Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A data hiding scheme using pixel value differencing and improving exploiting modification directions

Shu-Yuan Shen [a,b], *Li-Hong Huang* [a,c,*]

[a] *College of Mathematics and Econometrics, Hunan University, Changsha, Hunan 410082, China*
[b] *School of Software South China Normal University, Guangzhou 510631, China*
[c] *Institute of Applied Mathematics and Intelligent Information Processing, Hunan Women's University, Changsha, Hunan 410004, China*

ARTICLE INFO

Article history:
Received 5 January 2014
Received in revised form
15 June 2014
Accepted 28 July 2014
Available online 14 August 2014

Keywords:
Data hiding
Hilbert curve
PVD
Optimization problem
Exploiting modification directions

ABSTRACT

The fundamental requirements of information hiding systems are good visual quality, high hiding capacity, robustness and steganographic security. In this paper, we propose a new data hiding method which can increase the steganographic security of a data hiding scheme because it is less detectable by RS detection attack and the steganalytic histogram attack of pixel-value difference. In our method, a cover image is first mapped into a 1D pixels sequence by Hilbert filling curve and then divided into non-overlapping embedding units with two consecutive pixels. Because the human eyes tolerate more changes in edge and texture areas than in smooth areas, and pixel pairs in these areas often possess larger differences, the method exploits pixel value differences (PVD) to estimate the base of digits to be embedded into pixel pairs. Pixel pairs with larger differences are embedded with digits in larger base than those pixel pairs with smaller differences to maximize the payload and image quality. By using an optimization problem to solve the overflow/underflow problem, minimal distortion of the pixel ternaries cause by data embedding can be obtained. The experimental results show our method not only to enhance the embedding rate and good embedding capacity but also to keep stego-image quality.

1. Introduction

Data hiding techniques can be carried out in three domains (Langelaar et al., 2000), namely, spatial domain (Mielikainen, 2006), compress domain (Chang et al., 2006, 2009, 2009a), and frequency domain (Lee et al., 2007). Each domain has its own advantages and disadvantages in regard to hiding capacity, execution time, and storage space. The fundamental requirements of information hiding systems are good visual quality (i.e., image quality), high hiding capacity, robustness, and steganographic security (i.e., statistically undetectable) (Langelaar et al., 2000).

Designing a new data hiding system achieving good visual quality, high hiding capacity, robustness, and steganographic security is a technically challenging problem. Thus, there are different approaches in designing data hiding systems in the literature. Some of these approaches are as follows. The first

* *Corresponding author*. College of Mathematics and Econometrics, Hunan University, Changsha, Hunan 410082, China.
E-mail addresses: ssyuan02@126.com (S.-Y. Shen), lhhuang@hnu.edu.cn (L.-H. Huang).

http://dx.doi.org/10.1016/j.cose.2014.07.008
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

approach is to increase hiding capacity (also called embedding capacity or payload) while maintaining a good visual quality or at the cost of lower visual quality (Lan and Tewfik, 2006). This approach is appropriate to applications where high hiding capacity is desired. The second approach purposes to devise a robust data hiding scheme (Ni et al., 2008). This design serves robust watermarking systems. The third approach aims at enhancing visual quality while keeping the same hiding capacity or at the cost of lower hiding capacity (Ni et al., 2006). The fourth approach intends to devise a data hiding scheme with high embedding efficiency (Fridrich et al., 2006; Mielikainen, 2006; Westfeld, 2001). This approach can increase the steganographic security of a data hiding scheme because it is less detectable by statistical steganalysis (Fridrich et al., 2007).

In recent years many researchers are more enthusiastic to improve the embedding efficiency and decrease the possibility of detection. Least-significant-bit (LSB) matching is the conventional efficient steganography method, and it is proved much more difficult to detect than simple LSB replacement.

To defeat the histogram based steganalysis methods, many efforts have been made by researchers to protect the histograms of images. One of the first solutions to defeat these attacks was LSB matching. LSB matching increases or decreases the pixel values with the same probabilities when the least significant bit of the pixel value is not equal to the message bit. In 2006, Mielikainen (2006) developed a pairwise LSB matching method to improve the embedding efficiency. Nevertheless, Mielikainen's scheme is incomplete because the scheme only exploits two modification directions for secret data embedding.

Tan and Li (2012) showed that the readjusting step of LSB matching revised-based edge-adaptive (Luo et al., 2010) produces some effects in the long exponential tail of the histogram of the absolute difference of the pixel pairs. By using these effects, they proposed a steganalysis technique that could detect stego images and could estimate the used threshold in the data hiding process. In addition, Ghazanfari et al. (Qazanfari and Safabakhsh, 2012, 2013) proposed an adaptive steganography method based on the LSB matching which increases the capacity up to 150% (Qazanfari and Safabakhsh, 2012) and 158% (Qazanfari and Safabakhsh, 2013). Their second work (Qazanfari and Safabakhsh, 2013) is the extension of their previous scheme (Qazanfari and Safabakhsh, 2012) into the DCT domain. The LSB$^{=}$ method suggested by Wu et al. (Wu, 2008) preserved the image histogram in spatial domain by embedding some extra bits in images. This method, however, results in statistical and perceptual distortions. A new technique for image steganography, called LSB^{++}, was proposed in Kazem et al (2011), which improves the LSB^{+} by keeping some pixels from changing, results in reducing the number of extra bits. Their later work (Qazanfari and Safabakhsh, 2014), they improved the LSB^{++} method by proposing a technique to distinguish the sensitive pixels and keep them from extra bit embedding, as the embedding process causes fewer traces in the co-occurrence matrixes.

To fully exploit different modification directions for secret data embedding. Zhang and Wang (2006) also proposed the exploiting modification direction (EMD) method, which employs n pixels as an embedding unit, and embeds digits in $2n + 1$ base. Its maximum payload is $1/2\log_2 5 \approx 1.161$ bpp when $n = 2$. Zhang and Wang claimed that the modification directions of Mielikainen's scheme are not explored fully. Specifically, the PSNR value of the EMD method is slightly smaller than that of Mielikainen's scheme at hiding capacity of 1 bpp. In addition, for $n = 2$, Zhang and Wang's method only utilizes four modification directions. Kieu and Chang (2011) (FEMD) proposed a novel extraction function (also called the modified extraction function) by modifying the extraction function proposed by Zhang and Wang (2006). The modified extraction function allows the proposed method to exploit eight modification directions for embedding secret data, restrict the embedding distortion into a square of various sizes (e.g. 2×2, 3×3, and so on) and use the minimum distortion embedding (MDE) process. By this way, the proposed method can achieve various hiding capacities and good visual qualities compared to two recently published works, namely Mielikainen's method (Mielikainen, 2006), Zhang and Wang's method (Zhang and Wang, 2006). To solve the irreversibility of the EMD method in (Zhang and Wang, 2006; Qin et al. 2014) proposed a novel data hiding scheme based on EMD with reversibility by using two steganographic images, which can also achieve satisfactory performances of the hiding capacity and the stego image quality.

Inspired by EMD, Chao et al. (2009) proposed a diamond encoding (DE) method to greatly improve the payload of EMD. DE employs a search region of $B = 2k^2 + 2k + 1$ elements to increase the payload because digits in base B can be embedded into a pixel pair, where $k \geq 1$. A larger k indicates that a larger payload can be embedded with greater image distortion. DE employs an extraction function to generate diamond characteristic values (DCV), and uses an embedding parameter k to control the payload. A digit in a B-ary notational system can be concealed into two pixels by modifying the pixel pairs according to their DCV's neighborhood set. However, DE can't embed digits in any notation system and the distortion caused by DE is larger than some other embedding methods with the same payload. Although DE has these advantages, it does not allow embedding digits in multiple bases, Which is the essential requirement for an embedding method with the consideration of HVS. Besides, to prevent the overflow and underflow problems from occurring, the pixel values exceed 0 or 255 will be added or subtracted by B to keep the pixel values within the range [0, 255]. This adjustment may cause a large distortion, and may result in image noise when the embedding parameter k is large. For example, if $k = 5$, then the base B used to conceal data is $2 \times 5^2 + 2 \times 5 + 1 = 61$. However, a pixel value that is subtracted by 61 or added by 61 will cause a large distortion.

The aforementioned methods regard all pixels within an image can tolerate equal amounts of changes without causing visual artifacts to an observer. However, the tolerance of the changes to pixel values is different in smooth and edge areas according to human visual system (HVS). Based on the fact that edge areas can tolerate more severe changes than smooth areas, edge adaptive schemes have been proposed, which conceal more data in edge areas to acquire more embedding capacity whereas conceal less data in smooth area to preserve the visual quality. Moreover, in the kieu-Chang's scheme needs a storage place to store the search matrix data and they use the match method to embed the secret data. As a result, it is time-consuming and impractical for those method.

Another group of embedding strategies takes HVS into consideration, namely these methods embed more data in edge areas to acquire more payload whereas embed less data in smooth areas to preserve the visual quality. In 2003, Wu and Tsai (2003) proposed a data embedding method based on pixel value differencing (PVD). In their method, the difference of two pixels in the cover image is calculated. The number of bits to be embedded into these two pixels is determined by their absolute difference and a pre-defined range table. Data bits are then embedded by modifying these two pixel values. Because the same range in the range table will be referred before and after data embedding, the same number of data bits can be determined and thus the embedded data bits can be exactly extracted. Due to pixel pairs with larger difference are often located in complex regions, PVD embeds more data into pixel pairs with larger differences. However, the PVD method may cause considerable distortion, leading to degradation in image quality. Moreover, the difference histogram of the stego image apparently deviates from that of the natural image; therefore, it is vulnerable to the detection of histogram analysis. In 2008, Wang et al. (2008) adopted the concept of PVD and proposed a data embedding method using pixel value differencing and modulus (MF-PVD). MF-PVD used the same mechanism that was used in (Wu and Tsai, 2003) to determine the number of bits to be embedded into a given pixel pair, and then the remainder of these two pixels is calculated. Data is then embedded by modifying the remainder values. Compared to Wu and Tsai method, MF-PVD achieves a higher payload and better image quality.

Similarly, Hong (2012) proposed a new scheme using the concept of pixel value differentiation and a patched reference table (PVD-PRT) to provide a better image quality and extendable embedding capacity. Furthermore, Lee et al. presented a practical method of using a cover image to hide the secret message using tri-way pixel-value differencing. The goal of the proposed approach is to provide secrecy while avoiding the detection by dual statistics steganalysis (Lee, 2012). In addition, Hong and Chen (2012) proposed a steganography method based on pixel pair matching (PPM). This method utilizes the values of pixel pairs as a reference coordinate. To hide the message bits, this method first searches for a coordinate in the neighborhood set of this pixel pair based on the message bits. Then, this method replaces the pixel pair with the selected coordinate to embed the message bits.

In above PVD-based methods, the differences used for data hiding are collected along a simple travel route, such as in the raster scanning order or zig-zag scanning order. These scanning methods take no account of image's contents and destroy the correlation of local pixels to some extent, so some revealing clues for detectors will be leaved. Hilbert filling order has better locality-preserving behavior than raster order and zig-zag order. This locality property preserves the correlation of adjacent pixels well and thus makes the distortion caused by data embedding more inconspicuous (Westfeld, 2005).

In order to quick embedding secret and improve on these shortcomings, in this paper, we adopt the concept of PVD and employ two pixels as an embedding unit. Hilbert filling curve is used to map the cover image into a 1D pixel sequence. The proposed method not only consider HVS and the correlation of local pixels but also avoid storing the search matrix data.

The following is the introduction of each chapter. The second chapter is the related works, briefly reviewing EMD and Kieu-Chang's method. The third chapter explains the proposed method, describing the embedding and extracting algorithm by using a mathematical approach. The fourth chapter is an example of the embedding and extracting algorithms of the proposed method. The fifth chapter lists the experimental results. The sixth chapter is analysis and discussions. The seventh chapter is the conclusion and future work.

2. Related works

2.1. *Exploiting modification direction (EMD)*

In the EMD scheme, all pixels in a cover image are pseudo-randomly permuted using a secret key to partition the pixels into a series of groups. A pixel group will be denoted as (g_1, g_2,…, g_n), where $n \geq 2$. In order to hide secret digits, digits for hiding need to be converted into a sequence of digits of a $(2n+1)$-ary notational system. A secret binary message can be divided into $L = \lfloor K \times \log_2(2n+1) \rfloor$ bits, and the decimal value of each part of the secret will be represented by K digits in the $(2n+1)$-ary notational system. In this scheme, only one pixel in each pixel group is incremented or decremented by 1. A vector (g_1, g_2,…, g_n) in n-dimensional space is represented by its f value, which is calculated using Eq. (1).

$$f(g_1,\ g_2, \ldots,\ g_n) = (g_1 \times 1 + g_2 \times 2 + \ldots + g_n \times n)\mathrm{mod}(2n+1). \tag{1}$$

No modification of a pixel g is needed if a secret digit d equals the extraction function of the original pixel group. If the secret digit $d \neq f$, we must calculate $s = d - f \bmod (2n+1)$. If s is no more than n, the value of g_s is increased by 1; otherwise, the value of g_{2n+1-s} is decreased by 1. The merit of the EMD scheme is that it provides good stego image quality with a peak signal-to-noise ratio (PSNR) of more than 52 dB, because at most one cover pixel needs to be increased or decreased by 1 in each pixel group. Thus, the stego image has the advantage of resisting various steganalysis techniques. However, the EMD scheme has room for further improvement of its embedding capacity, because the embedding rate is $R = (\log_2 (2n+1))/n$.

2.2. *Kieu and Chang scheme (Kieu and Chang, 2011)*

In order to improve the data hiding capacity kieu and Chang modified the extract function and proposed a new data hiding scheme to improve the data hiding capacity from 1 bpp to 4.5 bpp. In other words, the main idea of Kier-Chang scheme is that the value of s^2 can be hidden into 2 adjacent pixels in the cover image. Therefore, Kieu and Chang proposed another extraction function F (x_i, x_{i+1}) shown as Eq. (2)

$$F(x_i,\ x_{i+1}) = [x_i \times (s-1) + x_{i+1} \times s] \quad \mathrm{mod}\ \ s^2. \tag{2}$$

where x_i is the ith pixel value, s is the weighting coefficient. Then, Kieu and Chang use a 256 × 256 $S-$ matrix to represent F

(x_i, x_{i+1}) where the value of the x_i^{th} row and the x_{i+1}^{th} column in $S-$ matrix is F (x_i, x_{i+1}). The symbol S [x_i] [x_{i+1}] is used to represent the matrix, i.e., $S[x_i][x_{i+1}] = F(x_i, x_{i+1})$. The result of the extraction function F (x_i, x_{i+1}) with different $s(s \in 2, 3, 4)$. Subsequently, using the search matrix structure $W_{(2r+1) \times (2r+1)}$ (s, (x_i, x_{i+1}), r) to embed the secret data by Kieu and Chang. In other words, the k-bit secret data can be embedded into pair (x_i, x_{i+1}) of cover image by using the $S-$ matrix structure with the search range r, where $k = \lfloor \log_2 s^2 \rfloor$ and $r = \lfloor s/2 \rfloor$. In order to reduce stego-image distortion, Kieu and Chang use the minimum distortion strategy method shown as

$$D_{\min} = \min_{j=a,b,c}\left(\left|x_i - x_j\right| + \left|x_{i+1} - y_j\right|\right). \tag{3}$$

to select local optimal solution $D_{\min}$ in S (x_j, y_j). According their embedding secret data method, it needs a storage place to store the search matrix data and then they use the match method to embed the secret data. As a result, it is time-consuming and impractical for this method.

3. The proposed scheme

For an image with size $M \times N$, we bring the image into a Hilbert 1D sequence and then partition the sequence into non-overlapping embedding units with two consecutive pixels, say (x_{2i}, x_{2i+1}). For a given embedding unit, we calculate the differences of the adjacent pixel values $d_i = |x_{2i+1} - x_{2i}|$. On the other hand, we design a range table which consists of the contiguous sub-ranges W_j ($j = 1, 2, \cdots, 6$). In other words,

$$\begin{aligned} W &= \{W_j = [l_j, u_j]\} \\ &= \{[0, 7], [8, 15], [16, 31], [32, 63], [64, 127], [128, 255]\}. \end{aligned}$$

where the lower bound, upper bound and width of the range W_j are denoted by l_j, u_j and w_j, respectively. The width w_j of W_j is calculated by $w_j = u_j - l_j + 1$. If d_i belongs to range W_j, then $s_i = \lfloor \log_2 w_j \rfloor$, $k_i = \lfloor \log_2 s_i^2 \rfloor$. We select k_i bits from a secret bit stream S and convert them into the decimal number s_t.

3.1. The embedding algorithm

The detailed embedding steps are summarized below.

Step 1: Obtain 1D sequence V by scanning image I with Hilbert curve and partition V into $L = M \times N/2$ non-overlapping blocks with two consecutive pixels (x_{2i}, x_{2i+1}).
Step 2: Calculate the difference value d_i for each adjacent pixel. From the w_j division, find out the range which d_i belong to.
Step 3: Compute $s_i = \lfloor \log_2 w_j \rfloor$, and $k_i = \lfloor \log_2 s_i^2 \rfloor$.
Step 4: Read the next k_i secret bits from the binary secret data and convert them into the decimal number m_i in s_i^2-ary system.
Step 5: Compute

$$F(x_{2i}, x_{2i+1}) = [x_{2i} \times (s_i - 1) + x_{2i+1} \times s_i] \mod s_i^2. \tag{4}$$

Step 6: If $m_i = F$ (x_{2i}, x_{2i+1}), then

$$(x'_{2i}, x'_{2i+1}) = (x_{2i}, x_{2i+1}). \tag{5}$$

Otherwise,

Case 1: If $m_i > F$ (x_{2i}, x_{2i+1}), then

$$x'_{2i} = x_{2i} - [m_i - F(x_{2i}, x_{2i+1})] \mod s_i. \tag{6}$$

$$x'_{2i+1} = x_{2i+1} + \left\lfloor \frac{m_i - F(x_{2i}, x_{2i+1})}{s_i} \right\rfloor + \left[m_i - F(x_{2i}, x_{2i+1})\right] \mod s_i. \tag{7}$$

Case 2: If $m_i < F$ (x_{2i}, x_{2i+1}), then

$$x'_{2i} = x_{2i} + [F(x_{2i}, x_{2i+1}) - m_i] \mod s_i. \tag{8}$$

$$x'_{2i+1} = x_{2i+1} - \left\lfloor \frac{F(x_{2i}, x_{2i+1}) - m_i}{s_i} \right\rfloor - \left[F(x_{2i}, x_{2i+1}) - m_i\right] \mod s_i. \tag{9}$$

If d_i and $d'_i(d'_i = \left|x'_{2i+1} - x'_{2i}\right|)$ are not belong to the same range w_j, we select from candidate pixel pair to produce the embedded pixel pair. The selection criterion is to choose(x^*_{2i}, x^*_{2i+1}) from one of six candidate pixel pairs $\{(x'_{2i} - 3s_i, x'_{2i+1} - 3), (x'_{2i} - 2s_i, x'_{2i+1} - 2), (x'_{2i} - s_i, x'_{2i+1} - 1), (x'_{2i} + s_i, x'_{2i+1} + 1), (x'_{2i} + 2s_i, x'_{2i+1} + 2), (x'_{2i} + 3s_i, x'_{2i+1} + 3)\}$ such that the final embedded pixel pair (x^*_{2i}, x^*_{2i+1}) has meet the condition which the pixel difference before and after embedding are belong to the same range w_j.

When the digit m_i is embedded into a pixel pair (x_{2i}, x_{2i+1}), using the proposed method, the pixel pair (x_{2i}, x_{2i+1}) is modified to (x^*_{2i}, x^*_{2i+1}). If x^*_{2i} or x^*_{2i+1} are not within the range [0, 255], the overflow or underflow problem occurs. To solve the problem, we find an alternative pixel pair($\overline{x}_{2i}$, $\overline{x}_{2i+1}$) that is the nearest to (x_{2i}, x_{2i+1}) and meets all the requirements for data extraction. ($\overline{x}_{2i}$, $\overline{x}_{2i+1}$) can be obtained by solving the unknowns (x, y) in the optimization problem listed below:

$$\text{Minimize}: (x_{2i} - x)^2 + (x_{2i+1} - y)^2;$$

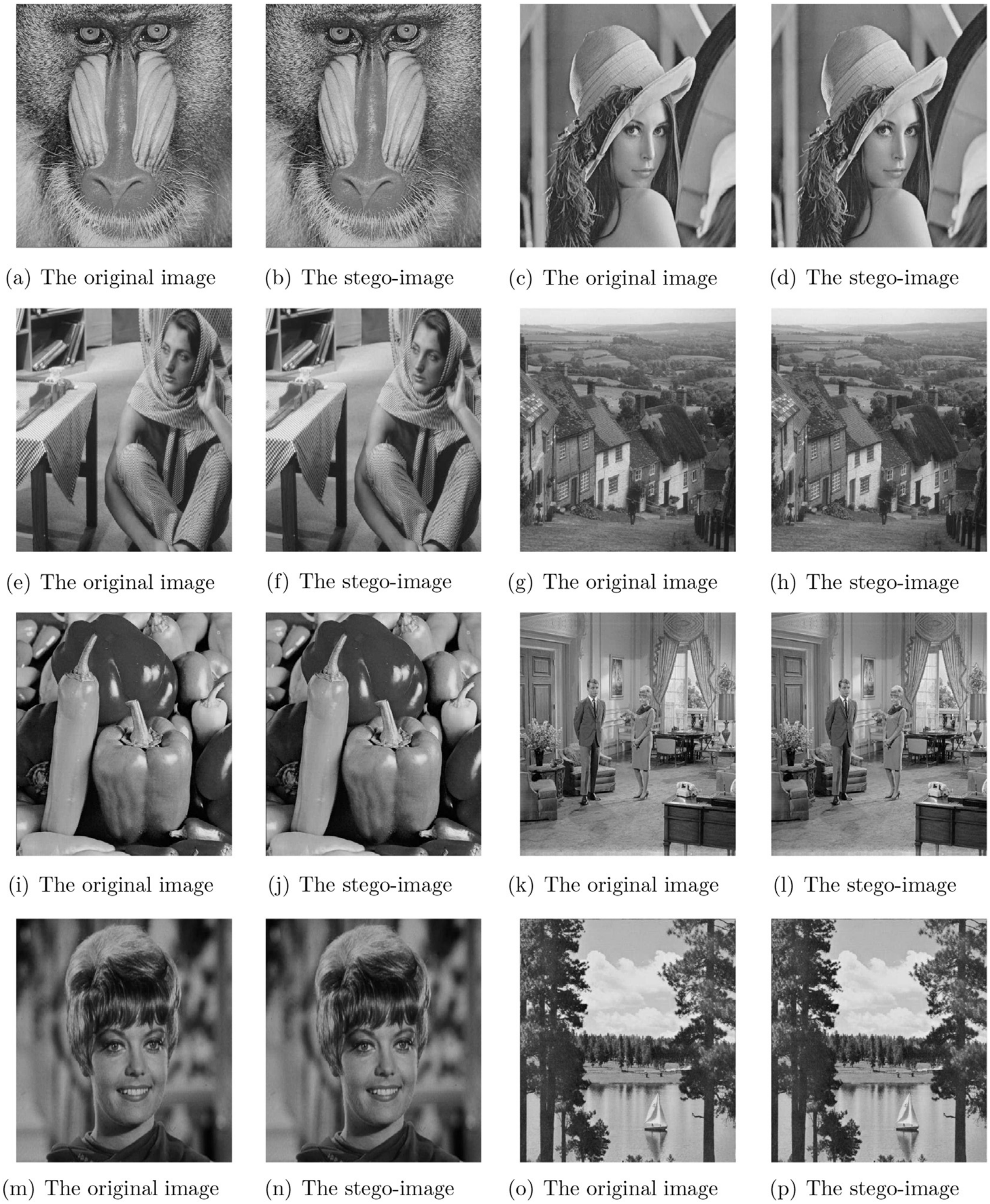
$$\text{Subject to}: F(x, y) = m_i, \ D(d_i) = D\left(\overline{d}_i\right).$$

Where $d_i = |x_{2i+1} - x_{2i}|$, $\overline{d}_i = \left|x - y\right|$ and D (d_i) is the division where the absolute difference d_i belong to. The optimization problem ensure that the value of $F((\overline{x}_{2i}, \overline{x}_{2i+1}))$ is m_i, the same division is maintained before and after data embedding, and ($\overline{x}_{2i}$, $\overline{x}_{2i+1}$) is in the range [0, 255], respectively.

3.2. The data extraction

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs, and the detailed steps are listed below:

Step 1: Do exactly the same things as Step 1 in data embedding, pixel blocks (x^*_{2i}, x^*_{2i+1}), $i \in \{1, 2, \cdots, L\}$ is obtained.



(a) The original image (b) The stego-image (c) The original image (d) The stego-image

(e) The original image (f) The stego-image (g) The original image (h) The stego-image

(i) The original image (j) The stego-image (k) The original image (l) The stego-image

(m) The original image (n) The stego-image (o) The original image (p) The stego-image

Fig. 1 – The eight test images.

Step 2: Calculate

$$d_i^* = |x_{2i+1}^* - x_{2i}^*|. \tag{10}$$

Step 3: From the w_j division, find out the range which d_i^* belong to, then calculate $s_i^* = \lfloor log_2 w_j \rfloor$, $k_i^* = \left\lfloor log_2 (s_i^*)^2 \right\rfloor$.

Step 4: Calculate

$$m_i^* = F(x_{2i}^*, x_{2i+1}^*) = [x_{2i}^* \times (s_i^* - 1) + x_{2i+1}^* \times s_i^*] \mod s_i^2. \tag{11}$$

The result is the embedded digit.

Step 5: Repeat Step 2–4 until all the message digits are extracted.

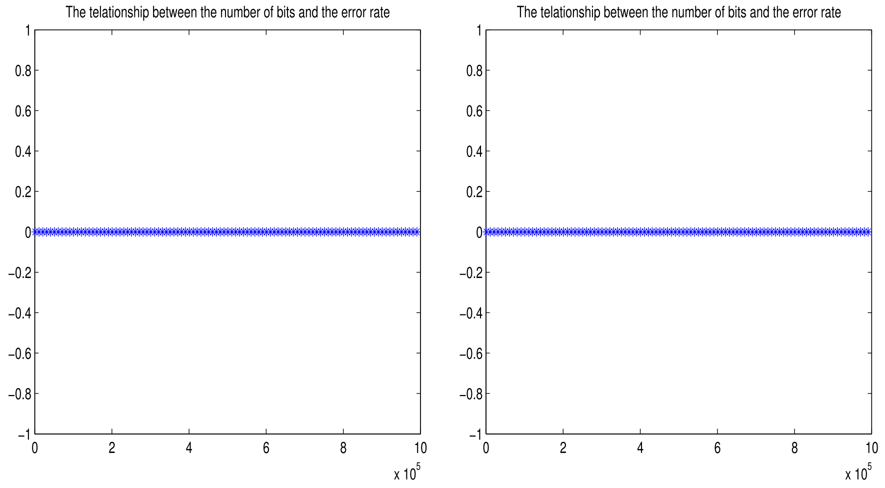
Step 6: Finally, the message bits S can obtained by converting the extracted message digits into a binary bit stream.

4. The example

4.1. *The example of the embedding process*

Assume $(x_{2i}, x_{2i+1}) = (3, 243)$, by the embedding Step 2, then

$d_i = |x_{2i+1} - x_{2i}| = |243 - 3| = 240 \in [128, \ 255]$.



(q) Pepper (r) Lena

Fig. 2 – The error rate and the number of bits of the experiment results.

So, $s_i = \lfloor \log_2 w_j \rfloor = \lfloor \log_2 128 \rfloor = 7$, and $k_i = \lfloor \log_2 s_i^2 \rfloor = \lfloor \log_2 7^2 \rfloor = 5$. Assume a five-bit of binary secret message is $m_i = (11110)_2 = (30)_{49}$, and using the Eq. (4) to compute

$$\begin{aligned} F(x_{2i}, x_{2i+1}) &= [x_{2i} \times (s_i - 1) + x_{2i+1} \times s_i] \mod s_i^2 \\ &= [3 \times 6 + 243 \times 7] \mod 49 = 4. \end{aligned}$$

Because $m_i > F\,(x_{2i}, x_{2i+1})$, according to the Eq. (6), we obtain

$$\begin{aligned} x'_{2i} &= x_{2i} - [m_i - F(x_{2i}, x_{2i+1})] \mod s_i = 3 - [30 - 4] \mod 7 \\ &= -2. \end{aligned}$$

$$\begin{aligned} x'_{2i+1} &= x_{2i+1} + \left\lfloor \frac{m_i - F(x_{2i}, x_{2i+1})}{s_i} \right\rfloor + [m_i - F(x_{2i}, x_{2i+1})] \mod s_i \\ &= 243 + \left\lfloor \frac{30 - 4}{7} \right\rfloor + \left(30 - 4\right) \mod 7 = 251. \end{aligned}$$

Because $x'_{2i} = -2 < 0$, by using the optimization problem, we have $(x^*_{2i}, x^*_{2i+1}) = (5, 252)$. Thus the data bits are embedded, the pixel units (3, 243) are modified to (5, 252).

4.2. The example of the extraction process

When we want to extract digits from the unit (5, 252), we first get the value of difference $d_i^* = |x^*_{2i+1} - x^*_{2i}| = |252 - 5| = 247 \in [128, 255]$. And we calculate $s_i^* = \lfloor \log_2 w_j \rfloor = \lfloor \log_2 128 \rfloor = 7$, and $k_i^* = \left\lfloor \log_2 (s_i^*)^2 \right\rfloor = \lfloor \log_2 7^2 \rfloor = 5$. The scheme exploits the Eq. (11).

$$\begin{aligned} m_i^* = F(x^*_{2i}, x^*_{2i+1}) &= [x^*_{2i} \times (s_i^* - 1) + x^*_{2i+1} \times s_i^*] \mod (s_i^*)^2 \\ &= \left[5 \times 6 + 252 \times 7\right] \mod 49 = 30. \end{aligned}$$

Convert 30 into its binary form, we obtain the message bits $(11110)_2$.

5. Experimental results and discussions

This section will investigate the performance of the proposed the data hiding method with experiments and will display some experimental results to demonstrate the visual quality and embedding capacity of our proposed method. The six standard gray images ("Lena", "Pepper", "Baboon", "House", "Sailboat", and so on), each of 512 × 512 pixel, are used in the experiment as depicted and the resulted cover images are show in Fig. 1. The embedded secret data is comprised of a random bit-stream that is generated from a random number generator beforehand. The operating system is Windows 7 Professional and our algorithms are programmed by Matlab 2013a. In order to compare visual quality between the cover image and the original image, a modified peak signal-to-noise ratio (PSNR), is defined in Eq. (12).

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}. \tag{12}$$

and the mean square error (MSE) for a $m \times n$ grayscale image is defined in Eq. (13).

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(A_{ij} - A'_{ij}\right)^2. \tag{13}$$

where m and n are the dimensions of the images, and A_{ij} and A'_{ij} are the pixel values of the cover image and stego-image, respectively. In principle, a lower value for MSE means less error, and as considered in Eq. (12), the inverse relationship between the MSE and PSNR translates to a high value of PSNR. Logically, a higher value of PSNR is good and signifies that the ratio of signal-to-noise is higher. In this representation, the "signal" is the original image, and the "noise" is the error in reconstruction. Therefore, the lower the MSE (and the higher the PSNR), the better the visual quality of the image.

Fig. 1 displays the experimental results of the original image and the cover image from the above experiment. Fig. 1(a, c, e, g, i, k, m, o) are the original images, Fig. 1(b, d, f, h, j, l, n, p) are the cover image. The experiment results show that our proposed method does not reduce the visual quality of the cover image when the secret bits are concealed. It can be seen that the images distortion can not be distinguished by human eyes.

Table 1 – The experiment result in our proposed method.

Image	PSNR	Capacity	Error	Overflow/underflow
Baboon	38.8831	443,472	0	53
Lena	42.4607	402,485	0	0
Barbara	40.1509	425,340	0	6
Boat	41.6081	408,777	0	2
Elaine	42.9876	398,250	0	0
Goldhill	41.8063	405,956	0	0
House	41.1631	412,354	0	3
Sailboat	41.2921	411,306	0	0
Toys	42.5201	402,011	0	0
Zelda	43.4371	396,553	0	0

With the cover image being the two in Fig. 1 and Fig. 2(a and b) indicate the relationship between the number of embedding secret bits and the extraction error rates. Furthermore, Fig. 2(a and b) show our scheme can keep the error rate of extraction secret bits is zero. Experiment results also prove that our algorithm is accurate extraction of secret bits.

In Table 1, the column labeled “capacity” is the number of bits can be embedded into the host-image, the column labeled “PSNR” is the peak-signal-to-noise- ratio of the cover image, the column labeled “error” is the number of bits in the extract error and the column labeled “overflow/underflow” is the total number of pixel value falling into the range [0.255] after embedded the secret data into the pixel. Table 1 summarizes the experimental results of the proposed algorithm. As we can see that the secret data are completely extracted from the cover image through the experiment results. And when the secret data is embedded into the cover image, the number of pixel is most belong to the range [0.255].

From Table 2, we clearly see that our approach has PSNR value about −0.02 db ~ 4.59 db, 1.92 ~ 5.97 db higher than Wu and Tsai's method, Yang and Weng et al.'s method, respectively. However, the hiding capacity has slightly dropped. In the same partition of range, higher PSNR value of our approach means that our scheme take account into human visual system and keep high quality of image.

In Table 3, it can be observed that the EMD concealed an equal amount of data into each pixel without causing visual artifacts to an observer. However, the tolerance of the changes to pixel values is different in smooth and edge areas according to human visual system (HVS). Based on the fact that edge areas can tolerate more severe changes than smooth areas, we conceal more data in edge areas to acquire more embedding capacity whereas conceal less data in smooth area to preserve the visual quality.

The approach outperforms previous approaches in terms of capacity, but maintains the high PSNR value, as seen in Table 4.

The PSNR is the most common used method to estimate the image quality. We can clearly know that if the cover image after embedding will be easily detected by human's eyes or not. However, we can not figure out the difference between the original image and the cover image accurately. Therefore, we will adopt the method proposed by Wang and Bovik (2002) in 2002 to compute the difference between two images except for the above experiment. The formula is as the following

$$Q = \frac{4\sigma_{xy}\bar{x} \times \bar{y}}{\left(\sigma_x^2 + \sigma_y^2\right)\left[\bar{x}^2 + \bar{y}^2\right]}. \tag{14}$$

In the formula, $\bar{x}$, $\bar{y}$ are the average value of the original grayscale image and the stego-image, respectively. The formula for $\bar{x}$, $\bar{y}$ are defined as the following

$$\bar{x} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} A_{ij}. \tag{15}$$

$$\bar{y} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} A'_{ij}. \tag{16}$$

$$\sigma_x^2 = \frac{1}{m \times n - 1}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij} - \bar{x}\right)^2, \tag{17}$$

$$\sigma_y^2 = \frac{1}{m \times n - 1}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A'_{ij} - \bar{y}\right)^2 \tag{18}$$

$$\sigma_{xy} = \frac{1}{m \times n - 1}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij} - \bar{x}\right)\left(A'_{ij} - \bar{y}\right). \tag{19}$$

The Q range proposed by Wang and Bovik is from −1 to 1. The more it is close to 1, the qualities of two images are more similar. In Table 5, we can find that the Q values by using our proposed method are much close to 1. Therefore, we can say that the image before and after embedding in this paper is very similar and its image quality is good. According to Table 5, our scheme has a higher capacity and maintains unnoticeable distortion of the image in each experiment. Table 6 indicates the fact that the proposed method provides superior perceptual invisibility than Chang et al.'s method and Lu et al.'s scheme.

Table 2 – Comparisons of other method and our proposed.

Cover image	Wu and Tsai method (Wu and Tsai, 2003)		Yang and Weng et al.'s method (Yang et al., 2011)		Our method	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	406,632	41.71	410,854	40.54	402,485	42.46
Baboon	437,806	38.90	482,515	34.67	443,472	38.88
Pepper	401,982	41.07	408,281	40.47	401,088	42.68
Toys	406,656	39.93	418,948	38.55	402,011	44.52
Sailboat	415,554	40.67	430,888	38.11	411,306	41.29

Table 3 – Comparisons of the proposed and EMD.

Cover image	Zhang and Wang's (EMD)		Our method	
	Capacity	PSNR	Capacity	PSNR
Lena	364,544	51.80	402,485	42.46
F16	365,000	51.79	404,945	42.17
Peppers	365,624	51.81	401,088	42.68
Baboon	364,408	51.80	443,472	38.88

6. Analysis and discussions

6.1. *Saturation and security at pixels*

In the past EMD embedding scheme, the critical *f* is operated under a modulo number of $2n + 1$ different varieties are accommodated. Similarly, in the Kieu and Chang's scheme, the critical *f* is operated under a modulo number of s^2. They have a common character which have a same value of *n* (or *s*) in the whole original image in the embedding process. By contrast, the modulo is by the number s_i^2 in our scheme, it was decided by the pixel-value difference, in other word, different pixel-value difference have different values of s_i. In addition, it therefore offers more accommodations than EMD and Kieu et al.'s method to the embedding secret to conduct the capacity-promoting for higher capacity required in information hiding studies. Since the value of s_i^2 is random rather than a fixed value in the whole image, our proposed is more secure than them. Additionally, in EMD method, to deal with the underflow or overflow problem, they change the saturated-pixel by one and run the embedding scheme again until the non saturated-pixel occurs. In our scheme, by using the six candidate pixel pairs decreases the number of the saturated-pixel and exploits the optimization problem to the rest of the pixel value encountering the condition of underflow or overflow among [0, 255].

6.2. *RS analysis*

In this section, to check whether the function of the proposed embedding method can be detected with some newly announced related statistical data hiding techniques, we tested the cover images yielded by our method with the dual statistics method proposed by Fridrich et al. (2001) as a demonstration. By the method, all the pixels of a cover 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 cover image will pass the RS statistical analysis when $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$. Otherwise, the cover image will be judged as a suspicious object. The detection results our scheme gave (with the cover image being the one in Fig. 1) are shown in Fig. 3, where the *x*-axis represents the percentage of hiding capacity and the *y*-axis represents the percentage of the regular and singular pixel groups with masks $m = [0110]$ and $-m = [0 - 1 - 10]$. Such diagrams are referred to as RS-diagrams. According to Fridrich et al., if more and more LSBs are replaced with random data, then the percentages R_m and S_m of the two pixel groups (regular and singular, respectively) in the diagram will become equal gradually when the mask of *m* is adopted in the statistics analysis process, or the percentages R_{-m} and S_{-m} will become more and more unequal when the mask of *m* is adopted. From the RS-diagram of Fig. 3(a and c), we can see that the function of conventional LSB-embedding techniques in images indeed can be detected because when the percentage of pixels embedded with data into their LSBs approaches 100%, the percentages of the regular and singular pixel groups will become more and more equal or unequal. But Fig. 3(b and d) indicate that the cover images seemingly do not contain any embedded data in their LSBs, because the expected value of R_m is seen close to that of R_{-m} and so are the case of S_m and S_{-m}, i.e., $R_m \cong R_{-m}$. and $S_m \cong S_{-m}$. Accordingly, we can make a solid statement that the proposed scheme is secure against the RS detection attack.

6.3. *PVD histogram analysis*

PVD histogram may be a potential characteristic to expose the hidden message of those stegos using the PVD based steganographic methods. In (Zhang and Wang, 2004), Zhang and Wang showed that the original PVD scheme (Yang et al., 2008) will inevitably introduce some undesired steps in the histogram of the differences between two continuous pixels in each embedding unit due to its fixed division of embedding units and its fixed quantization steps. By detecting and analyzing such artifacts, it is possible to estimate the size of hidden message especially when the embedding rate is high.

Fig. 4 shows the PVD histograms of some original image and their corresponding stegos using our proposed method with the maximum embedding capacity, respectively. Fig. 4(a and b) are one plane of Lena and Goldhill. It is observed that the PVD histograms can be well preserved after data hiding.

7. Conclusions and future work

In this paper, we propose a steganographic scheme to improve the hiding capacity of Zhang and Wang's method and conceals

Table 4 – Comparisons of other methods and our proposed.

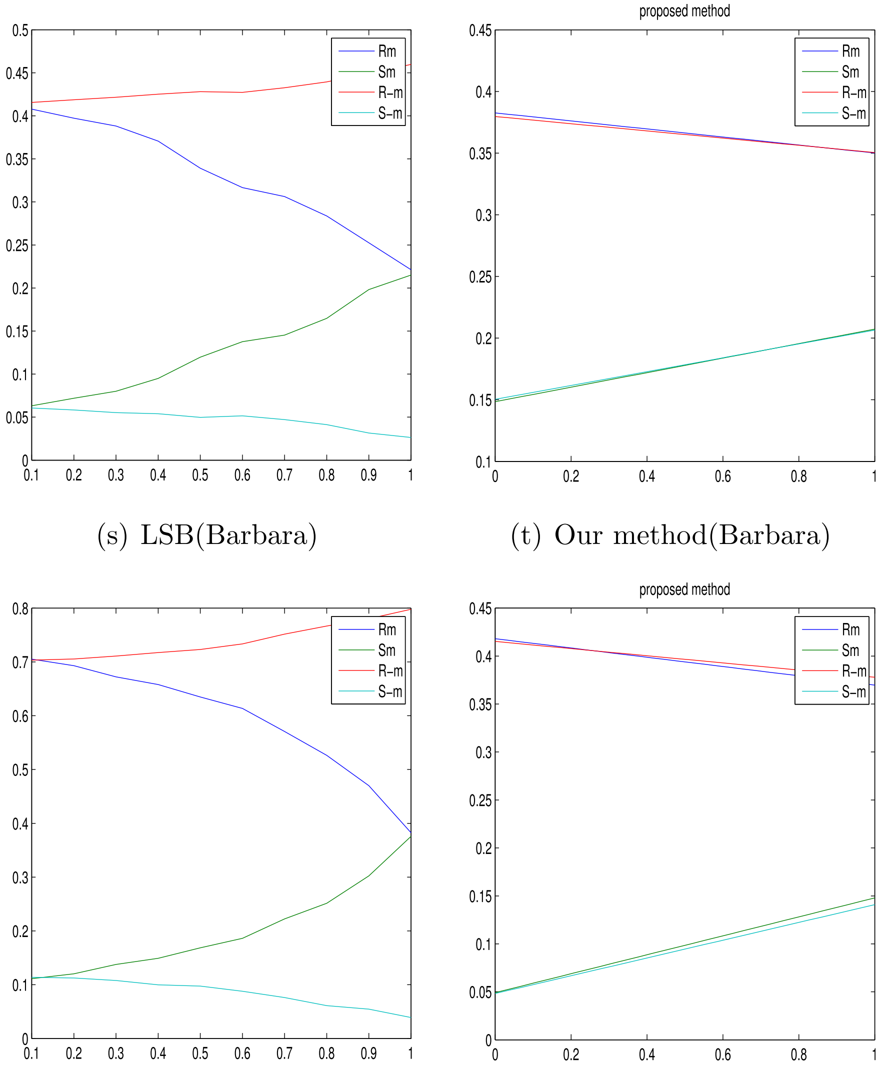
Cover image	Lin's method (Lin, 2012)		Wu et al. (Wu et al., 2014)		Suresh et al. (Mali et al., 2012)		Our method	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	152,389	36.44	335,254	36.22	14,357	41.72	402,485	42.46
baboon	66,437	34.90	269,891	31.46	40,075	39.67	443,472	38.88
sailboat	126,863	35.90	436,453	36.91	21,063	41.08	411,306	41.29

Table 5 – Estimate the difference by using Wang and Bovik's scheme.

Image	Baboon	Lena	Barbara	Boat	Bridge	Couple	Elaine
Q	0.9977	0.9992	0.9989	0.9992	0.9988	0.9988	0.9992
Image	Goldhill	House	Man	Pepper	Sailboat	Toys	Zelda
Q	0.9991	0.9989	0.9993	0.9995	0.9994	0.9989	0.9991

Table 6 – Comparisons Q value of other method and our proposed.

Cover image	Chang et al.'s (Chang and Lu, 2006)		Lu et al.'s ($\|B\| = 4$ (Lu et al., 2014))		Lu et al.'s ($\|B\| = 8$ (Lu et al., 2014))		Our method
	Q ($T = 15$)	Q ($T = 42$)	Q ($T = 3$)	Q ($T = 18$)	Q ($T = 3$)	Q ($T = 18$)	Q
Lena	0.9951	0.9914	0.9978	0.9943	0.9934	0.9910	0.9992
Baboon	0.9913	0.9297	0.9955	0.9807	0.9858	0.9768	0.9977
Pepper	0.9960	0.9892	0.9983	0.9963	0.9951	0.9938	0.9995
F16	0.9948	0.9815	0.9971	0.9923	0.9914	0.9863	0.9990



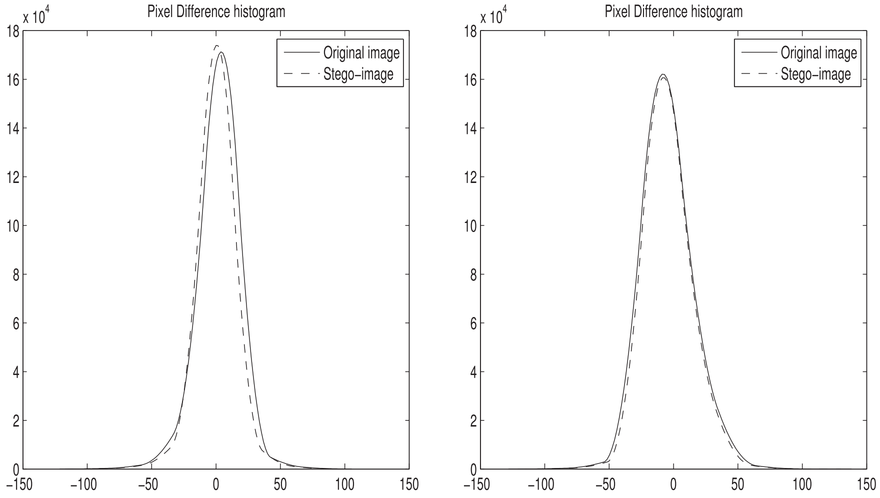
(s) LSB(Barbara)

(t) Our method(Barbara)

(u) LSB(Zelda)

(v) Our method(Zelda)

Fig. 3 – RS-diagrams yielded by the dual statistics method by Fridrich et al. for cover images produced by conventional LSB-embedding technique and our method.



(w) Lena (x) Goldhill

Fig. 4 – PVD histogram differences between covers and theirs corresponding stegos.

digits in any-ary notation adaptively according to the absolute difference of pixel pairs. In order to preserve the contents of the cover image better, we employ Hilbert filling curve to create 1D pixels sequence. The contributions of the proposed method are summarized as follows. Firstly, the original EMD method considers no image characteristic and embeds digits in the same base into the whole cover image; therefore, each pixel pair embeds equal amount of data. The proposed method modified the EMD method so that the digits in any bases can be embedded according to the local complexity of the cover image. Secondly, the proposed method reduces the detectable artifacts caused by the readjusting phase for overflow, underflow or falling-off boundary problem, which are serious in other PVD method. Third, our method does not require any memory space whereas Kier-Chang scheme requires about 524Kbytes (256 × 256 × 8 = 524.288 Kb) to store the embedding matrix, because they use the search matrix method to finish embedding the secret data. Finally, Our scheme is able to resist the RS detection attack and the steganalytic histogram attack of pixel-value difference, and our method is more secure than PVD in both resisting statistical analysis. In conclusion, our scheme takes advantage of among pixel value-differencing, EMD and Kieu-Chang's method enabling it to produce an embedded image with significantly low distortion. Thus we can conclude that the proposed method has some merits and is applicable to steganographic application such as privacy protection of information transmission which requires high confidentiality and large embedding capacity.

Acknowledgments

This work was supported by the Natural Science Foundation of P.R.China (11371127, 11101164) and Natural Science Foundation of Guangdong (S2011040003243).

REFERENCES

Chang CC, Kieu TD, Chou YC. A lossless data embedding technique by joint neighboring coding. Pattern Recognit 2009;42(7):1597–603.

Chang CC, Kieu TD, Chou YC. Reversible information hiding for VQ indices based on locally adaptive coding. J Vis Commun Image Represent 2009a;20(1):57–64.

Chang CC, Lu TC. A difference expansion oriented data hiding scheme for restoring the original host image. J Syst Softw 2006;79:1754–66.

Chang CC, Tai WL, Lin CC. A reversible data hiding scheme based on side match vector quantization. IEEE Trans Circuits Syst Video Technol 2006;16(10):1301–8.

Chao RM, Wu HC, Le CC, Chu YP. A novel image data hiding scheme with diamond encoding. EURASIP J Inf Secur 2009:1–9.

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

Fridrich J, Goljian M, Soukal D. Wet paper codes with improved embedding efficiency. IEEE Trans Inf Forensics Secur 2006;1(1):102–10.

Fridrich J, Lisonek P, Soukal D. On steganographic embedding efficiency. In: Proceedings of 8th international workshop on information hiding; 2007. p. 282–96. LNCS4437.

Hong W. Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique. Inf Sci 2012;221:473–89.

Hong W, Chen TS. A novel data embedding method using adaptive pixel pair matching. IEEE Trans Inf Forensics Secur 2012;7(1):176–84.

Kazem G, Shahrokh G, Saeed RK. LSB^{++}: an improvement to LSB^{+} steganography. In: TENCON 2011–2011 IEEE Region 10 Conference. IEEE; 2011. p. 364–8.

Kieu TD, Chang CC. A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 2011;38:10648–57.

Lan TH, Tewfik AH. A novel high-capacity data-embedding system. IEEE Trans Image Process 2006;15(8):2431–40.

Langelaar G, Setyawan I, Lagedijk R. Watermarking digital image and video data: a state-of-the-art overview. IEEE Signal Process Mag 2000;17(5):20–46.

Lee YP. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inf Sci 2012;191:214–25.

Lee S, Yoo CD, Kalker T. Reversible image watermarking based on integer-to integer wavelet transform. IEEE Trans Inf Forensics Secur 2007;2(3):321–30.

Lin YK. High capacity reversible data hiding scheme based upon discrete cosine transformation. J Syst Softw 2012;85:2395–404.

Lu TC, Chang CC, Huang YH. High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting. Multimed Tools Appl 2014;71(1):417–35.

Luo, Huang, Huang. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans Inf Forensics Secur 2010;5(2):201–14.

Mali SN, Patrl PM, Jalnekar RM. Robust and secured image-adaptive data hiding. Digit Signal Process 2012;22:314–23.

Mielikainen J. LSB matching revisited. IEEE Signal Process Lett 2006;13(5):285–7.

Ni Z, Shi Y, Ansari N, Su W. Reversible data hiding. IEEE Trans Circuits Syst Video Technol 2006;16(3):354–62.

Ni Z, Shi Y, Ansari N, Su W, Sun Q, Lin X. Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans Circuits Syst Video Technol 2008;18(4):497–509.

Qazanfari K, Safabakhsh R. Adaptive method for hiding data in images. J Electron Imaging 2012;21(1):3022.

Qazanfari K, Safabakhsh R. High-capacity method for hiding data in the discrete cosine transform domain. J Electron Imaging 2013;22(4):043009.

Qazanfari K, Safabakhsh R. A new steganography method which preserves histogram: generalization of LSB^{++}. Inf Sci 2014;277:90–101.

Qin C, Chang CC, Hsu TJ. Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimed Tools Appl 2014.

Tan SQ, Li B. Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting. IEEE Signal Process Lett 2012;19(6):336–9.

Wang Z, Bovik AC. A universal image quality index. IEEE Signal Process Lett 2002;9(3):81–4.

Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganographic method with pixel-value differencing and modulus function. J Syst Softw 2008;81(1):150–8.

Westfeld A. F5-A steganographic algorithm. In: proceedings of 4th international workshop on information hiding; 2001. p. 289–302. LNCS2137.

Westfeld A. Space filling curves in steganalysis. In: Proceedings of SPIE: Security, Steganography and Watermarking for Multimedia. San Jose, California: SPIE; 2005. p. 28–37.

Wu DC. A data mapping method for steganography and its application to images. In: 10th International Workshop on Information Hiding, vol. 5284; 2008. p. 236–50.

Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recognit Lett 2003;24:1613–26.

Wu HZ, Wang HX, Zhao H, Yu XY. Multi-layer assignment steganography using graphy-theoretic approach. Multimed Tools Appl 2014.

Yang CH, Wang CY, Sun HM. Information hiding technique based on blocked PVD. J Inf Manag 2008;15(3):29–48.

Yang CH, Weng CY, Tso HK, Wang SJ. A data hiding scheme using the varieties of pixel-value differencing in multimedia images. J Syst Softw 2011;84:669–78.

Zhang XP, Wang SZ. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit Lett 2004:331–9.

Zhang XP, Wang SZ. Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 2006;10(11):781–3.

Shu-Yuan Shen received her M.S degree in Applied Mathematics in School of Mathematical Sciences from South China Normal University, Guangzhou, China, in 2005. She is currently pursuing the PH.D. degree in Applied Mathematics and computer science at the college of Mathematics and Econometrics, Hunan University, Changsha, China. Since July 2005, she has been in South China Normal University, Guangzhou, China. Her research interests include differential equation, data hiding, image processing and neural network.

Li-Hong Huang received the M.S. degree and the Ph.D. degree in Applied Mathematics from Hunan University, Changsha, China, in 1988 and 1994, respectively. In June 1997 he became Doctoral Advisor of Applied Mathematics and Chair of the Department of Applied Mathematics. From July 2000 to July 2010 he was Dean of the college of Mathematics and Econometrics at Hunan University, Changsha, China. Since July2010 he has been vice president of Hunan Women's University, Changsha, China. He is the author or coauthor of more than 300 journal papers, ten edited books. His research interests are in the areas of qualitative theory of differential and difference equations.