Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

A secret image sharing scheme with improved embedding capacity and a deception recognition mechanism

Yixuan Du[1], Yanhai Zhang[1], Jinmei Fan[1,] ✉

[1] *School of Mathematics and Statistics, Guilin University of Technology, Guilin, Guangxi, 541006, China*

ABSTRACT

Image hiding is a technique for transmitting secret information under the cover of a digital image. It usually conceals sensitive information into images for the purpose of encryption. Currently, high embedding capacity and information security remain important research aspects of the image hiding. In this study, a secret image sharing scheme based on a reference matrix is proposed to enhance embedding capacity and verify data integrity. In the proposed scheme, a hill matrix is designed as a reference matrix and a location table is generated. Moreover, a location pair table is generated to ensure the uniqueness of data hiding locations. Then, leveraging the processing of the location pair table, as well as the mapping of the reference matrix and the location table, each pixel pair is exploited to conceal eight secret bits. Furthermore, based on the special construction of the hill matrix, a deception recognition mechanism is designed. This mechanism can detect deceptive behavior and identify tampered images by means of data hiding locations. The experimental results indicate that the proposed scheme achieves a higher embedding capacity and better deception recognition performance than that of most of existing schemes.

Keywords: secret image sharing, hill matrix, embedding capacity, deception recognition mechanism

1. Introduction

With the rapid development of cloud computing technology, image hiding has taken an important place in data protection, secure communication, and copyright management. In image hiding schemes, maximizing embedding capacity and ensuring information security are two important objectives [1-5]. Information security can be improved through the use of complex encryption algorithms or detection mechanism [6-11]. But a higher detection rate usually leads to a decrease in embedding capacity. Therefore, from a technical perspective, it is a significant challenge to balance visual quality, embedding

✉ Corresponding author.
E-mail address: duyixuan0425@163.com (J. Fan).
Received 25 October 2024; Revised 10 December 2024; Accepted 05 March 2025; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-110

capacity, as well as security. In the past few decades, various methods have been proposed to overcome this challenge. These traditional image hiding methods can be divided into two categories that are based on visual secret sharing (VSS) [12-14] and polynomial [15-21]. In the VSS schemes [12-14], the original information is divided into multiple shares, only by combining a sufficient number of shares can the original information be restored. However, the anti attack capacity of VSS schemes is still limited. Therefore, many schemes based on polynomial have been proposed. In 2002, Thien and Lin pro- posed a (k,n) threshold secret image sharing (SIS) scheme [17]. In the scheme, the secret data is encrypted into n shares using a polynomial, which are distributed to n recipients individually. The initial image can be recovered only when any k or more recipients collaborate, while any fewer than k recipients collaborating cannot recover the secret image. Compared with the Shamir's scheme [15], each shadow image is 1/t the size of the secret image in Thien's scheme, which is beneficial for storage and concealment of secret information. Furthermore, to enhance information security, Wu and Liu proposed a novel hierarchical secret image sharing scheme with multi-group joint management [18]. The scheme utilizes the Birkhoff interpolation algorithm to share the secret image among multiple groups with different thresholds. Therefore, the security of secret image is ensured by distributed storage on multiple clouds. Subsequently, Rama Singh et al. utilized the Huffman Cipher system to achieve an efficient lossless compression and enhance the embedding capacity [22]. On the other hand, the system's security is enhanced through a strategy of exchanging same level nodes, followed by scrambling to encrypt the dictionary.

However, due to the fixed threshold k, above-mentioned schemes cannot fully meet the requirements of dynamic security levels. To address this shortcoming, Zhang et al. proposed threshold changeable $t' > t$ scheme [19], which makes secret information be reconstructed under the (t', n) threshold condition. But the scheme has to meet strict threshold requirements and needs a high storage space and complex polynomial calculations. To overcome the weaknesses of Zhang's scheme, Yuan proposed an improved threshold changeable secret sharing scheme [20], where bi-variable one-way functions are used to resist attacks. Building upon [19-20], Liu et al. proposed a $(k' \leftarrow k \rightarrow k'', n)$ threshold variable secret image sharing scheme based on interpolation polynomials [21]. When the threshold requirement is reduced to k' or increased to k'', each participant can update their shadow based on the published information.

To further enhance data security, many reversible data hiding in encrypted domain (RDHEI) schemes have been proposed [23-25]. In 2014, Ma et al. proposed reserving room before encryption [23]. This method makes the data hiding process easy. Subsequently, a reversible data hiding method in encrypted images with two-MSB prediction was proposed [24]. In this scheme, the image is preprocessed before encryption to reserve room for data hiding. At the receiving end, the additional data is extracted using the hiding key. The original image is recovered using the encryption key. Compared with traditional methods, reserving room before encryption offers increased security. It prevents attackers from inferring encryption keys or other sensitive information based on the known relationship between plaintext and ciphertext. Reserving room after encryption is similar to reserving room before encryption. Ruchi Agarwal et al. used reserving room after encryption and the odd and even nature of prediction errors to distinguish between embedded and nonembedded pixels [25]. This avoids the computational overhead caused by location maps. The method improves the embedding capacity and visual quality of the stego image. It also enhances data security and flexibility through double-layer encryption and a separable design.

Recently, some secret image sharing methods based on mapping matrices have been proposed [2] [26-32]. Compared with traditional image hiding schemes, the special struction of mapping matrices not only allows for more information to be embedded into the image but also enhances the scheme's resistance to attacks. In 2014, Chang first proposed a secret image sharing scheme based on turtle shell matrices [28]. The scheme [28] constructs a turtle shell matrix with a size of 256 × 256. Using this turtle shell matrix,

each cover pixel pair is exploited to conceal three secret bits. Due to the turtle shell matrix and associated sets, each cover pixel pair generates an unique stego pixel pair. After processing all the binary secret data, the final stego image closely resembles the cover image leading to better visual quality. Based on the scheme from [28], Liu et al. introduced a high-capacity secret hiding scheme [29]. In this scheme, a location table is designed to conceal four bits of secret data by each cover pixel pair. Furthermore, Li proposed a secret sharing scheme [30] with higher hiding capacity and better visual quality. In Li's scheme, a new reference matrix is designed to enhance embedding capacity and the design of the reference area enhances its visual quality. Although above schemes enhance embedding capacity, there is a lack of consideration for information security. To further balance embedding capacity and information security, Liu et al. proposed a sharing scheme utilizing two different cover images [31] to generate two stego images that are stored by two participants. During reconstruction, the presence of deception is detected based on the hidden locations of secret data, thereby ensuring the accuracy of the secret information. In 2020, Chang et al. introduced a maze matrix-based secret image sharing scheme with cheater detection [32]. Compared with scheme in [31], Chang et al.'s scheme not only can detect the presence of deceptive behavior but also can identify tampered images. However, the deception recognition mechanism in this scheme only identifies tampered images under specific conditions.

To increase embedding capacity and improve the deception recognition mechanism, we proposed a secret image sharing scheme based on a reference matrix. In the proposed scheme, a hill matrix is designed as a reference matrix and a location table is generated. Moreover, a location pair table is generated to ensure the uniqueness of the data hiding positions. Then, leveraging the processing of the location pair table, as well as the mapping of the reference matrix and the location table, each pixel pair is exploited to conceal eight secret bits. Furthermore, based on the special construction of the hill matrix, a deception recognition mechanism is designed. This mechanism can detect deceptive behavior and identify tampered images by means of data hiding locations. The experimental results indicate that the proposed scheme achieves a higher embedding capacity and better deception recognition mechanism than that of most of previous schemes.

The rest of this paper is organized as follows. Section 2 briefly reviews Liu's high-capacity secret image sharing scheme [29] and the sharing scheme that utilizes two different cover images [31]. Section 3 describes the proposed image hiding scheme. Section 4 provides experimental results and performance comparisons. Our conclusions are presented in Section 5.

2. Related Work

In this section, we reviewed the high capacity secret image sharing scheme using a location table [29] and the sharing scheme that utilizes two different cover images [31].

2.1. The high capacity secret image sharing scheme using a location table [29]

Inspired by Chang et al.'s scheme [28], Liu et al. proposed a sharing scheme using a location table to achieve high embedding capacity. In the scheme, the location table T defines the elements at different positions in the turtle shell, which are divided into upper turtle back element, lower turtle back element, and turtle edge point element. As shown in Figure 1, kinds of sixteen elements uniquely correspond to the two indicators (p_j, p_{j+1}) in the location table. The indicators p_j and p_{j+1} respectively represent the first two bits and the last two bits of a set of secret data, belonging to {00, 01, 10, 11}. The turtle shell matrix M used in the scheme is shown in Figure 2. This scheme combined the location table T with the turtle shell matrix M to conceal four bits of secret data in a cover pixel pair. However, the embedding capacity of this scheme needs to be enhanced to efficiently conceal secret data.

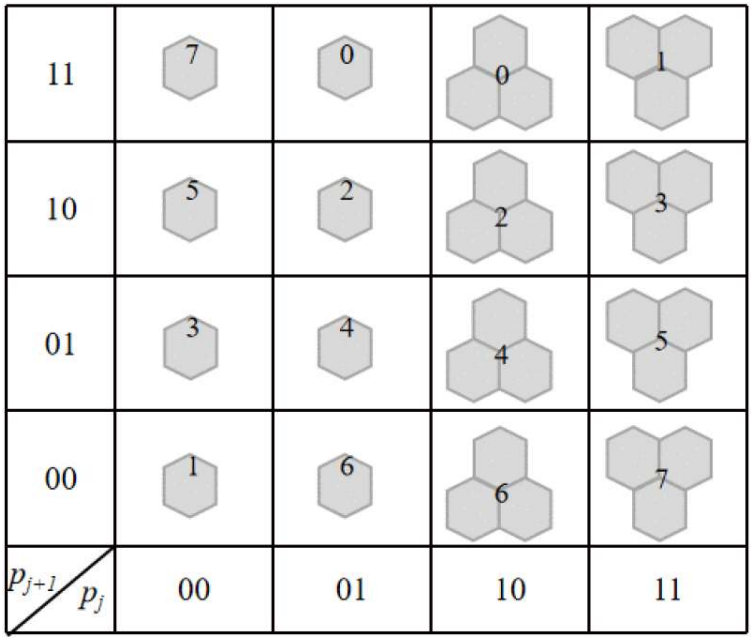


Fig. 1. A location table for the secret image sharing scheme

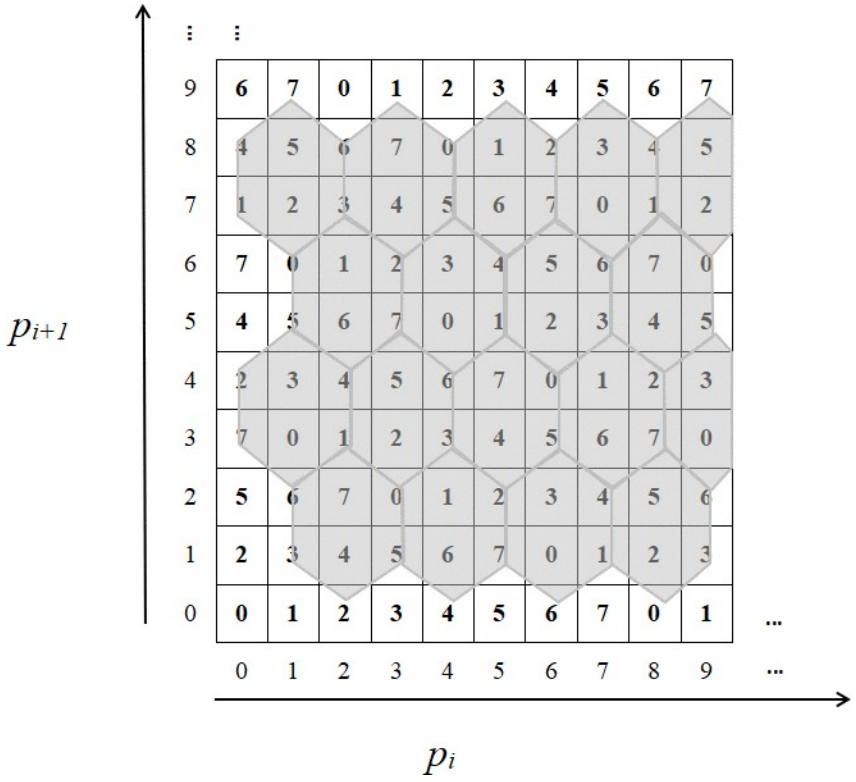


Fig. 2. Shell matrix M for the secret image sharing scheme

2.2. Secret image sharing scheme with cheating detection [31]

In [31], Liu et al. proposed a novel secret image sharing scheme with cheating detection. In this scheme, two types of reference area were designed, that is a flower-shaped area and a rocket-shaped area. The reference areas as shown in

Figure 3. Three bits of secret data are concealed into each cover image pixel by exploiting the two types of reference area. Furthermore, secret data can only be hidden on the back of the turtle. So, when the the

stego pixel pair corresponding to a turtle edge point element, it can be determined that deception has occurred in the process. However, in the scheme, it is difficult to judge the honesty of participants since only loyal participants can recognize deceivers. Moreover, this scheme has lower embedding capacity than that of the scheme in [29].

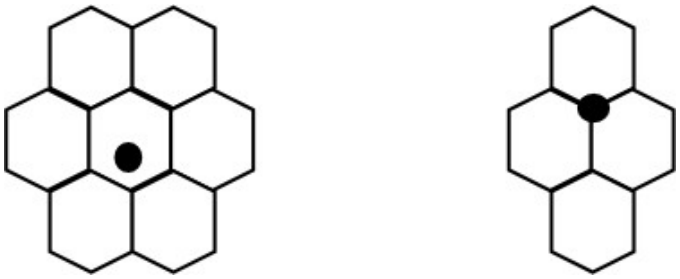


Fig. 3. Example of Reference area for Flower-shaped (left) and Rocket-shaped (right)

3. The proposed secret image sharing scheme

To enhance embedding capacity and improve the deception recognition mechanism, we propose a secret image sharing scheme that is based on a hill matrix. Assume that the binary secret message stream is denoted as $S=\{sg_k \mid k=1,2,...,n\}$, where eight bits of secret data are processed as a group. Assume that two cover images are denoted as $C_1=\{p_{1i} \mid i=1,2,...,H\times W\}$ and $C_2=\{p_{2i} \mid i=1,2,...,H\times W\}$. Leveraging the processing of the location pair table, as well as the mapping of the reference matrix and the location table, each cover pixel pair is exploited to conceal eight secret bits. Meanwhile, a stego pixel pair is generated. Furthermore, deceptive actions and tampered images can be identified by the locations of stego pixel pairs within the hill matrix. The proposed scheme is divided into preparation process, embedding process, and reconstruction process, which are described in detail in Subsection 3.1, 3.2, and 3.3, respectively. In addition, Subsection 3.4 provides a detailed description of the deception recognition mechanism.

3.1. Preparation process

In this stage, a hill matrix M, a location table T and a location pair table D are designed to embed secret data. And a reference area is designed to ensure the uniqueness of stego pixel pairs.

3.1.1. The construction of the hill matrix M. The construction of the hill matrix M is inspired by the turtle shell matrix [29]. The hill matrix is constructed as follows.

1) The correspondence between the rows and columns in the hill matrix and pixel values is confirmed according to the design concept of the turtle shell matrix. And the values corresponding to the rows and columns in the hill matrix are denoted as p_{2i} and p_{1i}, respectively.

2) When

$$\begin{cases} p_{1i}=3k, k=0,1,\cdots,85 \\ p_{2i}=3l+1, l=0,1,\cdots,84 \\ p_{2i}=255 \end{cases} \tag{1}$$

the elements corresponding to the rows and columns where above-mentioned p2i and p1i are located are modified to 'x'.

3) The elements corresponding to other locations remain unchanged. In the hill matrix, the locations where the element 'x' are located cannot be used to conceal secret data. Moreover, a series of 3 × 3 submatrices in the hill matrix M are selected as processing units. In each submatrix, eight elements are selected to form the shape of the left hill or right hill, as shown in Figure 4. The blue blocks in Figure 4 represent the eight selected elements in each submatrix, while the black blocks represent the elements that are not selected. Moreover, a submatrix that contains the shape of a left hill is called left hill submatrix, and a submatrix that contains the shape of a right hill is called right hill submatrix. A part of the hill matrix M is shown in Figure 5.

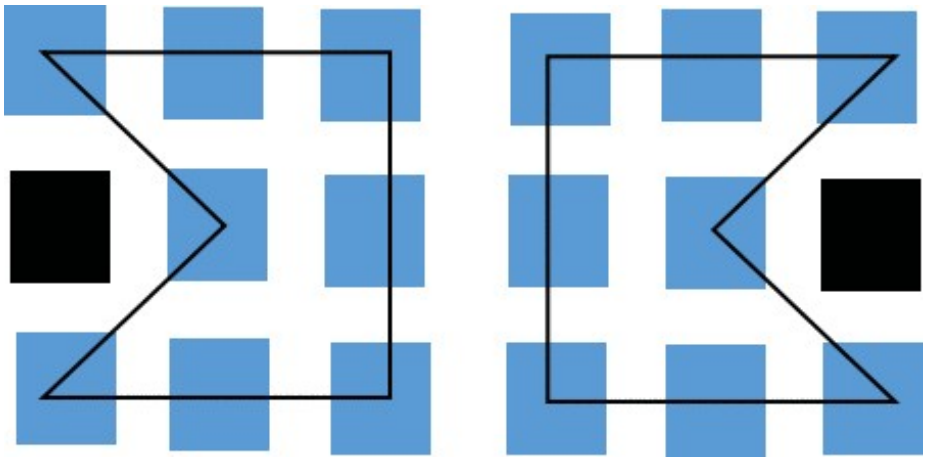


Fig. 4. Left Hill (left) and Right Hill (right)

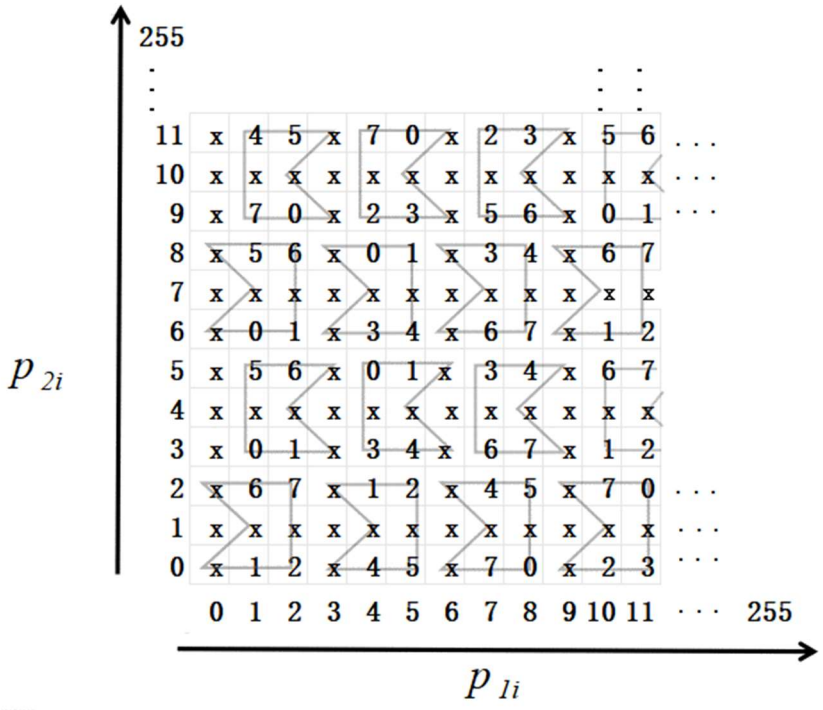
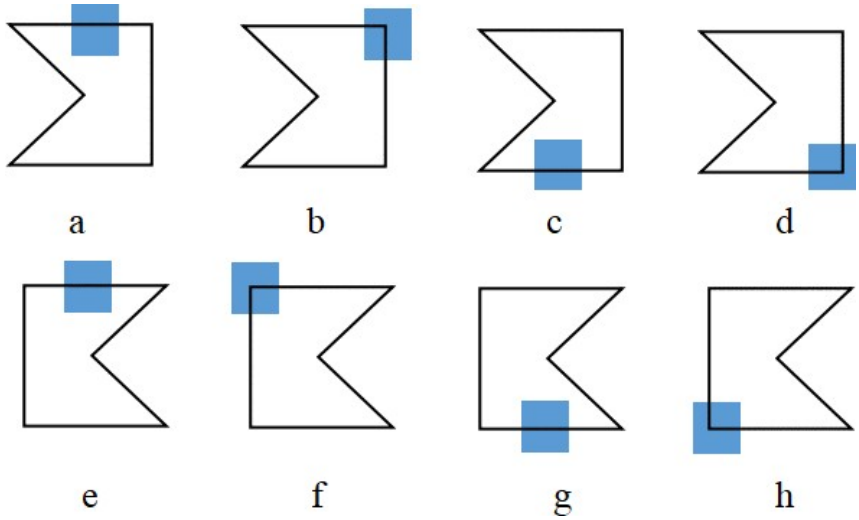


Fig. 5. A part of Hill Matrix M

3.1.2. The construction of location table T. In the proposed scheme, since only the eight legal locations in the left hill and right hill that are not 'x' are used to conceal secret data, as shown in Figure 6. Each location is a number from 0 to 7. So there are 64 different shapes in the location table T. Based on these

features, a location table T can be constructed, which is shown in Figure 7. The elements corresponding to the blue blocks in Figure 7 are called matching elements. The elements situated at non-blue block locations are called non-matching elements. Only the locations corresponding to the matching elements are considered when embedding secret data. In the location table T, each secret shape is composed of the shape of the hill (left hill or right hill), one matching element and eight non-matching elements. These secret shape are represented by two indicators (s_j, s_j+1). Two indicators s_j and s_j+1 are the row value and column value of the location table T, which belong to {000, 001, 010, 011, 100, 101, 110, 111}. The location table T can be used for embedding eight bits of secret data. In each secret data group, the third, fourth, and fifth bits correspond to the row value s_j of location table T, and the sixth, seventh and eighth bits correspond to the column value s_j+1 of location table T. Besides, the first and second bits are used to ensure the unique stego pixel pair (see 3.1.3). For example, assume a secret data group '11010011' is embedded in one cover image pixel pair, where the third, fourth, fifth bits are '010' and the sixth, seventh, eighth bits are '011'. So the corresponding secret shape of the secret data '11010011' is shown in Figure 8.



(a) Location 1; (b) Location 2; (c) Location 3; (d) Location 4; (e) Location 5; (f) Location 6; (g) Location 7; (h) Location 8

Fig. 6. Eight legal hiding locations

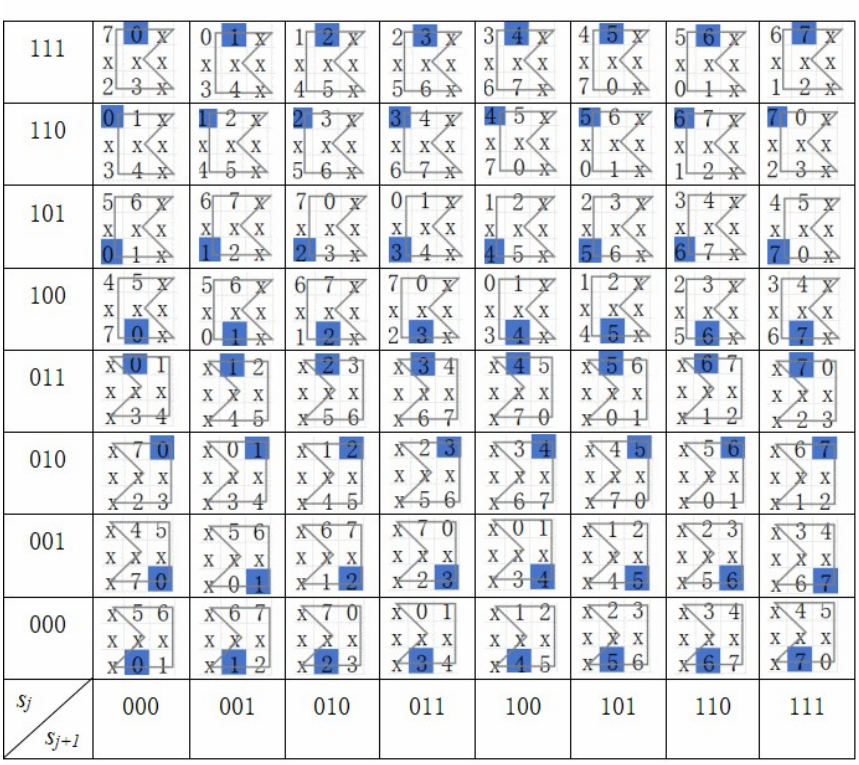


Fig. 7. Location table T

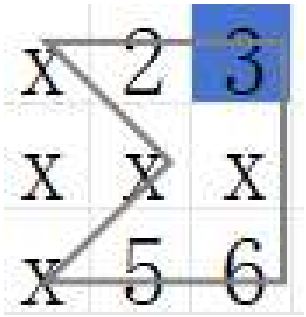


Fig. 8. Secret shape in Location table T

3.1.3. The construction of location pair table D. In the proposed scheme, to ensure the uniqueness of the stego pixel pair, a location pair table D is designed to correspond to the first bit and second bit of a group of secret data. Set the row value q_{2i} and column value q_{1i} of the location pair table D to the grayscale pixel values. Number pairs (u,v) in location pair table D are determined according to q_{1i} and q_{2i}, as follows

$$u=\begin{cases}0 & q_{1i} \bmod 4=0,1\\ 1 & q_{1i} \bmod 4=2,3\end{cases}$$
$$v=\begin{cases}0 & q_{2i} \bmod 4=0,1\\ 1 & q_{2i} \bmod 4=2,3\end{cases} \quad (2)$$

A part of the location pair table D is shown in Figure 9.

11	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	. . .
10	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	. . .
9	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	
8	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	
7	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	
6	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	
5	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	
4	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	
3	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	
2	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)	
1	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	
0	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)	. . .
q_{2i} / q_{1i}	0	1	2	3	4	5	6	7	8	9	10	11	. . .

Fig. 9. Partial location pair table D

3.1.4. The design of a reference area. In the proposed scheme, the reference area is a series of regions in the hill matrix M. Select the corresponding area A according to different cover pixel pairs (p_{1i}, p_{2i}), thereby the optional hiding locations of secret data are limited. The column value range m of area A is used to correspond to p_{1i}, and the row value range n of area A is used to correspond to p_{2i}. The speci fic method for determining the reference area is follows:

1) The range of column value m in area A can be divided into: $0 \le m \le 23$, $24 \le m \le 47, ..., 216 \le m \le 239$. In particular, when $240 \le m \le 255$, we define the range of column value as $231 \le m \le 255$.

2) The range of row value n in area A can be divided into:

When $0 \le n \le 233$,

if $n \mod 3 = 0$, the range of row value is $n : n + 23$,

if $n \mod 3 = 1$, the range of row value is $n - 1 : n + 22$,

if $n \mod 3 = 2$, the range of row value is $n - 2 : n + 21$.

When $234 \le n \le 254$,

if $n \mod 3 = 0$, the range of row value is $n - 21 : n + 2$,

if $n \mod 3 = 1$, the range of row value is $n - 22 : n + 1$,

if $n \mod 3 = 2$, the range of row value is $n - 23 : n$.

Peculiarly, when $n = 255$, the range of row value is $n - 24 : n$.

3.2. Embedding process

The secret data are embedded into two cover images to generate two stego images in the embedding process. In this stage, the binary secret data stream is divided into N groups, where each group contains eight bits of binary data. Since each group of secret data corresponds to a pair of cover pixels, N pairs of cover pixel pairs (p_{1i}, p_{2i}) are randomly selected from the cover images $C_1 = \{p_{1i} \mid i = 1, 2, ..., H \times W\}$ and $C_2 = \{p_{2i} \mid i = 1, 2, ..., H \times W\}$ to conceal N groups of secret data. The positions of these N cover pixel pairs are recorded and uploaded to the cloud. Then the last six bits of each group of secret data are mapped to the location table T to determine a secret shape. Within the reference area corresponding to the cover pixel pair (p_{1i}, p_{2i}), the shapes that are identical to the determined secret shape are found in the hill matrix. The locations of matching elements on these shapes are considered as candidate locations.

According to the (p_{1i}, p_{2i}) corresponding to the candidate positions, number pairs in the location table D are selected, where the column values p_{1i} are equal to p_{1i} and the row values p_{2i} are equal to p_{2i}. The elements of each number pair correspond to the first two bits of the secret data. Therefore, a unique number pair can be determined based on the first two bits of the secret data. The column value p_{1i} and row value p_{2i} corresponding to this unique number pair are the stego pixel values p'_{1i} and p'_{2i}. After iterating through N groups of secret data, stego images C_1 and C_2 with the same size as the cover images are generated.

Example 1: Assume that a cover pixel pair is (5,2) and the secret data is '11010011'. To embed the secret data into the cover pixel pairs. First, the last six bits of the secret data are mapped to the location table T, to obtain the secret shape as shown in Figure 8. The reference area is found by the cover pixel pair (5,2). The column value range is $0 \le p_{1i} \le 23$ and row value range is $0 \le p_{2i} \le 23$. Then, secret shapes within the reference area are found. The shape of the hill, matching element and non-matching elements of these secret shapes are identical to that in Figure 8. Furthermore, the locations of matching elements in these secret shapes are recorded, namely (14,2), (23,8), (8,14), and (17,20). Finally, according to the first bit and second bit of the secret data, the number pair (1,1) is found. Since the number pair (1,1) corresponds to (14,2), the stego pixel pair (p'_{1i}, p'_{2i}) that conceals the secret data is (14,2).

3.3. Reconstruction process

The reconstruction process is a procedure that the secret data in the stego images are extracted to reconstruct the secret image. In this stage, the positions of N pairs of cover pixel pairs are transmitted to the data extractor by the cloud. Then, the stego pixel pairs (p'_{1i}, p'_{2i}) at these positions are extracted. These stego pixel pairs correspond to the column value p_{1i} and row value p_{2i} of the location table D. According to the column value p_{1i} and row value p_{2i}, the number pair in the loaction pair table D is determined as the first two bits of the secret data. Meanwhile, to recover the last six bits of the secret data, the stego pixels p'_{1i} and p'_{2i} are firstly mapped to the column value p1i and row value p2i of the hill matrix M to find the matching element. Then, based on the special arrangement of the left hills and right hills in the hill matrix M, the matching element is used to determine one secret shape. Finally, the secret shape is mapped to the location table T. The row value sj that corresponds to the secret shape represents the third, fourth, and fifth bits of the secret data. The column value sj+1 that corresponds to the secret shape represents the sixth, seventh, and eighth bits of the secret data.

To better understand the process of extracting secret data, Example 1 in the embedding process above is continued. Firstly, the stego pixel pair (14,2) is used to determine the column value and row value of the location pair table D. According to the column value and row value, a number pair (1,1) is determined, which represents the first bit and the second bit of the secret data. Then, the stego pixel pair (14,2) maps to the hill matrix M to obtain the secret shape as shown in Figure 8. The row value '010' corresponding to the secret shape in the location table T is the third, fourth, and fifth bits of the secret data. And the column value '011' corresponding to the secret shape in the location table T is the sixth, seventh, and eighth bits of the secret data.

3.4. Deception recognition mechanism

To recover the secret image correctly, it is important to verify whether deceptive behavior exists in the stego images. Based on the special construction of the proposed hill matrix, a deception recognition mechanism is designed. This mechanism can detect whether deceptive behavior exists in the stego images. Furthermore, this mechanism can identify the cheater who provides a tampered stego image and is excluded from the trusted participants. The specific detection process of this mechanism is as follows.

Firstly, when the stego pixel pair (p'_{1i}, p'_{2i}) is corresponded to the element 'x', it can be identified that the deceptive behavior happened. Furthermore, to detect which participant provides a tampered stego image, a method is designed in the mechanism. In the method, the locations of the elements 'x' are divided into thirteen types, which are marked by the red serial number with cicle in Figure 10. The locations of 'x' in the left hill submatrix are classified into the first, third, fourth, eighth and tenth types marked by 1, 4, 8, 10 with cicle, respectively. The locations of 'x' in the right hill submatrix are classified into the second, fifth, sixth, seventh and ninth types marked by 2, 5, 6, 7, 9 with cicle, respectively. The locations corresponding to others 'x' are classified into the eleventh, twelfth and thirteen types marked by 11, 12 13 with cicle, respectively. The tampered images corresponding to these thirteen types of locations can be divided into the following three scenarios.

1) If the element 'x' corresponding to the stego pixel pair (p'_{1i}, p'_{2i}) is located at the third, fourth, fifth, sixth, eleventh, and thirteenth types of locations, p'_{1i} is a tampered pixel, no matter what value p'_{2i} is. It is reason that there is none p'_{2i} to make a stego pixel pair (p'_{1i}, p'_{2i}) legal.

2) If the element 'x' corresponding to the stego pixel pair (p'_{1i}, p'_{2i}) is located at the seventh, eighth, ninth and tenth types of locations, p'_{2i} is a tampered pixel, no matter what value p'_{1i} is. Because it is impossible to find a p'_{1i} to make a stego pixel pair (p'_{1i}, p'_{2i}) that can be used to conceal secret data.

3) If the element 'x' corresponding to the stego pixel pair (p'_{1i}, p'_{2i}) is located at the first, second and twelfth types of locations, p'_{1i} is a tampered pixel. It is reason that there is none p'_{2i} to make a stego pixel pair (p'_{1i}, p'_{2i}) legal. In the same reason, p'_{2i} is also a tampered pixel.

Generally, the first and second scenarios are called single tampering, and the third scenario is called combinatorial tampering. Moreover, the above method is summaried in Table 1.

Table 1. Method for determining tampered images

The location of the element 'x'	Tampered image
3,4,5,6,11,13	C_1
7,8,9,10	C_2
1,2,12	C_1 **and** C_2

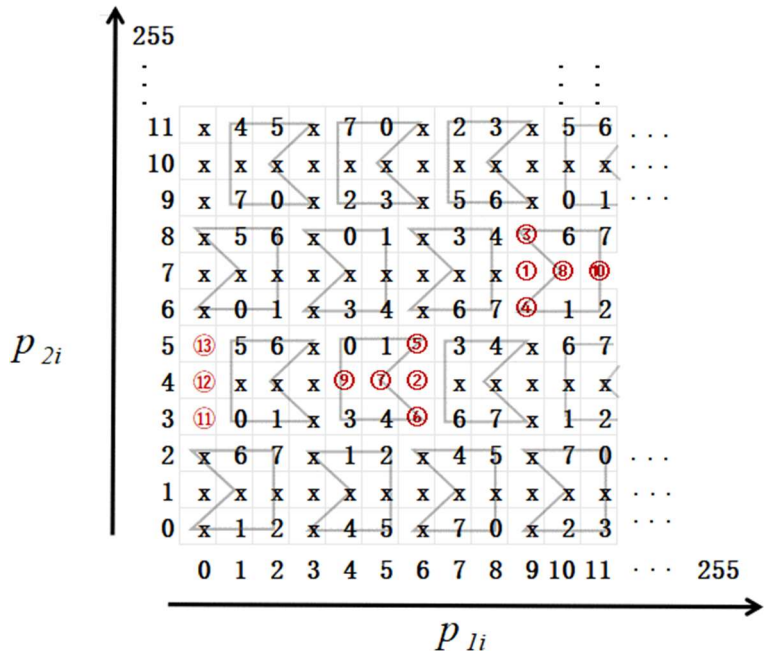


Fig. 10. A part of the hill matrix used for the deception recognition mechanism

Example 2: Assuming the pixel value extracted from the stego images C_1' is 9 and the pixel value extracted from the stego images C_2' is 8. To reconstruct the correct secret data, whether the stego pixel pair (9,8) is legal must be detected uti- lizing the deception recognition mechanism. From Figure 10, it can be observed that the stego pixel pair (9,8) corresponds to the element 'x' in the hill matrix, which means that the deceptive behavior happened. Furthermore, the location of the element 'x' corresponding to the stego pixel pair (9,8) belongs to the third type. According to Table 1, the tampered image is C_1'.

4. Experimental results

Our experimental results are described in this section to demonstrate the feasibility and good performance of the proposed scheme. In Subsection 4.1, the feasibility of the embedding process and data extraction process are demonstrated. Subsection 4.2 presents the effectiveness of the proposed scheme's deception recognition mechanism. In Subsection 4.3, experimental comparisons were conducted with existing schemes.

4.1. Share Generation and Data Extraction

In this Subsection, two pairs of cover images are used to test, each pair with a size of 512×512. As shown in Figure 11, the first pair of cover images are (a)'Airplane' and (c) 'Peppers'. The second pair of cover images are (b)'Tiffany' and (d) 'Baboon'. And 'Barbara' with size of 256×256 is used as the secret image. To coneal the secret image, the image 'Barbara' (as shown in Figure 12) is embedded into each of the two pairs of cover images. Four stego images are generated, as shown in Figure 13(a), (b), (c), (d). And in the recovery process, Figure 14(a), (b) are reconstructed from the two pairs of stego images of Figure 13, respectively. It is clear that the secret image can be embedded into a cover image in the proposed scheme. And the secret image can be recovered losslessly by using correct stego images. The above results validate the feasibility of the proposed scheme.

From Figure 11 and Figure 13, it can be seen that the differences between the cover images and stego images cannot be distinguished by the human eyes. So it can be preliminarily judged that the visual quality of the proposed scheme is good. Furthermore, two metrics are employed to further evaluate the image quality, that is, Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). PSNR is de fined as follows:

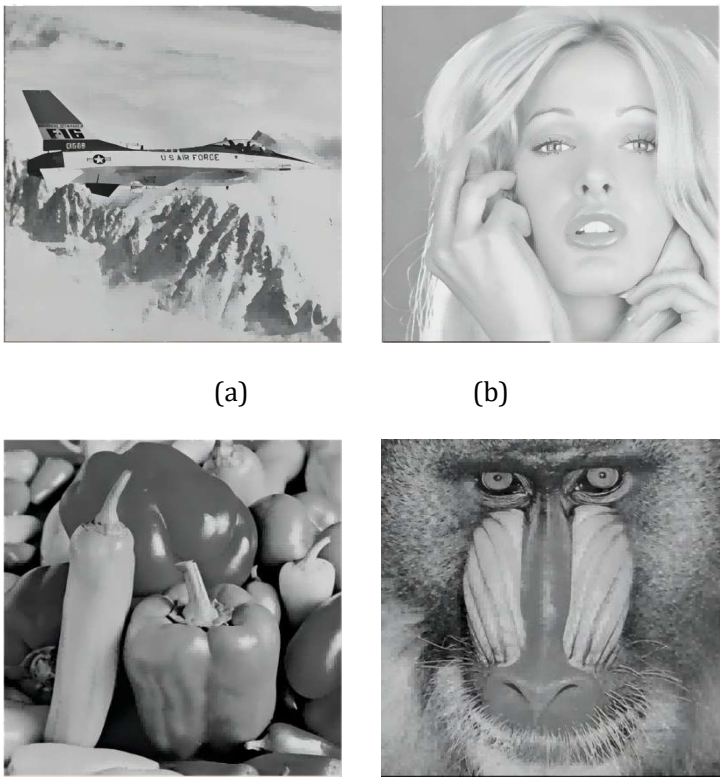
$$PSNR = 10\log_{10}\frac{255^2}{MSE}dB \tag{3}$$

where MSE is the Mean Squared Error between the cover image ck and the stego image s_k, defined as follows:

$$MSE = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(c_k(i,j)-s_k(i,j)\right)^2 \tag{4}$$

As shown in Table 2, the value of PSNR of two tests are within the range of 30 to 50, which indicates visual quality of the proposed scheme is good [33-34]. Additionally, the proposed scheme achieves higher embedding capacity, with an embedding capacity of up to 2,079,152 bits per pair of cover images.

Next, the Structural Similarity Index (SSIM) is used to evaluate the image quality, which evaluates image quality in terms of brightness, contrast, and structure. Compared with PSNR, it provides a more comprehensive evaluation of



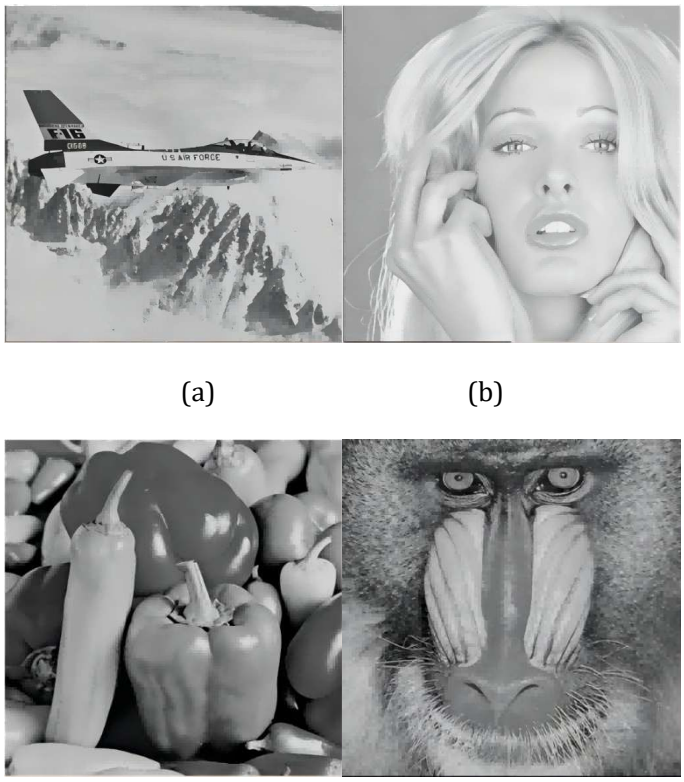
(a) (b)

(c) (d)

(a) The cover image 'Airplane'; (b) The cover image 'Tiffany'; (c) The cover image 'Peppers'; (d) The cover image 'Baboon'

Fig. 11. four cover images

Fig. 12. The secret image 'Barbara'



(a) The stego image 'Airplane'; (b) The stego image 'Tiffany'; (c) The stego image 'Peppers'; (d) The stego image 'Baboon'

Fig. 13. stego images

(a) The recovered secret images from the first pair of stego images; (b) The recovered secret images from the second pair of stego images

Fig. 14. The recovered secret images

image quality, which is similar to the character of human vision in [34]. The SSIM is defined as follows:

$$SSIM(x,y) = [1(x,y) \times c(x,y) \times s(x,y)]^{\alpha} \quad (5)$$

where $I(x,y)$ represents the luminance similarity, $c(x,y)$ represents the contrast similarity, $s(x,y)$ represents the structural similarity, and α is a weighting factor. A higher SSIM value indicates better image quality. When the two images are identical, the corresponding SSIM value is 1. As shown in Table 2, the

average SSIM value for the two tests is close to 1, indicating that the visual quality of the proposed scheme is good.

Table 2. PSNR values of the proposed scheme

	Cover Image 1	Cover Image 2	PSNR (dB)		SSIM		Embedding Capacity (bits)
			stego 1	stego 2	stego 1	stego 2	
test 1	Airplane	Peppers	34.2714	32.1570	0.9930	0.9946	2079152
test 2	Tiffany	Baboon	34.2734	32.1738	0.9812	0.9894	2079152

4.2. Effectiveness of the deception recognition mechanism

In this Subsection, the two pairs of stego images in Figure 13 are used to test the performance of the deception recognition mechanism, which is used in the scenarios of single tampering and combinatorial tampering. To demonstrate the preformance of the mechanism in the single tampering scenario, one stego image is tampered by inserting a small image into a local region, while another image is kept faithful. As shown in Figure 15, the stego image 'Peppers' is tampered by inserting an 64×64 image 'Elaine' in the lower left. The stego image 'Airplane' is kept faithful. The detection results is shown in Figure 15 (c). Similarly, to demonstrate the preformance of the mechanism in the combinatorial tampering scenario, two stego images are tampered by inserting a small image into different regions. As shown in Figure 16, the stego images 'Tiffany' and 'Baboon' are tam- pered by inserting an 64×64 image 'Elaine' into different regions. The detection results are shown in Figure 16(c), (d).

To display the experimental results clearly, the detected deceptive pixel pairs are illustrated by black pixels on the tampered stego image. Furthermore, the detection rate (DR) of the tampered image is calculated based on the following formula:

$$DR = \frac{n}{N(F)'} \tag{6}$$

where $N(F)$ is the number of detected tampered pixel pairs, and n is the number of the detected tampered pixel pairs that can be used to recognize the tampered image. It should be emphasized that in the combinatorial tampering scenario, n is the number of the detected tampered pixel pairs that can be used to recognize two tampered images simultaneously. Based on the above settings, the

(a) (b) (c)

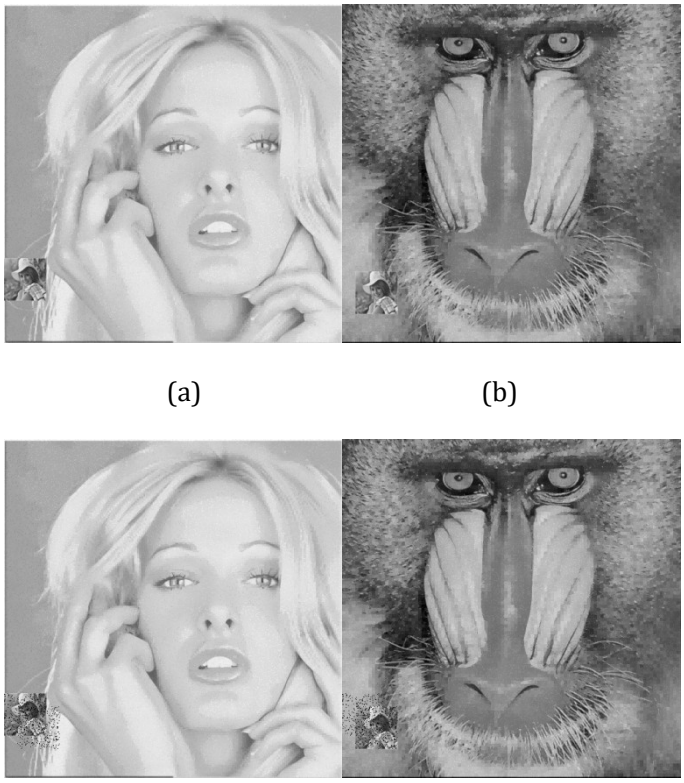
(a) Faithful Image 'Airplane'; (b) Tampered Image 'Peppers'; (c) Detection Mechanism Result

Fig. 15. The Deception recognition mechanism experiment of single tampering

experimental results in the two scenarios are obtained. In the single tampering scenario, the tampered image can be completely detected. And since the another stego image is not tampered, the tampering detection rate for the another stego image is zero. In the combinatorial tampering scenario, although it is a challenging issue to detected two tampered images simultaneously, the detection rate of both tampered images can still reach 13% in the proposed mechanism. The above results indicate that the deception recognition mechanism in the proposed scheme achieves better performance.

4.3. Comparisons

In terms of embedding capacity, the proposed scheme is compared with the schemes of Liu [29] and Li [30]. To make a fair comparison, the same cover images with a size of 512×512 and secret image with a size of 256×256 are used. As shown in Table 3, each cover pixel pair is exploited to conceal eight secret bits and the maximum embedding capacity of cover image is 2,097,152 bits.



(a) (b)

(c) (d)

(a) Tampered Image 'Tiffany'; (b) Tampered Image 'Baboon'; (c) Detection Mechanism Result; (d) Detection Mechanism Result

Fig. 16. The Deception recognition mechanism experiment of combinatorial tampered

in the proposed scheme. By comparison, in the schemes proposed by Liu [29] and Li [30], each cover pixel pair is exploited to embed four bits and six bits of secret data, respectively. And it is clearly that the maximum embedding capacity of these two schemes are lower than that of the proposed scheme. Therefore, the proposed scheme achieves a higher embedding capacity.

Table 3. Comparison of the proposed scheme with two existing schemes

scheme	Embedded bit	Embedded capacity (bit)	Number of modifi cations	embedding capacity of per pixel pair
Liu et al.'s scheme [29]	524288	1048576	131072	4
Li's scheme [30]	524288	1572864	87382	6
proposed scheme	524288	2097152	65536	8

Moreover, in terms of deception recognition mechanism, the proposed scheme is compared with the maze matrix-based scheme [32]. In the maze matrix, elements corresponding legal hiding locations occupy approximately 52% of the entire maze matrix, meaning that the highest detection rate of deceptive behavior is approximately 48%. However, in the hill matrix, elements corresponding legal hiding locations occupy approximately 44% of the entire hill matrix, meaning that the highest detection rate of deceptive behavior is approximately 56%. It is obvious that the proposed scheme achieves a higher detection rate of deceptive behavior than that of the maze matrix-based scheme [32] in theory.

Furthermore, for the experimental comparison, the results are shown in Table 4, where the detection rate of tampered image is calculated using formula 6. In Table 4, it can be observed that when a single tampering occurs, the DR of tampered image in the proposed scheme is 100%, which is better than the DR of the maze matrix-based scheme [32]. The reason is that in the single tampering scenario, the illegal hiding locations are always located in an entire 'x' row or an entire 'x' column in the proposed scheme. And when a combinatorial tampering occurs, the detection rate of tampered images in the proposed scheme is 13%, while the detection rate in the maze matrix-based scheme [32] is 5.5%. This result is because both tampered images can only be detected while the element 'x' is located at the first, second and twelfth types of locations in the proposed scheme. Similarly, in the maze matrix, both tampered images can only be recognized while the mapped element simultaneously lies at the horizontal and vertical gaps. From the above results, it can be seen that in both single tampering and combinatorial tampering, the performance of the proposed deception recognition mechanism outperforms that of the maze matrix-based scheme [32].

Table 4. Comparison of the proposed scheme with the maze matrix based scheme

scheme	DR	
	Tampering a single	Tampering a pair
Maze scheme [32]	46 %	5.5 %
proposed scheme	100 %	13 %

5. Conclusion

In this paper, we proposed a secret image sharing scheme with improved embedding capacity and a deception recognition mechanism. A hill matrix is designed as a reference matrix. Meanwhile, a location table and a location pair table are constructed. Leveraging the mapping of the hill matrix and location table, a series of candidate stego pixel pairs are generated. Then, according to the guidance of the location pair table, each cover pixel pair is exploited to conceal eight bits of secret data and a unique stego pixel pair is determined. Furthermore, based on the special construction of the hill matrix, a deception recognition mechanism is designed. This mechanism can detect deceptive behavior. And it can identify tampered images based on the data hiding locations without the information from other participants. The

experimental results indicate that the proposed scheme outperforms existing methods in terms of embedding capacity and deception recognition mechanism.

Funding

This research was supported by the National Natural Science Foundation of China (No. 12061027); Doctoral Research Foundation of Guilin University of Technology (No. GUTQDJJ2007027).

References

[1] Fei-Fei Qian, Nuo Xu, and Wan-Li Lyu. High capacity reversible data hiding scheme based on interpolation and tetris matrix. In 2022 41st Chinese Control Conference (CCC), pages 7471–7478. IEEE, 2022.

[2] Liaojun Pang, Deyu Miao, Huixian Li, Qiong Wang, et al. Improved secret image sharing scheme in embedding capacity without underflow and overflow. The Scientific World Journal, 2015, 2015.

[3] Hamidreza Rashidy Kanan and Bahram Nazeri. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert systems with applications, 41(14):6123– 6130, 2014.

[4] Xuehu Yan, Lintao Liu, Yuliang Lu, and Qinghong Gong. Security analysis and classification of image secret sharing. Journal of Information Security and Applications, 47:208–216, 2019.

[5] John Blesswin, Christhu Raj, and Rajeev Sukumaran. Enhanced semantic visual secret sharing scheme for the secure image communication. Multimedia Tools and Applications, 79:17057–17079, 2020.

[6] Lein Harn and Ching-Fang Hsu. Dynamic threshold secret reconstruction and its application to the threshold cryptography. Information Processing Letters, 115(11):851–857, 2015.

[7] Lifeng Yuan, Mingchu Li, Cheng Guo, Weitong Hu, Xinjian Luo, et al. Secret image sharing scheme with threshold changeable capability. Mathematical Problems in Engineering, 2016, 2016.

[8] Ji-Hwei Horng, Shuying Xu, Ching-Chun Chang, and Chin-Chen Chang. An efficient data-hiding scheme based on multidimensional mini-sudoku. Sensors, 20(9):2739, 2020.

[9] Kai Gao, Ji-Hwei Horng, Yanjun Liu, and Chin-Chen Chang. A reversible secret image sharing scheme based on stick insect matrix. Ieee Access, 8:130405– 130416, 2020.

[10] Arjun Singh Rawat, Maroti Deshmukh, and Maheep Singh. Meaningful shares based single secret sharing scheme using chinese remainder theorem and xor operation. In 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), pages 597–602. IEEE, 2023.

[11] Bishoy K Sharobim, Marwan A Fetteha, Salwa K Abd-El-Hafiz, Wafaa S Sayed, Lobna A Said, and Ahmed G Radwan. An efficient multi-secret image sharing system based on chinese remainder theorem and its fpga realization. IEEE Access, 11:9511–9520, 2023.

[12] Moni Naor and Adi Shamir. Visual cryptography. In Advances in CryptologyEUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13, pages 1–12. Springer, 1995.

[13] Young-Chang Hou. Visual cryptography for color images. Pattern recognition, 36(7):1619–1629, 2003.

[14] Jinu Mohan and R Rajesh. Enhancing home security through visual cryptography. Microprocessors and Microsystems, 80:103355, 2021.

[15] Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612– 613, 1979.

[16] George Robert Blakley. Safeguarding cryptographic keys. In Managing Requirements Knowledge, International Workshop on, pages 313–313. IEEE Computer Society, 1979.

[17] Chih-Ching Thien and Ja-Chen Lin. Secret image sharing. Computers & Graphics, 26(5):765–770, 2002.

[18] Zhen Wu, Yining Liu, and Xingxing Jia. A novel hierarchical secret image sharing scheme with multi-group joint management. Mathematics, 8(3):448, 2020.

[19] Zhifang Zhang, Yeow Meng Chee, San Ling, Mulan Liu, and Huaxiong Wang. Threshold changeable secret sharing schemes revisited. Theoretical Computer Science, 418:106–115, 2012.

[20] Lifeng Yuan, Mingchu Li, Cheng Guo, Kim-Kwang Raymond Choo, and Yizhi Ren. Novel threshold changeable secret sharing schemes based on polynomial interpolation. PloS one, 11(10):e0165512, 2016.

[21] Yan-Xiao Liu, Ching-Nung Yang, Chi-Ming Wu, Qin-Dong Sun, and Wei Bi. Threshold changeable secret image sharing scheme based on interpolation polynomial. Multimedia Tools and Applications, 78:18653–18667, 2019.

[22] Rama Singh, Saumya Patel, and Ankita Vaish. Secure most significant bit plane compression based reversible data hiding in encrypted image technique using huffman ciphersystem. Journal of Electronic Imaging, 33(1):013020–013020, 2024.

[23] K Ma, Weiming Zhang, Xianfeng Zhao, and Nenghai Yu. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Transactions on Information Forensics and Security, 8(3):553–562, 2014.

[24] Yi Puyang, Zhaoxia Yin, and Zhenxing Qian. Reversible data hiding in encrypted images with two-msb prediction. IEEE, 2018.

[25] R. Agarwal, A. Vaish, and M. Kumar. Odd-even discrimination-based reversible data hiding technique in encrypted images. Journal of Electronic Imaging, 32:013032 – 013032, 2023.

[26] Yi-Hui Chen, Jia-Ye Lee, Min-Hsien Chiang, and Shih-Hsin Chen. Verifiable (2, n) image secret sharing scheme using sudoku matrix. Symmetry, 14(7):1445, 2022.

[27] Mingze He, Yanjun Liu, Chin-Chen Chang, and Mingxing He. A minisudoku matrix-based data embedding scheme with high payload. IEEE Access, 7:141414–141425, 2019.

[28] Ching Chun Chang, Yanjun Liu, and Thai Son Nguyen. A novel turtle shell based scheme for data hiding. In 2014 tenth international conference on intelligent information hiding and multimedia signal processing, pages 89–93. IEEE, 2014.

[29] Yanjun Liu, Ching-Chun Chang, and Thai-Son Nguyen. High capacity turtle shell-based data hiding. IET Image Processing, 10(2):130–137, 2016.

[30] Xiao-Shuang Li, Chin-Chen Chang, Mingxing He, and Chia-Chen Lin. Secure high capacity data hiding scheme based on reference matrix. Int. J. Netw. Secur., 21(6):918–929, 2019.

[31] Yanjun Liu, Chin-Chen Chang, and Peng-Cheng Huang. Security protection using two different image shadows with authentication. Math. Biosci. Eng, 16(4):1914–1932, 2019.

[32] Ching-Chun Chang, Ji-Hwei Horng, Chia-Shou Shih, and Chin-Chen Chang. A maze matrix-based secret image sharing scheme with cheater detection. Sensors, 20(13):3802, 2020.

[33] Zhou Wang and Alan C Bovik. A universal image quality index. IEEE signal processing letters, 9(3):81–84, 2002.

[34] Yusra Al-Najjar and Der Chen. Comparison of image quality assessment: Psnr, hvs, ssim, uiqi. International Journal of Scientific and Engineering Research, 3(8):1–5, 2012.