Secure Image Hiding Scheme Based on Magic Signet
Chin-Feng Lee and Ying-Xiang Wang


View online: https://doi.org/10.11989/JEST.1674-862X.80206200

Articles you may be interested in


Follow JEST WeChat public account for more information
Secure Image Hiding Scheme Based on Magic Signet

Chin-Feng Lee* | Ying-Xiang Wang

Abstract—Image data hiding technology is secret communications that carry hidden data in such a way that no one except the sender and intended recipients can even realize there is a hidden message. High embedding capacity, good images quality, and security are three important essentials. In this paper, each confidential hexadecimal will be carried by two cover pixels based on a magic matrix generated from a square template to reach the goal of higher embedding capacity while keeping good image visualization. Experimental results reveal that the proposed scheme guarantees higher embedding capacity of 2 bits per pixel and has the peak signal-to-noise ratio (PSNR) of 44.7 dB on average. Moreover, secret keys are used to ensure security consideration.

Index Terms—Data hiding, embedding capacity, steganography, visual quality.

1. Introduction

People have been unable to leave the Internet now. Therefore, how to enhance information security has become an important issue at present. Steganography is an art of secret communication in an appropriate carrier. Image hiding technology is a particular subject of steganography. The secret information is accommodated in an original image (also called a cover image) based on a secure key, becoming a stego-image. Therefore, the image hiding technology can carry out message exchanges. A successful image hiding technique is required to reach the need of security, embedding capacity, and image visual quality.

Here, we mentioned the irreversible information hiding method. The irreversible advantage lies in the simple method, high possession, and wide applications. In 1989, Turner et al.[1] published the least significant bit (LSB) method. This method hides the confidential information bits one by one into the cover image. If the confidential information is different from the original image pixels, then the confidential information will directly replace the original image to obtain the stego-image. In 2006, Mielikainen[2] proposed an improved LSB matching method, which uses a pair of two pixel values and hides two confidential information bits at a time. Firstly, it determines if LSB of the first pixel value is equal to the hidden confidentiality bit. When the two are different, then it uses a binary function to select the pixel value to be modified. In 2004, Chan and Cheng[3] proposed a data hiding method by

*Corresponding author
Manuscript received 2018-02-06; revised 2018-05-07.
C.-F. Lee and Y.-X. Wang are with the Department of Information Management, Chaoyang University of Technology, Taichung 41349 (e-mail: lcf@cyut.edu.tw).
Color versions of one or more of the figures in this paper are available online at http://www.journal.uestc.edu.cn.
Publishing editor: Xin Huang
simple LSB substitution with an optimal pixel adjustment process (OPAP). This method can use the low additional calculation to enhance image quality.

In 2006, Zhang and Wang [4] proposed the method based on exploiting modification direction (EMD). The EMD method can hide each 5-ary data in two original pixels, where at most only one pixel increases or decreases the value to achieve high image quality. In 2013, a generalized EMD (GEMD) method was proposed by Kuo and Wang [5], which uses \( n \) cover-pixels in a group, and is able to embed \((n+1)\) bits of secret data. In 2010, Lee and Chen [6] developed a modulus function to maintain the image quality good and provide the hiding capacity, while reducing the memory requirements.

In 2003, Wu and Tsai [7] proposed the pixel value different (PVD) method. The PVD method calculates the difference between a pair of consecutive pixels. The difference between the pair of pixels is compared with the predefined interval widths to determine the amount of bits. In 2014, Chen [8] enhanced the improved modulus function for the PVD (IMF-PVD) hiding method. The amount of confidential information to be hidden in this method depends on the complexity of each hidden block. The number of bits hidden in the complex area is more, but the smooth area is less. The human eyes are less sensitive to changes in complex areas than smooth areas. Its purpose is to improve image quality by hiding more data and to protect the hidden information. In 2015, Shen and Huang [9] proposed a method that combines PVD and EMD. This method will first use the Hilbert curve to convert the original image into a one-dimensional pixel stream, and then divide the two consecutive pixels into non-overlapping hidden blocks. PVD is applied to estimate the cardinality of the number of bits and hides it in pixel pairs.

Chang et al. [10] introduced a data hiding scheme based on the Sudoku solution to hide secret data. Although the Sudoku scheme has less calculation, it owns lower image quality. In 2014, Chang et al. [11] proposed a turtle-shaped shell scheme with the high image quality of 53.3 dB on average. Both schemes can reach the embedding capacity of 1.5 bits per pixel (bpp). In 2015, Kurup et al. [12] proposed the octagon shape shell. This method has an octagonal shape that contains 16 different numbers. The reference matrix modifies the value of the overlay pixel pair, thereby hiding confidential information. In 2016, Liu et al. [13] increased the embedding capacity by using the location table to develop the turtle shell-based scheme to reach 2 bits per pixel on average. Jin et al. [14] minimized the turtle shell matrix based stego-image distortion using particle swarm optimization. Xie et al. [15] developed an approach based on a two-layer turtle shell matrix to enhance the embedding capacity.

To enhance the embedding capacity with an indistinguishable form, a square template is generated. This scheme is the extension of the pencil-shaped pattern embedding scheme [16]. Our scheme first designs a magic matrix with each dimension of the range from 0 to 255, and then adjusts pixel values according to the position where the data can be located on the magic matrix so that each cover pixel pair can carry a nibble, reaching the high embedding capacity of 2 bpp.

The rest of this paper is as follows. Section 2 gives a simple literature review. Section 3 describes the proposed scheme in detail. The experimental results and conclusions are discussed in Sections 4 and 5, respectively.

2. Related Work

In this section, a hiding scheme based on turtle-shaped shells developed by Chang et al. [11] is introduced. Assume that the secret message is expressed in binary. Each time three bits of secret data can be hidden within two pixels. Fig. 1 (a) shows an example of a magic matrix \( M \) based on turtle-shaped shells with a size of 256×256. Two adjacent elements in the same row of matrix \( M \) have a difference of 1; two adjacent elements of the same column have alternatively difference of 2 or 3, respectively. Let \( M(p_i, p_{i+1}) \) and \( M(q_i, q_{i+1}) \) be the numbers in the magic matrix \( M \) where \((p_i, p_{i+1})\) and \((q_i, q_{i+1})\) represent the pairs of cover pixels and stego-pixels before/after the 3-bit secret data \( s \) has been concealed.
Fig. 1. Magic matrix $\mathbf{M}$ based on turtle-shaped shells: (a) magic matrix $\mathbf{M}$, (b) $M(4, 5)$ is located within a turtle-shaped shell, (c) $M(4, 4)$ is an edge number, and (d) $M(0, 1)$ is not located at any turtle-shaped shell.

Fig. 2. Example of Sudoku: (a) element $M(4, 3)=7$, (b) candidate elements in vertical Sudoku grids, (c) horizontal Sudoku grids, and (d) square Sudoku grids.

If the number $M(p, p_i)$ falls in one turtle-shaped shell as shown in Fig. 1 (b), then the secret number $s_i$ also can be found in the same turtle-shaped shell such that $s_i = M(q, q_i)$. However, if $M(p, p_i)$ is an edge number, then the number $s_i$ can be found in the surrounding three turtle shells as shown in Fig. 1 (c). The calculation should be performed to find the minimum distance between $(p, p_i)$ and $(q, q_i)$ under the condition that $s=M(q, q_i)$. Another special case occurs when the number $M(p, p_i)$ is not located at any turtle-shaped shell; the solution as shown in Fig. 1 (d) is to find the shortest distance between $(p, p_i)$ and $(q, q_i)$ so that the number $M(q, q_i)$ equals to the secret data $s_i$.

The turtle-shaped shell scheme is a great idea and the one that we can have no doubt to dig deep. However, the embedded capacity payload has some limitations. The following discussion is also based on the Sudoku-based hiding method proposed by Chang et al. In 1979, Gams invented Sudoku. A Sudoku box contains nine 3×3 sub-boxes, and each row and each column of the Sudoku grid contains 0 to 8 different numbers. When $M(p, p_i)=M(4, 3)$, the value in matrix $\mathbf{M}$ is 7 as shown in Fig. 2 (a). Next, we assume that the confidential information is (011 001), which can be converted into values of base-9. So (011 001)$_9=(2 7)$_9. At this point, we will learn that the values to be searched for in the matrix $\mathbf{M}$ are 2 and 7, respectively. Next, we will follow the three known candidate elements, as shown in Figs. 2 (b) to (d). After three candidate elements are finally obtained, the three candidate elements are compared, and the original pixel $M(p, p_i)$ can be modified to the candidate pixel $M(q, q_i)$ is found. The candidate element with the shortest-distance is our final decision (stego-pixel pair) to hide the secret data.

Another topic to be introduced is an octagonal information hiding method proposed by Kurup et al. In this octagon, 0 to 15 different numbers are included, 4 secret bits are found from the confidential information and correspond to 0 to 15 digits and then hidden. The first step is to generate a 256×256 reference matrix. This matrix has two rules. The difference between adjacent pixels in the same row is set to 1; the difference between two adjacent pixels in the same column is set to 4 or 5, and the reference matrix is connected with multiple octagons. The pixel is modified according to the three rules below.
Rule 1: if \( M(p_i, p_{i+1}) \) is a number that is located in an octagon, then \( M(q_i, q_{i+1}) \) is one of the digits in this octagon, as shown in Fig. 3 (a)).

Rule 2: If \( M(p_i, p_{i+1}) \) is an edge digit involved in at least one octagon, then \( M(q_i, q_{i+1}) \) is one of the digits in all octagons which are adjacent, as shown in Fig. 3 (b)).

Rule 3: If \( M(p_i, p_{i+1}) \) does not belong to any octagon, then \( M(q_i, q_{i+1}) \) is one of all digits in a 4×5 sub-block where \( M(q_i, q_{i+1}) \) is located in the central of the sub-block.

Recently, Lee et al.\(^{[16]}\) proposed an embedding scheme based on a pencil-shaped pattern for raising the embedding capacity while keeping good visual quality of the stego-image. Based on this magic matrix, each cover pixel pair can carry 4-bit secret data so the embedding capacity is 2 bit per pixel. Therefore, the embedding capacity when compared with previous schemes is the best. However, the pencil-shaped pattern scheme involves more image distortion up to 5 dB compared with the turtle-shaped shell scheme. Therefore, it inspires to propose a high fidelity steganography technique of two bpp embedding capacity.

3. Proposed Scheme

The proposed scheme has three procedures: Matrix construction, message embedding, and data extraction.

First, create a square template of \( N_1 \times N_2 \) digits, and adopt the template to build a magic matrix size is \( 256 \times 256 \). Before considering how to create the magic matrix based square template, we use Fig. 4 to illustrate how an entry in the magic matrix can be specified by a pair of numerical coordinates. Similar to the Cartesian coordinate system, the \( H \times W \) magic matrix \( \mathbf{M} \) is arranged as shown in Fig. 4, the individual element or entry is denoted by \( M(x, y) \) where \( H=\max x \) and \( W=\max y \), each element or entry is a number ranging from 0 to \( (H \times W - 1) \), and each element can be referenced by a coordinate \( (x, y) \). For example, \( M(x, y) = 8 \), if \( x=0 \); \( M(x, y) = 0 \), if \( x=4 \) and \( y=7 \), as shown in Fig. 4.

3.1. Matrix Construction Procedure

A two-dimensional magic matrix of size \( H \times W \) is constructed based on a template of size \( N_1 \times N_2 \). For greyscale images, the values \( H=W=256 \) and \( N_1=N_2=4 \). In the hexadecimal notational system, four bits (a nibble) are represented by a single digit. The template is square and is shown in Fig. 5 (a) which contains \( N_1 \times N_2 \) different digits from 0 to \( (N_1 \times N_2 - 1) \). The square template is like a signet which is affixed to the two-dimensional matrix in a non-overlapping manner so that the magic matrix can be created as shown in Fig. 5 (b).

3.2. Generated by Secure Key

A signet can be generated by a secure key \( SK_i \), so there are \( 16! \approx 2.1 \times 10^{13} \) different templates. Moreover,
Fig. 5. Example of (a) 4×4 magic signet and (b) two-dimensional matrix.

Fig. 6. Generated matrix by secure key SK₁.

3.3. Embedding Procedure

Assume a to-be-hidden message \( S = \{s_j\}_{j=1, 2, \cdots, HW/2; 0 \leq s_j \leq 15} \), where every \( s_j \) is concealed by a pair of pixels. Let \( I \) be a gray-level image of height \( H \) and width \( W \), respectively. So \( I = \{i_p|p=1, 2, \cdots, HW; 0 \leq p \leq 255\} \). In order to improve the security of the proposed scheme, the pixels of an original image are shuffled using the third secure key SK₂ by a secure pseudo-random number generator (PRNG) before the embedding process is preceded. Fig. 8 shows the flow chart of the embedding procedure.

Afterward, the pixel values are put into pairs so each pair \((p'_j, p''_j)\) can be treated as a coordinate of the two-dimensional magic matrix. Let \( M(p'_j, p''_j) \) and \( M(q_s, q_{s+1}) \) be the numbers in the magic matrix \( M \) where \((p'_j, p''_j)\) and \((q_s, q_{s+1})\) represent the pairs of pixels before/after a 4-bit secret number \( s_j \) has been concealed. For a given to-be-
A two-dimensional matrix $256 \times 256$

$\begin{array}{cccccc}
255 & . & . & . & . & . \\
. & . & . & . & . & . \\
. & . & . & . & . & . \\
. & . & . & . & . & . \\
. & . & . & . & . & . \\
0 & . & . & . & . & 255 \\
\end{array}$

Put SK$_2$ matrix into $256 \times 256$ matrix

$\begin{array}{cccccc}
1 & 11 & 9 & 3 & . & . \\
5 & 15 & 13 & 7 & . & . \\
8 & 14 & 0 & 3 & . & . \\
4 & 10 & 12 & 2 & . & . \\
0 & . & . & . & . & 255 \\
\end{array}$

Fig. 7. Matrix in the size of $256 \times 256$ pixels is covered by secure key SK$_2$.

4. Experimental Results

Four test images were used, namely (a) Barbara, (b) Boat, (c) Lena, and (d) Peppers. All of them are $512 \times 512$ pixels grayscale images, which are shown in Fig. 9. The experiment uses the MATLAB random function generator to generate a sequence of bit streams as the secret data. The peak signal-to-noise ratio (PSNR), defined as

$$PSNR = 10 \log \left( \frac{255^2}{MSE} \right)$$

where MSE is the mean square error between the cover image and stego-image, (1) can be used to evaluate the distortion of the stego-image after the secret data have been embedded. MSE is defined as

$$MSE = \frac{1}{HW} \sum_{i=1}^{H} \sum_{j=1}^{W} (q_{ij} - p_{ij})^2$$

where $p_{ij}$ and $q_{ij}$ represent the pixel values of the cover image $I$ and the stego-image $SI$, respectively. The embedding capacity (EC) is defined as the maximal number of bits that can be embedded for each pixel (bpp).

If the PSNR value gets larger, then the quality of the image is closer to its original image. In general, a PSNR value greater than 30 dB indicates the closeness of the stego-image and the cover image. Thus, the quality of the stego-image with the PSNR value greater than 30 dB is taken as perceptually acceptable.
Table 1 shows the comparison of the proposed scheme with the other three related schemes proposed by Chang et al.[10], Chang et al.[11], and Lee et al.[16], respectively, in terms of the embedding capacity and image quality. From Table 1, the proposed scheme has 2 bpp of embedded capacity which is the same with the Pencil-shape scheme[16] and higher than those of the schemes proposed by Chang et al.[10] and Chang et al.[11].

Experimental results show that the proposed scheme, in comparison with Sudoku and Turtle-shaped schemes, outperforms in terms of embedding capacity and security. However, compared with Sudoku and Turtle-shaped schemes, it outperforms in terms of embedding capacity and security, but needs to pay the cost of image distortion. Compared with the pencil-shaped pattern embedding scheme[16], the proposed scheme has an equal amount of embedding capacity, but our scheme improves the image visual quality. The average PSNR values reach 44.12 dB higher than that with 42.87 dB of the pencil-shape scheme. Table 1 shows lower PSNR values compared with those of schemes proposed by Chang et al.[10] and Chang et al.[11]. However, when weighing up the relative advantages of embedding capacity and image quality in PSNR values, we are more concerned about whether our method has a higher payload. High embedding capacity indicates the better ability of information embedding and transmission. That means, under the same level of imperceptivity, that a cover image can carry more secret messages at once, which will earn in the data transfer rate, thus further reducing transmission complexity.

In Table 2, we use test images such as Lena, Baboon, Peppers, Airplane, and Boat to observe the change of image quality under different payloads in the proposed method. This experimental result shows the payloads at each stage are $1 \times 10^5$ bits, $2 \times 10^5$ bits, $3 \times 10^5$ bits, $4 \times 10^5$ bits, and $5 \times 10^5$ bits, respectively, and the corresponding image quality by PSNR will change with the payload. For example, when the payload is $1 \times 10^5$ bits, PSNR of Lena, Baboon, Peppers, Airplane, and Boat reaches 53.9 dB on average. Next, when the payload is $2 \times 10^5$ bits, PSNR reaches 50.9 dB on average. Even if the payload is up to $5 \times 10^5$ bits, PSNR still preserves in 46.9 dB on average. PSNR of each image is very close at each stage of payload; thus, our proposed method has good stability.
5. Conclusions

We propose a scheme exploiting a square template to conceal confidential information. The scheme has high embedded capacity and provides good image quality. Based on the magic square, each cover pixel pair can carry the secret data of 4 bits. Moreover, the image quality can keep in 44.12 dB on average, which can be applied to some applications that require high embedded capacity and stable image quality. The proposed method can bring more benefits for information exchange. In the future, a good design of the magic matrix should be conducted to enhance the performance in terms of image quality and embedding capacity as well.

References


Chin-Feng Lee was born in Kaohsiung in 1969. She received her Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taipei in 1998. She is currently a professor in information management with Chaoyang University of Technology, Taichung. Her research interests include steganography, image processing, information retrieval, and data mining.

Ying-Xiang Wang received his B.S degree in information management from Chaoyang University of Technology in 2016. At present, he is pursuing the M.S. degree in information management with Chaoyang University of Technology. His research interest is steganography.