Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Tangram Algorithm: High Image Quality Secret Sharing Scheme Using Two Steganographic Images

Wanli Lyu [a)], Jiahao Deng [b)], Yu Zhang and Dongshuo Yin

Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Key Lab of Industrial Image Processing and Analysis of Anhui Province, China.

[a)] wanly_lv@163.com
[b)] 291951523@qq.com

Abstract. In this paper, our proposed scheme using two steganography images. Unlike other data hiding schemes, this scheme studies the characteristics of the Tangram puzzle model and the secret message bytes that make up the eight binary bits that are hidden into the two graphs. Key matrix M *, horizontal and vertical coordinate range from 0 to 255, and the pixel pairs in the cover image are used to help hide the secret message bytes in our scenario. The paired pixel points into single and double number hidden in two figures. Experiments show that the program can hide relatively more pixels in a cover image with less losing image quality.

Key words: steganography images; Tangram puzzle; matrix M *; hide relatively; scenario.

INTRODUCTION

With the military image processing, medical image processing, multimedia file management and other applications of the secret information more efficient embedded requirements. Steganography is an important secret information and communication technology in which people can send messages without people's awareness of the information being sent. Digital steganography has been recognized by recent and most popular data hiding techniques.

Due to the limited storage space of mobile devices such as mobile phones, people rely more on cloud computing. For information security, we need an algorithm that can meet the needs of high embedding capability and low image distortion. Among these data image hiding categories, the EMD method [1] is high-capacity, but weak in embedding. Lyu et al's method [2] is a high-volume technology, but image quality can have an impact. Chaotic map based random image steganography using LSB technique method [3] is a good image quality but can only hide information in a figure. Considering that if the hidden information can be placed in two places, respectively, which will increase the security of information hiding, we propose a new scheme based on the EMD algorithm and a digital concealment scheme based on the Tangram puzzle model. We still use the mode 5 magic matrix, but we recommend using two pictures to hide the secret information, which is stored in two steganographic images. The mobile terminal only needs to keep the Tangram puzzle secret key, the information encryption is hidden in two clouds, and when the information is extracted, the information can be matched according to the secret key. The focus of this paper is to improve the security of the secret image without causing more distortion of the host image, improving the embedding rate and reducing the processing time of image hiding.

The rest of this paper is organized as follows. In Section 2, we introduce and describe the EMD algorithm and discuss the implementation of the EMD algorithm, which is the relevant part of our proposal. In Section 3, we propose an information hiding scheme based on the Tangram puzzle model, which details our scheme and its

implementation. In Section 4, we present the results report of the experiment. In section 5, the entire article is summarized.

REVIEW OF THE EMD METHOD

The EMD method is to inject secret information into a set of cover image pixels.

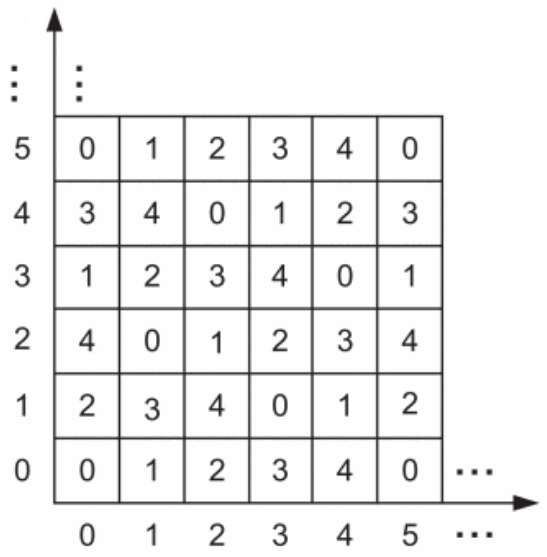

FIGURE 1. Diagram of mode 5 of the magic matrix M

The secret data is embedded in the cover image using the magic matrix M in fig.1. The pixels of the cover image are listed as $(p_1, p_2, \cdots, p_n)$, where n represents the number of pixels in the pixel group, p_i is the i -th pixel, and mod is the module operator. Before the hiding begins, the binary secret data is converted to a base-$(2n+1)$ digital system. Each secret digital message d is embedded into $(p_1, p_2, \cdots, p_n)$. If $d = y$, the cover image pixels $(p_1, p_2, \cdots, p_n)$ do not change to embedding d , otherwise $(p_1, p_2, \cdots, p_n)$ should be modified to at most one gray scale of a pixel to embed. After that, the extraction function f is defined as Equation (1).

$$y = f(p_1, p_2, \ldots\ldots, p_n) = \left[\sum_{i=1}^{n} p_i \times i \right] \bmod(2n+1) \tag{1}$$

The extraction phase for extracting the password is very easy. When all secret numbers are extracted, these numbers can be converted to the original binary password. Using EMD method can get a relatively high hidden image quality, but the key is simple, making it easy for people to crack and extract secret information. And with the development of cloud computing, the embedment capability of EMD methods is insufficient to meet people's need for embedded capabilities.

PROPOSED SCHEME

To enhance the high-authority of the data-hiding, we want to gain larger payloads with acceptable visual quality. Inspired by the EMD method, the proposed scheme uses two steganographic images to record the modification of cover images to achieve a data-hiding scheme. The proposed scheme uses a magic matrix similar to the EMD method in the embedding phase, and then explores another attribute, a data-hiding algorithm based on the Tangram puzzle model.

Key Matrix with Tangram Puzzle Model

The proposed scheme utilizes a key matrix M^* with horizontal and vertical coordinate ranges from 0 to 255 to hide the information.

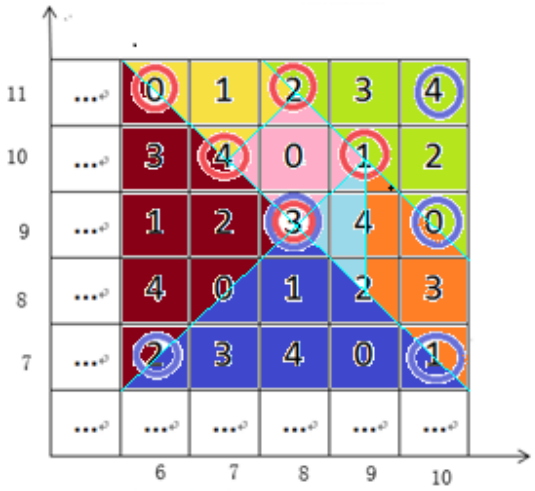

FIGURE 2. Diagram of 5×5 window of the magic matrix M^* with the tangram puzzle model method

Figure 2 shows the two properties of the key matrix M^*. One is a key matrix centered on a randomly selected point 5×5 as the key matrix M^*, and where the blue circle position in the Tangram puzzle model shown in Fig. 2, the red circle position must have $0,1,2,3,4,5$ .The other important attribute of the key matrix is that if any of the blue circles in the square of the 5×5 square centered on any of the key matrices M^* are randomly selected, the corresponding red position must have a number corresponding to one and the corresponding position is at random.

For example, suppose the random point $(8,9)$ is the center of the 5×5 key matrix M^*, where the corresponding red position of the blue position $(6,7)$, $(6,7)$ is $(8,11)$,we can see that the two positions correspond to the same number.

The Embedding Phase

Our idea is to use the cover image to carry secret information to protect the secret information. In other words, the visual quality of the two steganographic images is the same, and we carry the secret information by converting the cover image into two steganographic images.

First, using a pair of pixels in the cover image, one for horizontal coordinates and the other for vertical coordinates and can locate a point in the key matrix M^*. For a pair of pixels (p_i, p_j) as the origin of the coordinates, in the key matrix M^*, the extension point (p_i, p_j) is horizontal and vertical in the key matrix M^*. We can extend the selected 5×5 rectangle, as shown in Fig 2. When the value of two positions in the horizontal direction of the cover image is taken as the horizontal and vertical coordinates in the key matrix M^*, get the value of this position and compare it with two consecutive secret values. If the comparison result is the same, the horizontal and vertical coordinates are respectively assigned to the two steganographic images. If the comparison results of the odd positions of the secret information are not the same, then the horizontal and vertical coordinates with the same comparison result are found in the blue position of the jigsaw puzzle model centered on the current position and assigned them to the first steganographic image. If the comparison result of the even-numbered positions of the secret information is not the same, then the horizontal and vertical coordinates with the same comparison result are found in the red position of the jigsaw puzzle model centered on the current position and assigned to the second steganographic image.

Enter the grayscale image $I = p_1, p_2, ..., p_{h\times w}$. Where p_i denotes the pixel of the i-th and the size of I is $h \times w$, the secret bits denote as S and the key matrix shows as $M*$, 15 steps of the embedding phase is as follows:

Input: cover image $I = p_1, p_2, ..., p_{h\times w}$, secret bit S and key matrix $M*$.

Output: two steganographic image $I' = p_1', p_2', ..., p_{h\times w}'$ and $I'' = p_1'', p_2'', ..., p_{h\times w}''$, whose size is $h \times w$.

Step 1: Convert S into the base-5 numeral system $(S)_5 = (s_1, s_2, ..., s_{h\times w})_5$. Once all the bits of the secret S are processed, then move to step 2.

Step 2: Set $i = 1$ then move to step 3.

Step 3: Read a cover pixel pairs p_i, p_{i+1} from the cover image. The value of the pixel to be read is taken as the horizontal and vertical values $M^*(p_i, p_{i+1})$ of the key matrix $M*$. When s_i is a secret bit and $s_i == M^*(p_i, p_{i+1})$, $p_i' = p_i$, $p_{i+1}' = p_{i+1}$, go to step 8. Otherwise, go to step 4.

Step4: When $s_i == M^*(p_i+2, p_{i+1}+2)$, $p_i' = p_i + 2$, $p_{i+1}' = p_{i+1}+2$, go to step 8. Otherwise, go to step 5.

Step 5: When $s_i == M^*(p_i-2, p_{i+1}-2)$, $p_i' = p_i - 2, p_{i+1}' = p_{i+1} - 2$, go to step 8. Otherwise, go to step 6.

Step 6: When $s_i == M^*(p_i+2, p_{i+1})$, $p_i' = p_i+2, p_{i+1}' = p_{i+1}$, go to step 8. Otherwise, go to step 7.

Step 7: When $s_i == M^*(p_i+2, p_{i+1}-2)$, $p_i' = p_i + 2$, $p_{i+1}' = p_{i+1} - 2$ Go to step 8.

Step 8: Compare the range of i, if $i <= 512\times512$, set $i = i + 2$, then go to step 3. Until all the secret number is embedded and goes to step 9.

Step 9: Set $i = 1$, and move to step 10.

Step 10: Read two-pixel pairs, p_i, p_{i+1} from the cover image. The value of the pixel to be read is taken as the horizontal and vertical values $M^*(p_i, p_{i+1})$ of the key matrix $M*$. And when $s_{i+1} == M^*(p_i, p_{i+1})$, $p_i'' = p_i$, $p_{i+1}'' = p_{i+1}$, go to step 15. Otherwise, go to step 11.

Step 11: When $s_{i+1} == M^*(p_i, p_{i+1}+2)$, $p_i'' = p_i$, $p_{i+1}'' = p_{i+1}+2$ go to step 15. Otherwise, go to step 12.

Step 12: When $s_{i+1} == M^*(p_i-2, p_{i+1}+2)$, $p_i'' = p_i - 2$, $p_{i+1}'' = p_{i+1}+2$, go to step 15. Otherwise, go to step 13.

Step13: When $s_{i+1} == M^*(p_i-1, p_{i+1}+1)$, $p_i'' = p_i - 1$, $p_{i+1}'' = p_{i+1}+1$, go to step 15. Otherwise, go to step 14.

Step 14: When $s_{i+1} == M^*(p_i+1, p_{i+1}+1)$, $p_i'' = p_i+1$, $p_{i+1}'' = p_{i+1}+1$, Go to step 15.

Step 15: Compare the range of i, if $i <= 512\times512$, set $i = i+2$, then go to step 10. Until all the secret numbers are embedded, ending the operation.

For example, suppose that a pair of pixels in the cover image is $(p_i, p_{i+1}) = (6,3)$. By taking the horizontal coordinate 6 and the vertical coordinate 3, we can locate a point in the key matrix $M*$. In the horizontal and vertical direction to expand into pairs of pixels, we can extract a key matrix to the point as the center of the 5×5 matrix, as shown in Fig.2. To embed the secret message, suppose the secret byte is 001010112, we first calculate the secret byte to the corresponding pentad value to get the secret bit value of 43. By looking at the Tangram position in the 5×5 matrix in the blue circle with the secret bit get the same point, and then we get the new point (p_k, p_r). Find the point in the red and blue circle with the same value as the secret bit in the Tangram position in the 5×5 matrix, and then we get the new point (p_t, p_d).It will be our two hidden pixels, one is $(6,3)$, and the other is $(6,5)$, which will be my two hidden pixels. Finally, the sender sends two steganographic images to the authorized recipient after the secret message is embedded.

The Secret Message Extraction Phase

The receiver extracts the secret message accurately by using the following extraction phase:

Input: two hidden images $I' = p_1', p_2', \ldots, p_{h\times w}'$ and $I'' = p_1'', p_2'', \ldots, p_{h\times w}''$, whose size is $h\times w$ and the key matrix $M*$.

Output: Secret bit S'.

Step 1: Set $i=1$, then move to step 2.

Step 2: Obtain a pair of hermit pixels p_i' , p_{i+1}', and both from the hidden image I', the secret information extracted is $M^*\left(p_i', p_{i+1}'\right)$. p_i'', p_{i+1}'' from the hidden image I'', and the secret information extracted by the pair of steganographic pixels $\left(p_i'', p_{i+1}''\right)$ and the secret information extracted is $M^*\left(p_i'', p_{i+1}''\right)$.

Step 3: Output Message Bit S'. When the S' bit output is not complete, $i=i+2$, and then go to step 2. Follow the example given in Section 3.2 to clearly describe the extraction phase. The example is the extraction phase of the presentation as follows. Assuming that the receiver obtains two pairs of pixels from two invisible images, one is $(p_i', p_{i+1}')=(6,3)$, which are two invisible pixels of the invisible image I' and the other is $(p_i'', p_{i+1}'')=(6,5)$, which is the hidden image I'' of two hidden pixels. Find the value 4 by $M^*(6,3)$, through $M^*(6,5)$ when the value 3 is found, the secret message 43 is extracted and 43 is converted to a binary bit, so we have a secret binary message $(00101011)_2$.

EXPERIMENTAL RESULTS

The purpose of our program is to hide relatively more pixels in a cover image with less losing image quality. Nine 512×512 grayscale images are used as overlay images for later comparison of image quality. We implemented the EMD method and used the software proposed by MATLAB R2016a.

The image quality is evaluated with a peak signal-to-noise ratio (PSNR). The PSNR of the $h\times w$ grayscale image is defined as equation (2):

$$PSNR=10\times\log_{10}\frac{255^2\times3}{MSE}$$
$$MSE=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(x_{ij}-\overline{x_{ij}}\right)^2 \tag{2}$$

In equation (2), x_{ij} represents the original pixel value, and $\overline{x_{ij}}$ represents the pixel value of the steganographic image.

(a) Shadow 1 of Baboon, Boat, Lean, and Tiffany.

(b) Shadow 2 of Baboon, Boat, Lean, and Tiffany.

(c) Shadow 1 of Pepper, Zelda, Barbara, and Plane.

(d) Shadow 2 of Pepper, Zelda, Barbara, and Plane.

FIGURE 3. The steganographic images with secret message based on proposed scheme

Figure 3 shows the embedded image based on our proposed scheme. At the same time, it shows that this approach provides a better visual quality than the Lyu et al's method at an acceptable degree of visual unnoticeability. Our average PSNR is 45dB and the Lyu et al's method is 36dB. With the same two steganographic images, our scheme has low distortion and better image concealment.

TABLE 1. The PSNR of a steganographic image with secret messages and original cover image

PSNR(db)	Lyu et al's method [2]		The proposed scheme	
	Steganographic image1	Steganographic image2	Steganographic image1	Steganographic image2
Baboon	36.2604	36.1902	46.1244	43.6923
Boat	36.1810	36.2073	46.1243	43.6913
Lean	26.2357	36.2408	46.1213	43.6957
Tiffany	36.2296	36.2140	46.0751	43.6301
Pepper	36.2055	36.1677	46.1175	43.6797
Zelda	36.2067	36.2552	46.1186	43.6957
Barbara	36.2322	36.2174	46.1186	43.6957
Plane	36.2318	36.2145	46.0882	43.6839

TABLE 2. A comparison of visual quality and capacity comparisons with methods by Lee and Huang [6] and Peng et al [4].

	Lee and Huang's Method [6]		Peng et al.'s Method [4]		The proposed scheme	
	Payload (bpp)	PSNR (db)	Payload (bpp)	PSNR (db)	Payload (bpp)	PSNR (db)
Boat	2.270	20.49	1.000	25.49	1.161	45.20
Barbara	1.580	20.96	1.200	26.66	1.161	44.90
Lena	1.320	22.32	1.500	27.45	1.161	44.90
Pepper	1.290	22.45	1.200	27.74	1.161	44.89
Average	1.615	21.55	1.255	26.83	1.161	44.98

Compared with the Lee and Huang's method, the PSNR average only 21.55dB and the payload is 1.615bpp. Our method at a loss of less than 0.5bpp hidden amount has increased by 1 times the visual quality. Compared with Peng et al.'s method, the average PSNR is only 26.83dB and the payload is 1.255bpp. Our method lost less than 0.09bpp hidden amount but increased 1 times the visual quality. Therefore, as can be seen from Table 2, it is clear that our plan PSNR significantly more than the other two programs. Our proposed scheme could bring better picture hiding effect.

CONCLUSION

In this paper, we propose a method to hide information as much as possible while hiding it in two steganographic images and requiring high image quality. This research can be more suitable for efficient embedded and secure cloud computing storage that needs secret information Encryption. This method can improve the hidden capacity and low distortion and design a Tangram puzzle model key. Mobile users can efficiently and conveniently store and retrieve information using cloud computing while retaining only the jigsaw puzzle key. Pixel pair uses image processing when embedding data. The experimental results confirm that this scheme can improve the image quality and hide more secret information cover image.

REFERENCES

1. X. P. Zhang and S. Z. Wang, "Efficient steganographic Embedding by Exploiting Modification Direction," IEEE communications Letters, Vol. 10, No. 11, (2006), pp.1-3.
2. Y. J. Lu and W. L. Lyu, "A novel high-capacity reversible data-hiding scheme using two steganographic images," International Conference on Biomedical Engineering and Informatics. IEEE, 667-671(2015).
3. S. Rajendran and M. Doraipandian, "Chaotic map based random image steganography using LSB technique," International Journal of Network Security 19(2017).
4. C. C. Chang and T. D. Kieu and Y. C. Chou, "Reversible Data Hiding Scheme Using Two steganographic Images," IEEE TENCON, (2007), pp.1-4.
5. F. Peng and X. L. Li and B. Yang, "Adaptive Reversible Data Hiding Scheme Based on Integer Transform," Signal Processing, Vol. 92, NO. 1, (2012), pp. 54-62.
6. C. F. Lee and Y. L. Huang, "An Efficient Image Interpolation Increasing Payload in Reversible Data Hiding," Expert Systems with Applications, Vol. 39, No. 8, 6712-6719(2012).
7. P. Maniriho and T. Ahmad, "Enhancing the capability of data hiding method based on reduced difference expansion," Engineering Letters, Vol.26, NO.1, (2018), pp.45-55.
8. M. A. Hameed and S. Aly and M. Hassaballah, "An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD)," Multimedia Tools & Applications, Vol.8, (2017), pp. 1-19.
9. M. M. Haque and J. Sheikh and M. J. A. Rashid, "An improved steganographic technique based on diamond encoding method," International Conference on Electrical, (2017), pp.583-588.
10. C. C. Chang and C. T. Li, "Secure Secret Sharing in the Cloud," 2017 IEEE International Symposium on Multimedia (ISM), (2017), pp. 358 – 361.
11. X. Li and W. Zhang and X. Gui, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification," IEEE on Information Forensics and Security, Vol.8, NO.7, (2013), pp.1091-1100.