proposed a new approach that integrates the concept of secret image sharing and steganographic techniques with the additional capability of image authentication (Lin and Tsai, 2004). Lou and Liu (2002) proposed a LSB-based steganographic method that can resist the common-cover-carrier attack by embedding variable-size secret data and redundant Gaussion noise.

There are many steganographic schemes have also been proposed for binary images. For example, Tseng et al. (2002) designed a binary matrix and an integer weight matrix so as to increase the payload of each sub-image. It can hide $\lfloor \log_2(m \times n + 1) \rfloor$ into a sub-image with $m \times n$ pixels by manipulating at most two bits of the original content. In addition, Tseng and Pan (2002) further proposed a high quality data hiding scheme based on (Tseng et al., 2002) that searches for the more undetectable pixels of the cover image as targets of modification. Wu and Liu (2004) used the shuffling method to equalize the uneven embedding capacity of each image block for the purpose of providing a greater hiding capacity and higher security. The hidden message of their scheme can be used to serve various purposes such as authentication, annotation, and verification. In addition, aside from regular digital images, some other multimedia forms such as 3D models and PDF texts can also serve as the cover media. The first steganographic method built on point-sampled geometry has been presented by Wang and Wang (2006), and the first steganographic system that works on PDF English texts has been created by Zhong et al. (2007). Recently, various kinds of steganalysis detectors have been under steady development, and some have been presented in an attempt to help detect the existence of messages hidden in images in place of visual inspection. For example, the well-known RS steganalytic algorithm by Fridrich et al. (2001) is able to detect the existence of LSB steganography. Basically, the detection capability of the RS steganalytic algorithm depends on the capacity of the hidden message. Specifically, the algorithm can detect the existence of the LSB scheme with high precision when the hidden capacity is more than 0.005 bits per pixel. However, when the hidden capacity is less than 0.005 bits per pixel, the RS steganalytic algorithm is completely ineffective (Fridrich et al., 2001; Ker, 2004).

The LSB-based methods mentioned above, directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is higher than that of a smooth area. That is to say, an edge area can conceal more secret data than a smooth area. With this concept in mind, Wu and Tsai presented steganographic scheme that offers high imperceptibility to the stego-image by selecting two consecutive pixels as the object of embedding. The payload of Wu and Tsai's scheme is determined by the difference value between the pixels (Wu and Tsai, 2003). In Wu and Tsai's method, they determine whether the two consecutive pixels belong to an edge or smooth area by checking out the difference value between the two consecutive pixels. If the difference value is large, that means the two pixels are located in an edge areas, and more secret data can be hidden here. On the contrary, if the difference value is small, that means the two pixels are located in a smooth area, and less secret data can be embedded. Therefore, their scheme produces stego-images that are more similar to the original images than those produced by LSB substitution schemes, which directly embed secret data into the cover image without considering the differences between adjacent pixels. Furthermore, Chang and Tseng have proposed a new method based on side match where the users can consult more than two neighboring pixels to determine the payload of each pixel (Chang and Tseng, 2004).

In this paper, in order to provide a better stego-image quality than Wu and Tsai's scheme (Wu and Tsai, 2003), we shall propose a novel technique based on pixel-value difference and modulus function. In Wu and Tsai's scheme, which is also known as the PVD method, the difference value between two consecutive pixels is regarded as a feature for recording the secret message. When the original difference value is unequal to the secret message, the two consecutive pixels will be directly adjusted so that their difference value can stand for the secret data. However, considerable stego-image distortion can happen when the PVD method adjusts the two consecutive pixels to hide the secret data in the difference value. To make a difference, with our new method, we shall improve the stego-image quality by adjusting the remainder of the two consecutive pixels instead of the difference value. Besides that, the falling-off-boundary problem may probably worsen the situation when the PVD method alone is used, especially either when the two consecutive pixels are located in an extreme edge or smooth area, or when the values of the two consecutive pixels form a contrast. To overcome the falling-off-boundary problem, our new method re-revises the remainder of the two consecutive pixels.

The rest of this paper is organized as follows. We will briefly review Wu and Tsai's scheme in Section 2. In Section 3, the embedding and extracting algorithms of the proposed method based on the modulus operation will be presented respectively. The experimental results and analyzes will be in Section 4, followed by some concluding remarks in Section 5.

2. Review of Wu and Tsai's scheme

Let us begin with the background on which the embedding algorithm of method (Wu and Tsai, 2003) is build up. Given a cover image F sized $M \times N$. F_i is a sub-block of F that has two consecutive pixels broken down by partitioning F in raster scan order such that $F = \{F_i | i = 1, 2, \ldots, \frac{M \times N}{2}\}$. By definition each F_i has two elements $P_{(i,L)}$ and $P_{(i,R)}$. The pixel values of $P_{(i,L)}$ and $P_{(i,R)}$ are $P_{(i,x)}$ and $P_{(i,y)}$, respectively. The difference value d_i of $P_{(i,x)}$ and $P_{(i,y)}$ can be derived by Eq. (1).

$$d_i = |P_{(i,x)} - P_{(i,y)}|. \tag{1}$$

On the other hand, they design a range table R which consists of n contiguous sub-ranges R_j; in other words, $R = \{R_j | j = 1, 2, \ldots, n\}$. The major job of the range table is to provide information about the hiding capacity of each F_i. Each sub-range R_j has its lower and upper bound values, say l_j and u_j, so that we have $R_j \in [l_j, u_j]$. The width w_j of each R_j is selected to be a power of 2, and can be computed by $w_j = u_j - l_j + 1$. Each sub-block F_i relates to its sub-range R_j from the range table R such that $R_j = \min(d_i, w_j)$ and $d_i \in [l_j, u_j]$. This way, hiding capacity of two consecutive pixels can be obtained by

$$t_i = \lfloor \lg(w_j) \rfloor. \tag{2}$$

Here, t_i is the number of bits that can be hidden in F_i. Read t_i bits from the binary secret data stream and transform t_i into its decimal value t'_i. A new difference value d'_i can be generated by putting l_j and t'_i together:

$$d'_i = t'_i + l_j.$$

Now the secret data can be embedded into F_i by modifying its $P_{(i,x)}$ and $P_{(i,y)}$ such that $d_i = d'_i$. The details of the embedding criteria are as follows:

$$(P'_{(i,x)}, P'_{(i,y)}) = \begin{cases} (P_{(i,x)} + \lceil m/2 \rceil, P_{(i,y)} - \lfloor m/2 \rfloor), \\ \quad \text{if } P_{(i,x)} \geqslant P_{(i,y)} \text{ and } d'_i > d_i; \\ (P_{(i,x)} - \lfloor m/2 \rfloor, P_{(i,y)} + \lceil m/2 \rceil), \\ \quad \text{if } P_{(i,x)} < P_{(i,y)} \text{ and } d'_i > d_i; \\ (P_{(i,x)} - \lceil m/2 \rceil, P_{(i,y)} + \lfloor m/2 \rfloor), \\ \quad \text{if } P_{(i,x)} \geqslant P_{(i,y)} \text{ and } d'_i \leqslant d_i; \\ (P_{(i,x)} + \lceil m/2 \rceil, P_{(i,y)} - \lfloor m/2 \rfloor), \\ \quad \text{if } P_{(i,x)} < P_{(i,y)} \text{ and } d'_i \leqslant d_i, \end{cases} \tag{3}$$

where $m = |d'_i - d_i|$. We can gain new pixel values $P'_{(i,x)}$ and $P'_{(i,y)}$ after the calculation in Eq. (3) and replace $P_{(i,x)}$ and $P_{(i,y)}$ in the cover image with the new values so that the embedding process is accomplished. An illustration of how $P_{(i,x)}$ and $P_{(i,y)}$ can be adjusted by Wu and Tsai's scheme for the purpose of hiding secret data is shown in Table 1. In Table 1, assume the pixel values of sub-block F_i are $P_{(i,x)} = 32$, $P_{(i,y)} = 32$, and the width w_j of their sub-range is 8 with $l_j = 0$ and $u_j = 7$. Then, 3 bits of the secret data is taken out and put into F_i. All the possible ways of adjusting $P_{(i,x)}$ and $P_{(i,y)}$ are shown in Table 1. Obviously, the falling-off-boundary problem will occur and would not conform Eq. (3) if $0 \leqslant P_{(i,x)} \leqslant 3$ and $0 \leqslant P_{(i,y)} \leqslant 3$.

Table 1
An illustration of Wu and Tsai's embedding process

Secret data (decimal value)	$P_{(i,x)} = 32$	$P_{(i,y)} = 32$	New difference value of $P_{(i,x)}$ and $P_{(i,y)}$
0	No modify	No modify	0
1	+1	No modify	1
2	+1	−1	2
3	+2	−1	3
4	+2	−2	4
5	+3	−2	5
6	+3	−3	6
7	+4	−3	7

The recovery process of Wu and Tsai's method is quite simple and easy. Given two consecutive pixels $P'_{(i,x)}$ and $P'_{(i,y)}$ of the stego-image, compute their difference value d'_i and obtain $d'_i = |P'_{(i,x)} - P'_{(i,y)}|$. Use the original range table R in the embedding phase to obtain the same R_j and w_j. The length t_i of the hiding capacity also can be gained by using Eq. (2). Calculate the real difference value $d''_i = d'_i - l_j$ and convert the decimal value d''_i into a binary string whose length is t_i bits. For example, assume $d''_i = 7_{(10)}$ and $t_i = 3$, and then secret data $111_{(2)}$ is extracted.

3. The proposed method

Instead of the difference value, the proposed scheme modifies the remainder of two consecutive pixels $P_{(i,x)}$ and $P_{(i,y)}$ for better stego-image quality. The proposed embedding and extracting algorithms are presented in the subsections below.

3.1. The embedding algorithm

Step 1: Given a sub-block F_i composed of two continuous pixels $P_{(i,x)}$ and $P_{(i,y)}$ from the cover image, obtain the difference value d_i, the sub-range R_j such that $R_j \in [l_j, u_j]$, the width $w_j = u_j - l_j + 1$, the hiding capacity t_i bits, and the decimal value t'_i of t_i for each F_i by using Wu and Tsai's scheme according to Section 2.

Step 2: Compute the remainder values $P_{rem(i,x)}$, $P_{rem(i,y)}$ and $F_{rem(i)}$ of $P_{(i,x)}$, $P_{(i,y)}$ and sub-block F_i respectively by using the following equations:

$$
\begin{aligned}
P_{rem(i,x)} &= P_{(i,x)} \bmod t'_i,\\
P_{rem(i,y)} &= P_{(i,y)} \bmod t'_i,\\
F_{rem(i)} &= (P_{(i,x)} + P_{(i,y)}) \bmod t'_i. \qquad (4)
\end{aligned}
$$

Step 3: Embed t_i bits of secret data into F_i by altering $P_{(i,x)}$ and $P_{(i,y)}$ such that $F_{rem(i)} = t'_i$. The optimal approach to altering the $P_{(i,x)}$ and $P_{(i,y)}$ to achieve the minimum distortion is as follows:

Case 1: $F_{rem(i)} > t'_i$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lceil m/2 \rceil, P_{(i,y)} - \lfloor m/2 \rfloor);$

Case 2: $F_{rem(i)} > t'_i$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lfloor m/2 \rfloor, P_{(i,y)} - \lceil m/2 \rceil);$

Case 3: $F_{rem(i)} > t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lfloor m_1/2 \rfloor, P_{(i,y)} + \lceil m_1/2 \rceil);$

Case 4: $F_{rem(i)} > t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lceil m_1/2 \rceil, P_{(i,y)} + \lfloor m_1/2 \rfloor);$

Case 5: $F_{rem(i)} \leqslant t'_i$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lfloor m/2 \rfloor, P_{(i,y)} + \lceil m/2 \rceil);$

Case 6: $F_{rem(i)} \leqslant t'_i$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lceil m/2 \rceil, P_{(i,y)} + \lfloor m/2 \rfloor);$

Case 7: $F_{rem(i)} \leqslant t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lceil m_1/2 \rceil, P_{(i,y)} - \lfloor m_1/2 \rfloor);$

Case 8: $F_{rem(i)} \leqslant t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lfloor m_1/2 \rfloor, P_{(i,y)} - \lceil m_1/2 \rceil).$

In the above approach, $m = |F_{rem(i)} - t'_i|$, $m_1 = 2^{t_i} - |F_{rem(i)} - t'_i|$ and $P'_{(i,x)}, P'_{(i,y)}$ are new pixel values after the embedding of t_i bits of the secret data into sub-block F_i. After Step 3, if $P'_{(i,x)}$ or $P'_{(i,y)}$ overflows the boundary value 0 or 255, then execute Step 4 for revising $P'_{(i,x)}$ and $P'_{(i,y)}$. If not, the purpose of concealing secret data will be completed after the replacement of ($P_{(i,x)}$,$P_{(i,y)}$) by $(P'_{(i,x)}, P'_{(i,y)})$ in the cover image.

Step 4: Consider the three situations below where the falling-off-boundary problem happens and revise $P'_{(i,x)}$ and $P'_{(i,y)}$ as follows:

Case 1: If $P_{(i,x)} \approx 0$, $P_{(i,y)} \approx 0$ and $P'_{(i,x)} < 0$ or $P'_{(i,y)} < 0$, then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be $P''_{(i,x)}$ and $P'_{(i,y)}$ by

$$(P''_{(i,x)}, P''_{(i,y)}) = (P'_{(i,x)} + (2^{t_i})/2, P'_{(i,y)} + (2^{t_i})/2).$$

Case 2: If $P_{(i,x)} \approx 255$, $P_{(i,y)} \approx 255$ and $P'_{(i,x)} > 255$ or $P'_{(i,y)} > 255$, then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be $P''_{(i,x)}$ and $P''_{(i,y)}$ by

$$(P''_{(i,x)}, P''_{(i,y)}) = (P'_{(i,x)} - (2^{t_i})/2, P'_{(i,y)} - (2^{t_i})/2).$$

Case 3: If $P_{(i,x)}$ and $P_{(i,y)}$ form a great contrast (i.e. $d_i > 128$), then re-adjusted $P'_{(i,x)}$ and $P'_{(i,y)}$ by

$$
(P''_{(i,x)}, P''_{(i,y)}) = \begin{cases}
(0, P'_{(i,y)} + P'_{(i,x)}), \\
\quad \text{if } P'_{(i,x)} < 0 \text{ and } P'_{(i,y)} \geqslant 0; \\
(P'_{(i,x)} + P'_{(i,y)}, 0), \\
\quad \text{if } P'_{(i,x)} \geqslant 0 \text{ and } P'_{(i,y)} < 0; \\
(255, P'_{(i,y)} + (P'_{(i,x)} - 255)), \\
\quad \text{if } P'_{(i,x)} > 255 \text{ and } P'_{(i,y)} \geqslant 0; \\
(P'_{(i,x)} + (P'_{(i,y)} - 255), 255), \\
\quad \text{if } P'_{(i,x)} \geqslant 0 \text{ and } P'_{(i,y)} > 255.
\end{cases}
$$

After Step 4, $(P'_{(i,x)}, P'_{(i,y)})$ can be corrected so that the range of $(P''_{(i,x)}, P''_{(i,y)})$ cannot go below 0 or over 255. Finally, we put use $(P''_{(i,x)}, P''_{(i,y)})$ in place of ($P_{(i,x)}$, $P_{(i,y)}$) in the cover image and the embedding algorithm is accomplished.

Table 2
An illustration of the proposed algorithm modifying the remainder of two consecutive pixels

Secret data (decimal value)	$P_{(i,x)} = 32$ $P_{rem(i,x)} = 0$	$P_{(i,y)} = 32$, $P_{rem(i,y)} = 0$	The total remainder $F_{rem(i)}$
0	No modify	No modify	0
1	+1	No modify	1
2	+1	+1	2
3	+2	+1	3
4	+2	+2	4
5	−2	−1	5
6	−1	−1	6
7	−1	No modify	7

A simple example of regulating the remainder value for hiding secret data is shown in Table 2. Suppose we have a sub-bock F_i with two successive pixel values $P_{(i,x)} = 32$ and $P_{(i,y)} = 32$. Then, the remainder value $F_{rem(i)}$ of F_i is 0. If the 3 bits (i.e. $t_i = 3$, and $t'_i = 2^3 = 8$) of the secret data are selected to be embedded into F_i, $P_{(i,x)}$ and $P_{(i,y)}$ will be modified to hold the 3-bit secret data. Table 2 demonstrates that our scheme has better performance in reducing the difference between ($P_{(i,x)}$, $P_{(i,y)}$) and $(P'_{(i,x)}, P'_{(i,y)})$.

Next, we offer an example to show how our mechanism of keeping the pixel values from exceeding the range $[0, 255]$ after secret data embedding. As shown in Table 3, we reassume $P_{(i,x)} = 0$ and $P_{(i,y)} = 0$ in the previous example, and then the falling-off-boundary problem happens such that $P'_{(i,x)} < 0$ or $P'_{(i,y)} < 0$ when the decimal value of the secret data is 5, 6, or 7. However, $P'_{(i,x)}$ and $P'_{(i,y)}$ can be re-adjusted by adding up to 4 synchronously. After that, the values of $P''_{(i,x)}$ and $P''_{(i,y)}$ will fall within the range of 0–255.

3.2. The extracting algorithm

In the recovery process, we can quickly extract the secret data without using the original image. Nevertheless, it is

Table 3
An illustration of solving the falling-off-boundary problem by re-modifying the $(P'_{(i,x)}, P'_{(i,y)})$

Secret data (decimal value)	$P_{(i,x)} = 0$, $P_{rem(i,x)} = 0$	$P_{(i,y)} = 0$, $P_{rem(i,y)} = 0$	The total remainder $F_{rem(i)}$
0	No modify	No modify	0
1	+1	No modify	1
2	+1	+1	2
3	+2	+1	3
4	+2	+2	4
5	$(-2) + 4 = 2$	$(-1) + 4 = 3$	5
6	$(-1) + 4 = 3$	$(-1) + 4 = 3$	6
7	$(-1) + 4 = 3$	$(0) + 4 = 4$	7

essential to use the original range table R designed in the embedding phase in order to figure out the embedding capacity for each sub-block F_i. Given a sub-block F_i with two consecutive pixels from the stego-image with their pixel values being $P_{(i,x)}$ and $P_{(i,y)}$ respectively, the difference value d_i of $P_{(i,x)}$ and $P_{(i,y)}$ can be derived by Eq. (1). Each F_i can be related to its optimal sub-range R_j from the original table R according to the difference value d_i. Hence, we can compute the width of the sub-range by $w_j = u_j - l_j$, and the number of bits t_i of the secret data can be extracted from F_i by Eq. (1). Eventually, we compute the remainder value of F_i by using Eq. (2) and transform the remainder value $F_{rem(i)}$ into a binary string with the length t_i. After that, the extracting algorithm is accomplished. For example, assume two successive pixel values of the stego-image are $P_{(i,x)} = 34$ and $P_{(i,y)} = 33$, and the hidden capacity is 3 bits (i.e. $t_i = 3$). $F_{rem(i)}$ can be gained by $(33 + 34) \bmod 2^3 = 3$. Convert the remainder value 3 into a binary string whose length is 3, and then we have $3_{(10)} = 011_{(2)}$. That is to say, the secret data $011_{(2)}$ is retrieved from the sub-block in which the pixel values are $P_{(i,x)} = 34$ and $P_{(i,y)} = 33$.

4. Experimental results and analysis

4.1. Experimental results

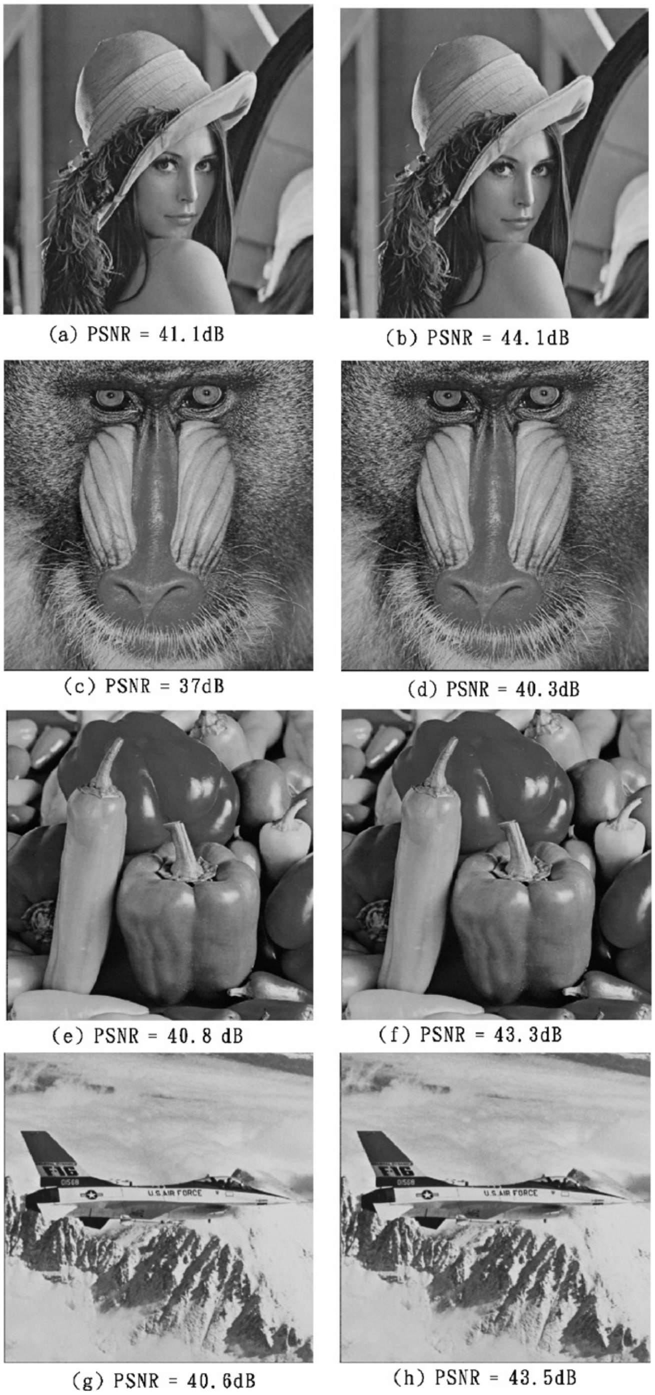
In this section, we shall present our experimental results to demonstrate the proposed algorithm can perform better than Wu and Tsai's scheme. We designed a range table R consisting of 6 sub-ranges R_j, for $j = 1, 2, \ldots, 6$, where their widths were 8, 8, 16, 32, 64, and 128 respectively. The range of each R_j was $R_1 = [0, 7]$, $R_2 = [8, 15]$, $R_3 = [16, 31]$, $R_4 = [32, 63]$, $R_5 = [64, 127]$ and $R_6 = [128, 255]$. Twelve cover images "Lena", "Baboon", "Peppers", "Jet", "Tank", "Airplane", "Truck", "Elaine", "Couple", "Boat", "Man", and "Tiffany", shown in Figs. 1–3, were used as test images in our experiments. The size of all the cover images was 512×512. We used a series of pseudo-random numbers as the secret data to be embedded into the cover images. The peak signal-to-noise ratio (PSNR) was utilized to evaluate the stego-image quality. The PSNR is defined as follows:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}\ \text{dB}$$

and

$$\text{MSE} = \left(\frac{1}{M \times N}\right)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{i,j} - \beta_{i,j})^2.$$

Here, $\alpha_{i,j}$ is the pixel of the cover image where the coordinate is (i,j), and $\beta_{i,j}$ is the pixel of the stego-image where the coordinate is (i,j). M and N represent the size of the image. A larger PSNR value indicates the fact that the discrepancy between the cover image and the stego-image is more invisible to the human eye.


(a) PSNR = 41.1dB

(b) PSNR = 44.1dB

(c) PSNR = 37dB

(d) PSNR = 40.3dB

(e) PSNR = 40.8 dB

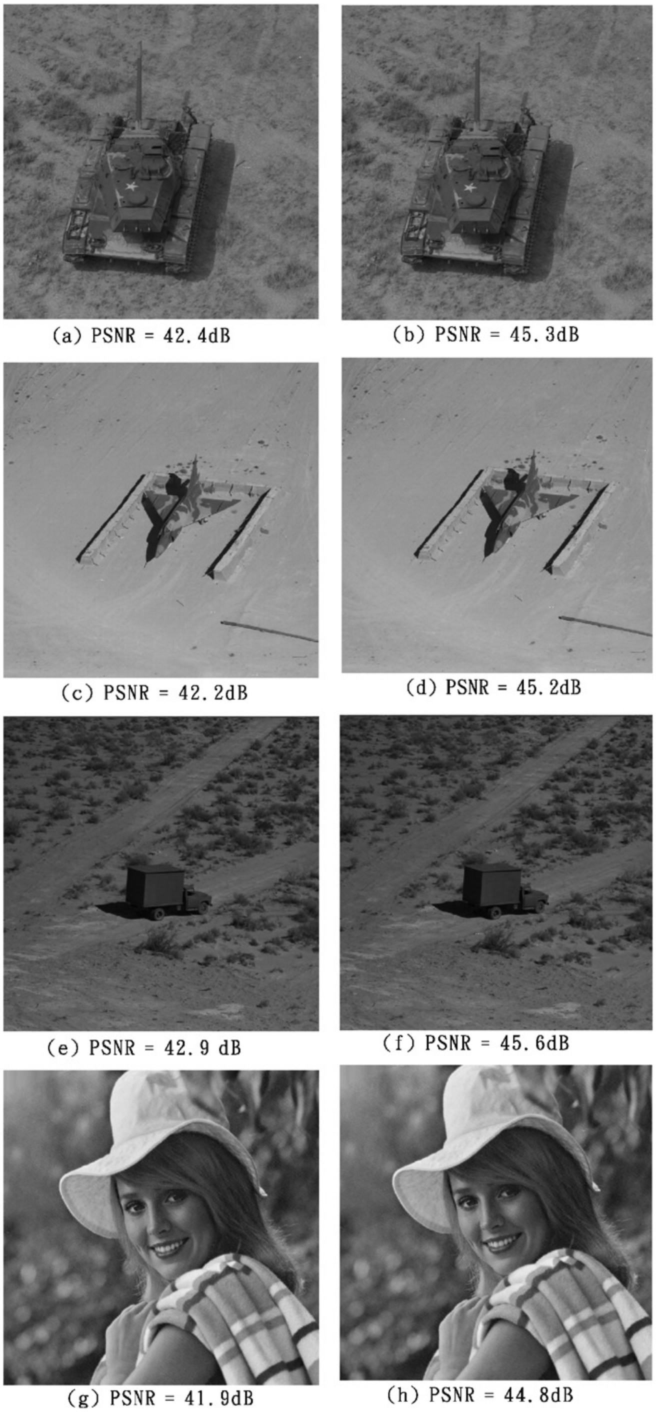
(f) PSNR = 43.3dB

(g) PSNR = 40.6dB

(h) PSNR = 43.5dB

Fig. 1. The size of each stego-image is 512×512: (a), (c), (e), and (g) are the stego-images produced by Wu and Tsai's scheme; (b), (d), (f), and (h) are the stego-images produced by our method.

The results in parts (a), (c), (e), and (g) of Figs. 1–3 are the stego-images produced by Wu and Tsai's method, and those in parts (b), (d), (f), and (h) of Figs. 1–3 are the stego-images produced by the proposed method. As the figures show, whether it is our scheme or Wu and Tsai's scheme, there are not any visual artifacts present. However, the PSNR values obtained demonstrate that the proposed scheme is superior to Wu and Tsai's scheme (see Table 4).



(a) PSNR = 42.4dB (b) PSNR = 45.3dB

(c) PSNR = 42.2dB (d) PSNR = 45.2dB

(e) PSNR = 42.9 dB (f) PSNR = 45.6dB

(g) PSNR = 41.9dB (h) PSNR = 44.8dB

Fig. 2. The size of each stego-image is 512 × 512: (a), (c), (e), and (g) are the stego-images produced by Wu and Tsai's scheme; (b), (d), (f), and (h) are the stego-images produced by our method.

(a) PSNR = 40.2dB (b) PSNR = 43.5dB

(c) PSNR = 38.9dB (d) PSNR = 42.1dB

(e) PSNR = 39.1dB (f) PSNR = 42.1dB

(g) PSNR = 40.8dB (h) PSNR = 43.9dB

Fig. 3. The size of each stego-image is 512 × 512: (a), (c), (e), and (g) are the stego-images produced by Wu and Tsai's scheme; (b), (d), (f), and (h) are the stego-images produced by our method.

In Table 4, we see that the PSNR values given by our method where increased by 2.5–3.3 dB. This is because the distortion of the edge areas can be greatly improved by the proposed scheme. Fig. 4 shows that the major difference between Wu and Tsai's scheme and our scheme lies in the edges of the image after secret data embedding. Fig. 4 shows the gray-level values scaled twenty times. As a result, there is no doubt that the stego-image quality produced by the proposed scheme was quite good with no visible difference from the original cover image.

Finally, we have also compared the proposed scheme with the two-side match scheme by Chang and Tseng (2004). The two-side match method is similar to Wu and

Table 4
The results of embedding the same random message by Wu and Tsai's including the proposed methods

Cover-images (512×512)	Wu and Tsai's method		Our method	
	Capacity (bytes)	PSNR(dB)	Capacity (bytes)	PSNR (dB)
Lena	51,219	41.1	51,219	44.1
Baboon	57,146	37	57,146	40.3
Peppers	50,907	40.8	50,907	43.3
Jet	51,224	40.6	51,224	43.5
Tank	50,449	42.4	50,449	45.3
Airplane	49,739	42.2	49,739	45.2
Truck	50,065	42.9	50,065	45.6
Elaine	51,074	41.9	51,074	44.8
Couple	51,603	40.2	51,603	43.5
Boat	52,635	38.9	52,635	42.1
Man	52,945	39.1	52,945	42.1
Tiffany	50,920	40.8	50,920	43.9

Tsai's scheme in the way that two consecutive pixels are picked out each time to hide data. The comparison results are shown in Table 5, where the PSNR values demonstrate that the proposed scheme can improve the stego-image quality of Chang and Tseng's scheme.

4.2. Analysis and discussions

In this section, we analyze the performance of PVD and that of the proposed method in terms of the stego-image quality and the robustness against the RS detection attack. To evaluate the schemes in terms of the stego-image quality, we can check out both the optimal stego-image quality, where the minimum pixel value alteration happens, and the worst stego-image quality, where the maximum pixel-value alteration happens. First, we present a simple example to show the optimal case of the PVD method. Assume the secret data is 3 bits, and the pixel values are 30 and 34 respectively. All the possibilities of modifying the pixel values 30 and 34 such that $d_i = t_i'$ are shown in Table 6.

In Table 6, we can see the maximum variation of single pixel value is 2. In this optimal case for Wu and Tsai's scheme, the original difference value d_i is approximated to (2^{t_i-1}). Naturally, if the original difference value d_i is approximated to 0 or 2^{t_i}, then it will make the worst case. An example of the worst case can be seen in Table 1. In Table 1, the original difference value is 0 and the maximum modification of pixel value is 4. Apparently the worst case wastes about double the stego-image quality of the optimal case. The stego-image quality of PVD method can vary between the optimal case and the worst case. However, there is only the optimal case when the proposed optimal embedding algorithm is used. In our scheme, assume the secret data is 3 bits. Then, the maximum modification of pixel value is 2 whether the original remainder value approximates 0 or 2^{t_i-1} or 2^{t_i}. Take Table 2 for example. In spite of that fact that the original remainder approximates 0, the maximum variation of pixel value is 2. Accordingly, the proposed method can reduce the distortion of the stego-image based on the remainder value of the two consecutive pixels.

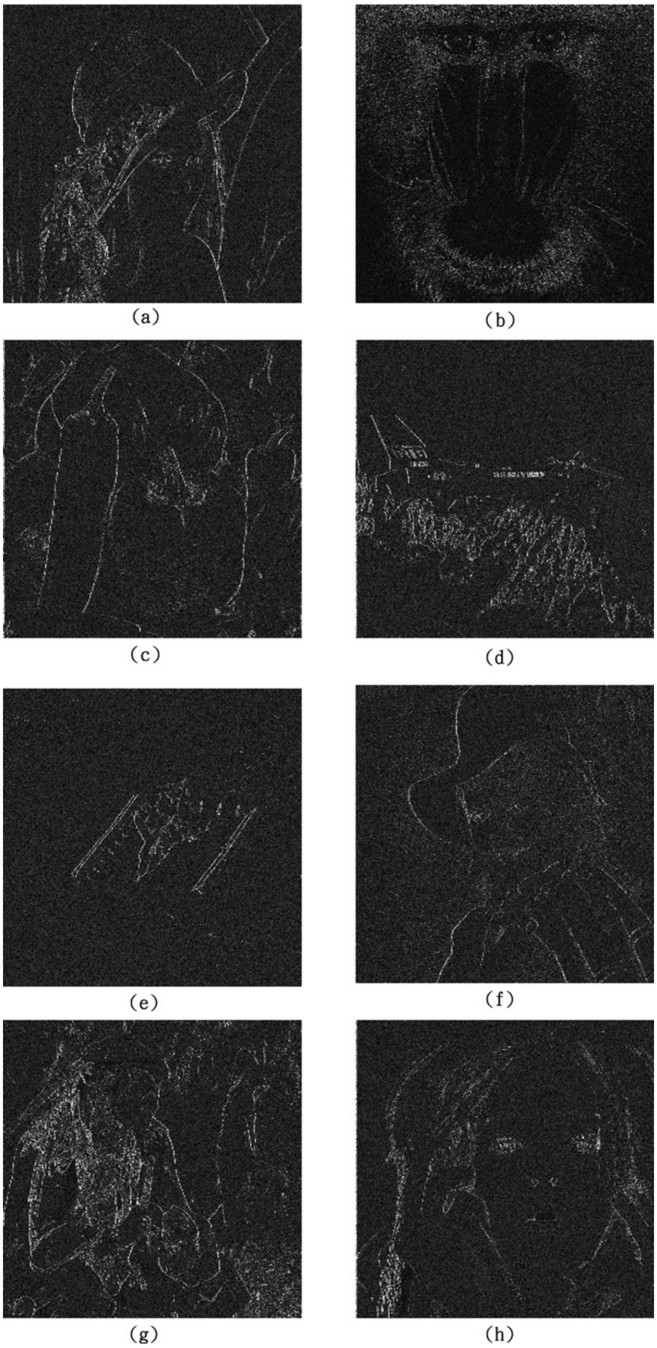


Fig. 4. The difference images between the stego-image of Wu and Tsai's scheme and the proposed scheme.

In addition, the proposed scheme is secure against the RS detection attack. The RS detection method by Fridrich et al. (2001) can directly judge whether the stego-image is secure without visual inspection. Fridrich et al. utilize the dual statistics method to classify all the pixels of a stego-image into three pixel groups: the regular group R_m or R_{-m}, the singular group S_m or S_{-m}, and the unusable group. The stego-image will pass the RS steganalysis when $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$. Otherwise, the stego-image will

Table 5
The results of embedding the same random message by Chan and Tseng's including the proposed methods

Cover-images (512 × 512)	Chan and Tseng's method		Our method	
	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)
Lena	48,626	41.2	51,219	44.1
Baboon	57,146	34.1	57,146	40.3
Peppers	50,907	40.6	50,907	43.3
Jet	51,224	40.3	51,224	43.5
Tank	50,449	41.7	50,449	45.3
Airplane	41,829	42.7	49,739	45.2
Truck	50,065	42.2	50,065	45.6
Elaine	51,074	40.8	51,074	44.8
Couple	51,603	37.1	51,603	43.5
Boat	52,635	38.7	52,635	42.1
Man	52,945	38.3	52,945	42.1
Tiffany	50,920	41.2	50,920	43.9

Table 6
An illustration of optimal case by using Wu and Tsai's method

Secret data (decimal value)	$P_{(i,x)} = 30$	$P_{(i,y)} = 34$	New difference value of $P_{(i,x)}$ and $P_{(i,y)}$
0	+2	−2	0
1	+1	−2	1
2	+1	−1	2
3	No modify	−1	3
4	No modify	No modify	4
5	No modify	+1	5
6	−1	+1	6
7	−1	+2	7

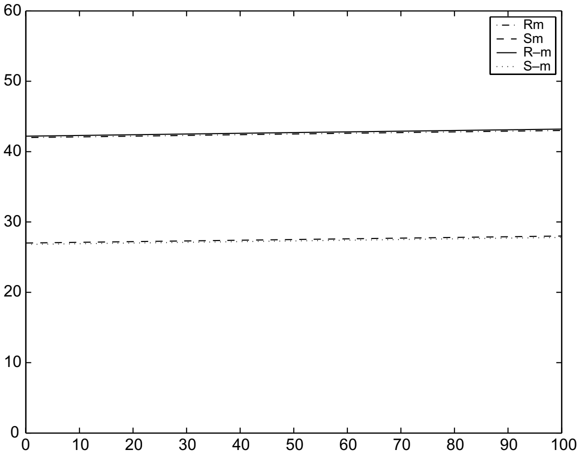


Fig. 5. The RS-diagram yields by the dual statistics detecting for stego-image produced by the proposed scheme.

be judged as a suspicious object. The detection results our scheme gave (with the stego-image being the one in Fig. 1b) are shown in Fig. 5, where the x-axis represents the percentage of hiding capacity and the y-axis the percentage of the regular and singular pixel groups with masks $m = [0110]$ and $-m = [0-1-10]$. In Fig. 5, the expected values of R_m and S_m are almost equal to those of R_{-m} and S_{-m} respectively. Moreover, we have also tested the other stego-images processed by using the proposed scheme, and the detection results are the same as what Fig. 5 reveals. Accordingly, we can make a solid statement that the proposed scheme is secure against the RS detection attack.

5. Conclusions

In this paper, we propose a novel scheme to greatly reduce the visibility of the hiding effect present in the PVD method. The proposed scheme utilizes the remainder of the two consecutive pixels to record the information of the secret data which gains more flexibility, capable of deriving the optimal remainder of the two pixels at the least distortion. The hiding effect that appears in the stego-image when Wu and Tsai's scheme is used to hide the secret data can be significantly decreased by the proposed optimal embedding algorithm. Besides, the proposed method can also solve the falling-off-boundary problem by re-adjusting the remainder of the two pixels, staying secure against the RS detection attack. Experimental results show the proposed scheme has a much better performance than Wu and Tsai's scheme in terms of stego-image quality.

Acknowledgements

We thank many anonymous referees for their suggestions to improve this paper. This work is supported in part by National Science Council and Taiwan Information Security Center at NCTU, Taiwan, ROC.

References

Chan, C.K., Cheng, L.M., 2004. Hiding data in images by simple LSB substitution. Pattern Recognition 37 (March), 469–474.

Chang, C.C., Tseng, H.W., 2004. A steganographic method for digital images using side match. Pattern Recognition Letter 25 (September), 1431–1437.

Chang, C.C., Hsiao, J.Y., Chan, C.S., 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognition 36 (July), 1583–1595.

Feng, J.B., Lin, I.C., Tsai, C.S., Chu, Y.P., 2006. Reversible watermarking: current status and key issues. International Journal of Network Security 2 (May), 161–170.

Fridrich, J., Goljan, M., Du, R., 2001. Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of ACM Workshop on Multimedia and Security, pp. 27–30.

Ker, A.D., 2004. Quantitative evaluation of pairs and RS steganalysis. In: Proceedings of the SPIE Security, Steganography, and Watermarking of Multimedia Contents, vol. 5306, pp. 83–97.

Liao, Z., Huang, Y., Li, C., 2007. Research on data hiding capacity. International Journal of Network Security 5 (September), 140–144.

Lin, C.C., Tsai, W.H., 2004. Secret image sharing with steganography and authentication. The Journal of Systems and Software 73 (November), 405–414.

Lou, D.C., Liu, J.L., 2002. Steganographic method for secure communications. Computers and Security 21 (October), 449–460.

Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., 1999. Information hiding – a survey. In: Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Content, vol. 87, pp. 1062–1078.

Simmons, G.J., 1984. The prisoners' problem and the subliminal channel. In: Proceedings of Crypto'83, pp. 51–67.

Thien, C.C., Lin, J.C., 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognition 36 (December), 2875–2881.

Tseng, Y.C., Pan, H.K., 2002. Data hiding in 2-color images. IEEE Transactions on Computers 51 (July), 873–878.

Tseng, Y.C., Chen, Y.Y., Pan, H.K., 2002. A secure data hiding scheme for binary images. IEEE Transactions on Communications 50 (August), 1227–1231.

Wang, S.J., 2005. Steganography of capacity required using modulo operator for embedding secret image. Applied Mathematics and Computation 164 (May), 99–116.

Wang, C.M., Wang, P.C., 2006. Steganography on point-sampled geometry. Computers and Graphics 12 (April), 244–254.

Wang, R.Z., Lin, C.F., Lin, J.C., 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 34 (March), 671–683.

Wu, N.I., Hwang, M.S., 2007. Data hiding: current status and key issues. International Journal of Network Security 4 (January), 1–9.

Wu, M., Liu, B., 2004. Data hiding in binary image for authentication and annotation. IEEE Transactions on Multimedia 6 (August), 528–538.

Wu, D.C., Tsai, W.H., 2003. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters 24 (June), 1613–1626.

Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings – Vision Image and Signal Processing 152 (October), 611–615.

Zhong, S., Cheng, X., Chen, T., 2007. Data hiding in a kind of PDF texts for secret communication. International Journal of Network Security 4 (January), 17–26.