symmetry

Article

Research on Image Steganography Based on Sudoku Matrix

Tsung-Chih Hsiao [1,2], Dong-Xu Liu [1,2], Tzer-Long Chen [3,*] and Chih-Cheng Chen [4,5,*]

[1] College of Computer Science and Technology, Huaqiao University, Quanzhou 361021, China; hsiaotc@hqu.edu.cn (T.-C.H.); 19934083001@hqu.edu.cn (D.-X.L.)
[2] Xiamen Key Laboratory of Data Security and Blockchain Technology, Huaqiao University, Quanzhou 361021, China
[3] Department of Finance, Providence University, Taichung 43301, Taiwan
[4] Department of Automatic Control Engineering, Feng Chia University, Taichung 40724, Taiwan
[5] Department of Aeronautical Engineering, Chaoyang University of Technology, Taichung 413310, Taiwan
* Correspondence: tlchen1976@pu.edu.tw (T.-L.C.); ccc@gm.cyut.edu.tw (C.-C.C.)

Abstract: At present, the Sudoku matrix, turtle shell matrix, and octagonal matrix have been put forward according to the magic matrix-based data hiding methods. Moreover, the magic matrices to be designed depend on the size of the embedding capacity. In addition, by determining the classification of points of pixel pairs after applying a magic matrix and by determining the traversal area, the average peak signal-to-noise ratio (PSNR) can be improved. Therefore, this topic intends to propose a data hiding method based on a 16 × 16 Sudoku matrix by using the 16 × 16 Sudoku matrix and extending it to a double-layer magic matrix. Low-cost data embedding methods are also studied, in order to improve the PSNR and maintain good image quality with the same embedding capacity.

Keywords: data hiding; magic matrix; double-layer

Citation: Hsiao, T.-C.; Liu, D.-X.; Chen, T.-L.; Chen, C.-C. Research on Image Steganography Based on Sudoku Matrix. *Symmetry* **2021**, *13*, 387. https://doi.org/10.3390/sym13030387

Academic Editor: Charles Tijus, Teen-Hang Meen and Jih-Fu Tu

Received: 31 January 2021
Accepted: 23 February 2021
Published: 27 February 2021

1. Introduction

The development and popularization of Internet technology make the exchange and dissemination of information easy and allows people to get information from all over the world by just clicking a button. However, there are increasing concerns about information security. A great deal of information is transmitted over the Internet, and everyone's privacy may be accessed or stolen by others. At present, it is a common phenomenon that the information and privacy of individuals, companies, and governments are leaked.

The Internet provides a public and convenient channel for exchanging information; however, the security becomes a critical issue on the Internet. Especially, the illegal users on the Internet may retrieve, intercept, camouflage, or copy the information on transferring. Fortunately, the steganography technology provides practical solutions for exchanging secret message on the Internet. At present, information hiding technology play an increasingly more important role in government, military intelligence, financial systems, and the area of medical and health. It is also widely used in secret communications, digital copyright protection, e-commerce security, data integrity, reliability validation, and so on [1,2].

With the rapid development of Computer Science and Internet Technology and the advent of era for Big Data, increasing amounts of digital information (image, text, video, audio, etc.) will be frequently transmitted in the network, causing the protection of digital information security becomes very prominent. Traditional information encryption technology can effectively protect the security of digital information, while the information hiding technology can achieve copyright protection, tamper detection, access control, authentication, and other security features by hiding secret information in the digital information. The combination of information encryption technology and information hiding technology, which hides information in encrypted information, can guarantee digital information security and effective management and control for digital information. Information hiding technology in encrypted domain plays an important role in the information security field for its superiority [3]. There is vivid research on securely delivering a secret message by using a data hiding technique in digital images. Different from cryptography, which requires secret information to be encrypted, this technology usually protects secret information by hiding it into standard images. Because the stego-images are mixed with numerous social images on the Internet, it is hard to attract the attention of the attackers. The most concerning performance indicators of steganography are embedding capacity and stego-image quality. Traditional steganography schemes usually lack flexibility or have the problem of the low quality of stego-image [4–6]. In recent years, achieving higher steganography capacity and quality of stego-image has become a hot research topic.

The rapid development of the Internet also faces serious security problems, such as illegal eavesdropping, interception, and malicious tampering with data. Researchers are paying increasingly more attention to relevant information in the security field. As an important branch in the field of information security, data hiding is a technology that embeds the important secret message into common used digital multimedia data, such as audio, text, image, and video, and aims to make the transmission of secret message invisible. However, compared with the traditional cryptography, the research on data hiding technology is still in an emerging stage. There are still many key problems that need to be explored and solved. Therefore, it is of great significance and value to study efficient data hiding techniques.

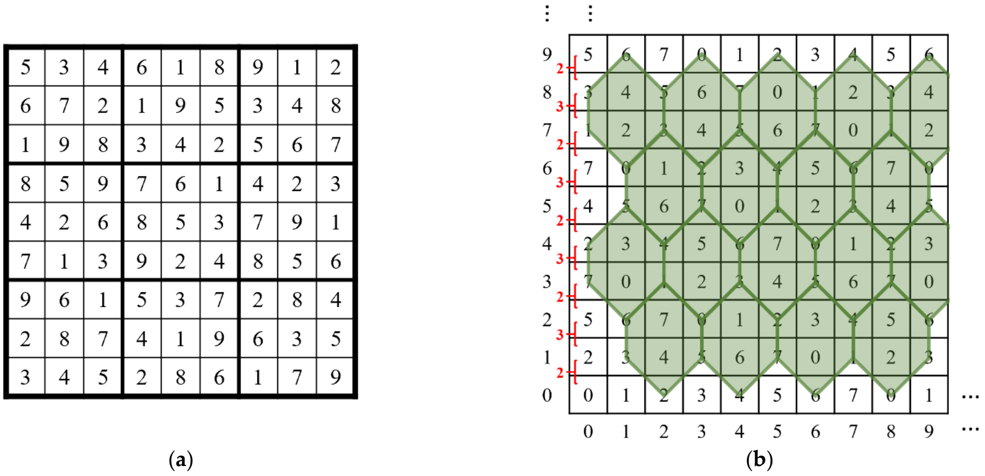
Sudoku-based data hiding technology is a novel data hiding method in recent years. It begins from the mathematical characteristics of Sudoku and makes data hiding algorithms based on it with higher security. This paper presents a high-capacity data hiding scheme based on the Sudoku game, which expands the usage of Sudoku, not only as a reference matrix for data hiding, but also participating in the data hiding algorithm. On the other hand, it also increases hiding capacity and improves data hiding algorithm security which can prevent violent crackdown more effectively. The data hiding algorithm can also promote the use of other different order of the Sudoku matrix, so it has good scalability and adaptability.

2. Research Status

The existing data hiding techniques mainly focus on three domains: frequency domain, compression domain, and spatial domain. In the frequency domain, because most of the digital images in Internet are compressed, the transform domain is used to hide secret message on these compressed images. However, many block-based data hiding schemes are proposed on the spatial domain but cannot be applied directly to the transform domain. A block-based high-capacity reversible data hiding scheme for JPEG images is proposed. After studying the algorithm characteristics of Hamming code and histogram shift, our scheme combines them and achieves the purpose of making full use of AC coefficient in DCT block [4,7] or the discrete wavelet transform (DWT) coefficients [8,9], in which the secret data are embedded. The scheme improves the embedding capacity and maintains a good visual quality, and, more importantly, has good security (hard to perceive by third parties). It also can use different quality factors to meet the user's different hidden needs. If the sender has a larger number of secret bits to hide, it selects a lower quality factor for compression image. If the sender needs a stego image that has a higher visual quality to avoid being suspected by third-party eavesdroppers, a higher quality factor should be a better choice. Some researchers have proposed the data hiding scheme based on vector quantization (VQ) compression [10–13]. The data hiding scheme based on side match vector quantization (SMVQ) and search-order code (SOC) is proposed. In this scheme, the VQ image is compressed by SMVQ technology to reduce redundancy, and then the image is recompressed by SOC. In the embedding process, the embedding capacity of image is changed dynamically by threshold to meet different embedding capacity requirements. The experimental results show that the proposed scheme can improve the embedding capacity and reduce the image distortion.

In the spatial domain, there are about three types of schemes: the least significant bit (LSB) substitution [14–19], the exploiting modification direction (EMD) [20–22], and the magic matrix-based (MMB) schemes [23–33]. In 1996, Bender et al. first proposed that LSB was the most common scheme [3]. Wang et al. [14] proposed an optimal LSB substitution algorithm to improve the image quality and a genetic algorithm to solve the huge computation issue, with an embedding capacity of 1 bit per pixel (bpp). The LSB substitution algorithm is very simple, but the hidden data can be easily detected [16]. Mielikainen et al. [15] improved the LSB matching method and embedded data in pairs by modifying the parity check, with an embedding capacity of 1 bpp. In recent years, Sahu et al. [17–19] proposed some new data hiding methods based on LSB to further improve the embedding capacity. Zhang and Wang et al. [20] fully exploited the modification direction to embed one secret (2n + 1)-bit digit into a vector with n pixels by changing at most one LSB of one pixel.

Unlike the above methods, several kinds of image steganography based on MMB have been put forward in the last few years. In 2008, Chang et al. [23] proposed a novel data hiding scheme using Sudoku. This scheme takes pixel pairs as the coordinates of a Sudoku matrix to specify the value to embed one 9-bit digit into each pixel pair, with an embedding capacity of 1.5 bpp. Figure 1a shows an example matrix of this scheme. Most image data hiding schemes divide the original cover image into non-overlapping small blocks and then use each block idea; the space complexity of the data hiding algorithm can be reduced; the algorithm is more concise, efficient, easy to implement, and convenient for future modification and optimization; and more importantly, it is more suitable for the complicated network environment. In order to design a more efficient data hiding scheme, this paper studies a large number of data hiding schemes and related knowledge, then proposes two image data hiding algorithms based on blocks with higher embedding capacity [23–26]. This scheme can maintain an embedding capacity of 1.5 bpp with less distortion, and Figure 1b is an example matrix of this scheme. In 2016, Liu's method can maintain good image quality with an average peak signal-to-noise ratio (PSNR) of 41.87dB when the embedding capacity is up to 2.5 bpp [27–29]. This scheme improves the embedding capacity and maintains a good visual quality, and, more importantly, has good security (hard to perceive by third parties). It can also use different quality factors to meet the user's different hidden needs. If the sender has larger number of secret bits to hide, a lower quality factor for the compression image should be selected. If the sender needs a stego-image with a higher visual quality to avoid being suspected by third-party eavesdroppers, a higher quality factor should be a better choice. In 2018, Xie et al. [30] put forward a two-layer turtle shell matrix-based data embedding method, which added one layer of matrix with the turtle shell as a cell based on the turtle shell matrix-based data hiding method proposed by Chang et al. [26] maintained an embedding capacity up to 2.5 bpp and achieved larger embedding capacity and high image quality with a PSNR of 47.12dB. In recent years, the mini-Sudoku matrix-based data hiding schemes [31–33] have also been proposed. In 2019, He et al. [31] proposed a mini-Sudoku matrix-based image steganographic scheme which could reach an embedding capacity of 2 bpp and a PSNR of 46.37dB. In 2020, Horng et al. [32] proposed a cubic mini-Sudoku matrix-based image steganographic method in which the algorithm uses a cubic magic cube at the plane matrix stage. In the same year, Chen et al. [33] put forward a multi-layer mini-Sudoku matrix-based data hiding method, which showed an embedding capacity up to 3 bpp and a PSNR of 40.01 dB.



5	3	4	6	1	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

(**a**)

⋮	⋮										
9	5	6	7	0	1	2	3	4	5	6	
8	3	4	5	6	7	0	1	2	3	4	
7	1	2	3	4	5	6	7	0	1	2	
6	7	0	1	2	3	4	5	6	7	0	
5	4	5	6	7	0	1	2	3	4	5	
4	2	3	4	5	6	7	0	1	2	3	
3	7	0	1	2	3	4	5	6	7	0	
2	5	6	7	0	1	2	3	4	5	6	
1	2	3	4	5	6	7	0	1	2	3	
0	0	1	2	3	4	5	6	7	0	1	⋯
	0	1	2	3	4	5	6	7	8	9	⋯

(**b**)

Figure 1. (**a**) Example of 9 × 9 Sudoku Matrix. (**b**) Example of Turtle Shell Matrix.

3. Research Methods

In terms of the data embedding method that employs magic matrices, the key to improving the embedding capacity and the image quality lies in the construction of a magic matrix and the conditions of a traversal area. The general objective of this topic is to improve the embedding capacity while maintaining good image quality. Specifically, taking the previous research as the basis, this topic studies the construction of a magic matrix and the conditions of a traversal area.

3.1. Research Plan

This topic is based on the magic matrix-based data hiding methods. In most magic matrix-based data hiding methods, Sudoku matrix, turtle shell matrix, octagonal matrix, and other matrices with constraints are used. In this research, in order to improve the embedding capacity, a 16 × 16 Sudoku matrix will be used for data hiding.

The magic matrix-based data hiding method is a novel method proposed in recent years. According to this method, the magic matrix construction information, embedded images, and binary ciphertext should be input. First, the binary ciphertext is converted to a string as required by the method. For example, in the turtle shell matrix-based data hiding method, every three-bit binary ciphertext is converted to an octal ciphertext, and a corresponding magic matrix is generated according to the magic matrix construction information. Second, data is embedded; two-bit consecutive pixels in the image are read; the traversal area and method are determined by classifying the corresponding points on the magic matrix; the ciphertext value to be embedded is found in the traversal area; and the pixel pairs in the original image are modified as the coordinates of the ciphertext value, which is looped according to the length of the ciphertext until the end of the ciphertext or the pixels in the image are all modified; and the stego-image is output in the end.

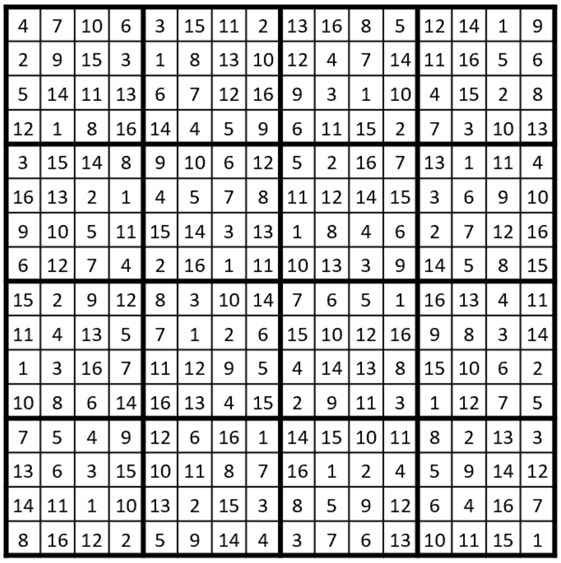
With the magic matrix-based data hiding methods, decoding becomes easy. After the stego-image and magic matrix are input, the ciphertext can be extracted from the magic matrix based on the pixel pairs of the stego-image.

3.1.1. Design of Magic Matrices

The design of magic matrices is one of the focuses of this topic. The 9 × 9 Sudoku matrix, turtle shell matrix, octagonal matrix, and other matrices with diverse shapes and constraints have been proposed. Magic matrices are constructed by referring to the existing mathematical magic matrices or based on the matrices designed by researchers.

1. 16 × 16 Sudoku matrix

A 16 × 16 Sudoku matrix is a magic matrix developed from a 4 × 4 magic matrix by adding conditions and complexity. Moreover, a Sudoku matrix can generate countless combination patterns. It is not easy to decode and then extract the steganographic content even if the Sudoku matrix-based image steganography is identified. Therefore, the security of such an algorithm is relatively high. Figure 2 is an example of the 16 × 16 Sudoku matrix.

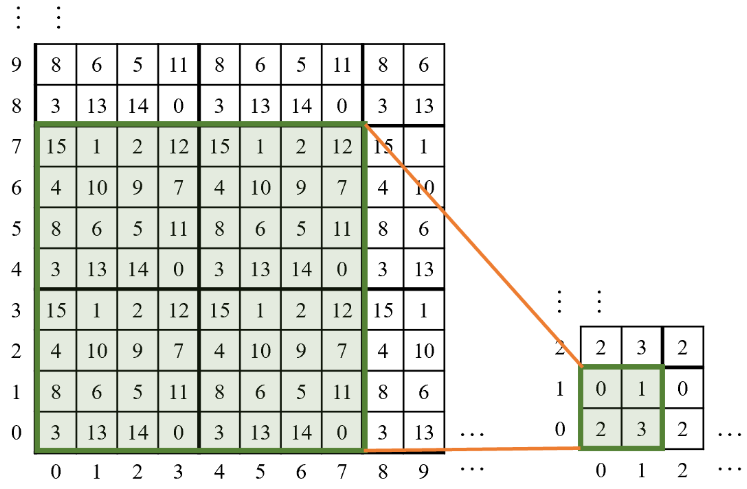


4	7	10	6	3	15	11	2	13	16	8	5	12	14	1	9
2	9	15	3	1	8	13	10	12	4	7	14	11	16	5	6
5	14	11	13	6	7	12	16	9	3	1	10	4	15	2	8
12	1	8	16	14	4	5	9	6	11	15	2	7	3	10	13
3	15	14	8	9	10	6	12	5	2	16	7	13	1	11	4
16	13	2	1	4	5	7	8	11	12	14	15	3	6	9	10
9	10	5	11	15	14	3	13	1	8	4	6	2	7	12	16
6	12	7	4	2	16	1	11	10	13	3	9	14	5	8	15
15	2	9	12	8	3	10	14	7	6	5	1	16	13	4	11
11	4	13	5	7	1	2	6	15	10	12	16	9	8	3	14
1	3	16	7	11	12	9	5	4	14	13	8	15	10	6	2
10	8	6	14	16	13	4	15	2	9	11	3	1	12	7	5
7	5	4	9	12	6	16	1	14	15	10	11	8	2	13	3
13	6	3	15	10	11	8	7	16	1	2	4	5	9	14	12
14	11	1	10	13	2	15	3	8	5	9	12	6	4	16	7
8	16	12	2	5	9	14	4	3	7	6	13	10	11	15	1

Figure 2. Example of 16 × 16 Sudoku matrix.

2. Double-layer magic matrix

The double-layer magic matrix is a method to improve the embedding capacity while maintaining good image quality. With the same embedding capacity, this method narrows the traversal area when compared with the image steganography with a one-layer magic matrix and is more applicable due to the properties of a magic matrix. Figure 3 is an example of a 4-2 double-layer magic matrix with a 4 × 4 magic matrix as the first layer and a 2 × 2 magic matrix as the second layer.



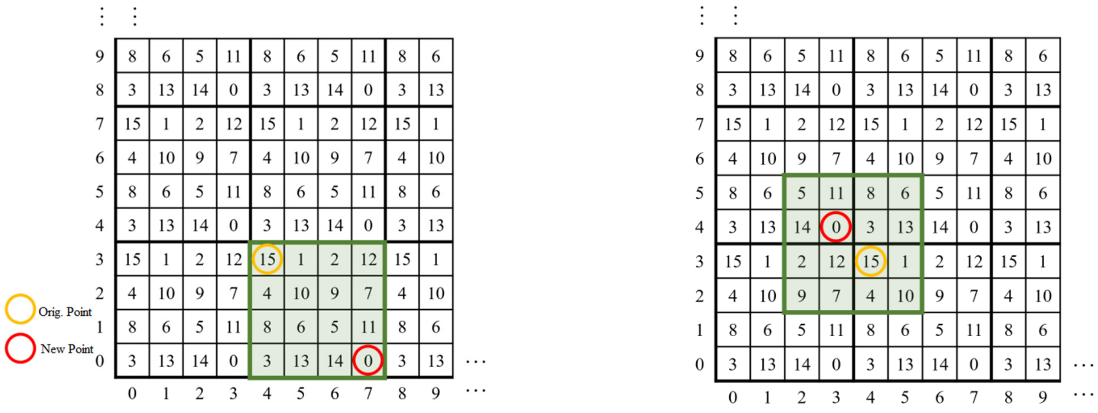
⋮	⋮										
9	8	6	5	11	8	6	5	11	8	6	
8	3	13	14	0	3	13	14	0	3	13	
7	15	1	2	12	15	1	2	12	15	1	
6	4	10	9	7	4	10	9	7	4	10	
5	8	6	5	11	8	6	5	11	8	6	
4	3	13	14	0	3	13	14	0	3	13	
3	15	1	2	12	15	1	2	12	15	1	
2	4	10	9	7	4	10	9	7	4	10	
1	8	6	5	11	8	6	5	11	8	6	
0	3	13	14	0	3	13	14	0	3	13	…
	0	1	2	3	4	5	6	7	8	9	…

⋮	⋮			
2	2	3	2	
1	0	1	0	
0	2	3	2	…
	0	1	2	…

Figure 3. Example of 4-2 double-layer magic matrix.

3.1.2. Determination of Traversal Area

The traversal area is an area determined by the structure and construction constraints of a magic matrix. All values in the area, and how to search the closest satisfactory point, need to be considered in its design. For example, the methods for determining the traversal area in the 4 × 4 magic matrix-based data hiding method are shown in Figure 4a,b. The construction constraints of a 4 × 4 magic matrix are that the column sum, row sum, and diagonal sum are all 30. This magic matrix as the basic magic matrix fills in loops to generate a 256 × 256 matrix. This magic matrix is used to simulate the process of hiding the ciphertext 0 from the pixel pair $p(4,3)$. In Figure 4a, the basic magic matrix serves as the traversal area for data hiding, and a new pixel pair $p'(7,0)$ is got as an outcome. The PSNR, in this case, is 38.59dB. In Figure 4b, the 4 × 4 area where the origin is located on the inside lower right serves as the traversal area for data hiding, and a new pixel pair $p'(3,4)$ is obtained as an outcome. The PSNR, in this case, is 48.13. The determination of the traversal area depends on the image quality.



⋮	⋮										
9	8	6	5	11	8	6	5	11	8	6	
8	3	13	14	0	3	13	14	0	3	13	
7	15	1	2	12	15	1	2	12	15	1	
6	4	10	9	7	4	10	9	7	4	10	
5	8	6	5	11	8	6	5	11	8	6	
4	3	13	14	0	3	13	14	0	3	13	
3	15	1	2	12	15	1	2	12	15	1	
2	4	10	9	7	4	10	9	7	4	10	
1	8	6	5	11	8	6	5	11	8	6	
0	3	13	14	0	3	13	14	0	3	13	…
	0	1	2	3	4	5	6	7	8	9	…

(**a**)

⋮	⋮										
9	8	6	5	11	8	6	5	11	8	6	
8	3	13	14	0	3	13	14	0	3	13	
7	15	1	2	12	15	1	2	12	15	1	
6	4	10	9	7	4	10	9	7	4	10	
5	8	6	5	11	8	6	5	11	8	6	
4	3	13	14	0	3	13	14	0	3	13	
3	15	1	2	12	15	1	2	12	15	1	
2	4	10	9	7	4	10	9	7	4	10	
1	8	6	5	11	8	6	5	11	8	6	
0	3	13	14	0	3	13	14	0	3	13	…
	0	1	2	3	4	5	6	7	8	9	…

(**b**)

Figure 4. (**a**) Basic magic matrix as traversal area. (**b**) Traversal area with origin on the inside lower right.

3.2. Evaluation Methods

The main evaluation criteria of magic matrix-based data hiding methods are visual effect, embedding capacity (EC), and average peak signal-to-noise ratio (PSNR).

1. Visual effect

The visual effect is the contrast between the original image and the stego-image through human eyes. The contrast mainly depends on the color difference, degree of difference, and other details of images to check traces of data embedding. Figure 5 displays the image contrast according to the 4 × 4 magic matrix-based data hiding method, in which the images are sourced from the USC-SIPI Image Database [34], and the images in the green box are stego-images.

2. Embedding rate (ER)

The embedding rate in bpp (bit per pixel) is used to calculate the size of binary ciphertext data that can be embedded into a pixel. The embedding rate is calculated according to Equation (1), where H is the image height, W is the image width, and S is the size of binary ciphertext.

$$ER = \frac{|S|}{H \times W} \tag{1}$$

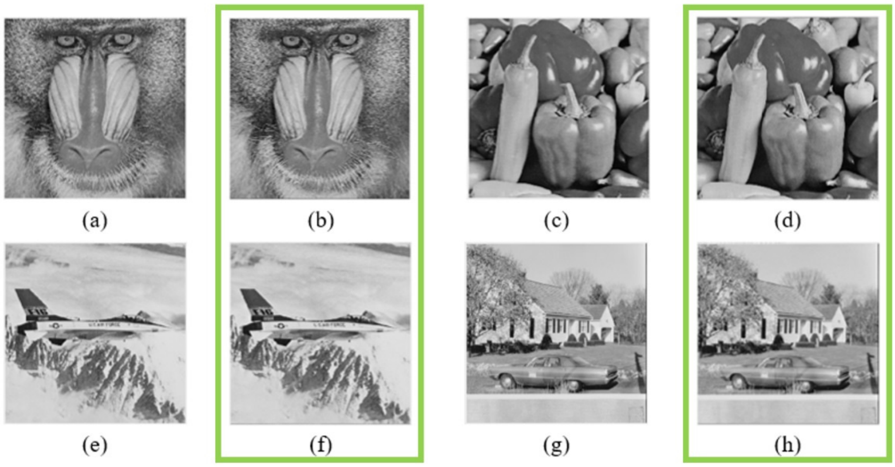


Figure 5. Image contrast according to 4 × 4 magic matrix-based data hiding method, with stego-images displayed in green box; they should be listed as (**a**) original image of baboon, (**b**) stego-image of (**a**), (**c**) original image of pepper, (**d**) stego-image of (**c**), (**e**) original image of airplane, (**f**) stego-image of (**e**), (**g**) original image of house, and (**h**) stego-image of (**g**).

3. Peak signal-to-noise ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) refers to the parameter for evaluating the difference between the carrier image and the hidden image; it is also one of the most important indicators for evaluating the performance of an image information hiding scheme. An image's PSNR is defined by the Mean Square Error (MSE) of the pixels of the carrier image and the hidden image. For example, for an M × N grayscale image, its MSE is defined as shown in Equation (2). The PSNR can reflect, to a certain extent, the change of the carrier image before and after the information hiding operation. The higher the PSNR value, the smaller the difference between the carrier image and the hidden image, that is, the better the performance of the image information hiding algorithm. On the contrary, the smaller the PSNR value, the greater the difference between the carrier image and the hidden image, indicating that the higher the distortion of the image, the easier it is to be detected by the human visual system. In general, when the PSNR value exceeds 30dB, it can be considered that there is no visual difference between the carrier image and the hidden image.

The PSNR is used to evaluate the image quality of the stego-image by comparing the original image with the stego-image by computer. PSNR is calculated according to Equation (3), where MSE is the mean squared error. In Equation (2), $I(i,j)$ is the pixel in row i, column j in the original image and $I'(i,j)$ is the pixel in row i, column j in the stego-image.

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

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE} \right) \tag{3}$$

Equation (3) demonstrates that in 8-bit grayscale images (signal sequences), each pixel (signal) may output a value in the range of 0 to 255. Each image is only a case in the 8-bit grayscale image. If the range of pixel values is fixed for each image, then the result is no longer an 8-bit grayscale image, but the experimental results of the image within that range.

4. Experimental Analysis

To perform the experiment, Matlab 2018a, AMD3700X (CPU), and RTX 2070 super (GPU) are used. The experimental images are grayscale images of 512 × 512 pixels.

This paper studies the information embedding and extracting based on the encrypted domain information hiding and proposes the tag-based encrypted domain information embedding and extracting algorithm. We analyze each algorithm by simulation to compare their effectiveness, security, and so on. Besides, this paper implements the Information embedding and extracting to evaluate its function and performance.

4.1. Turtle Shell Magic Matrix-Based Image Steganography

Four images are processed by steganography. According to the experimental results, this scheme can achieve an embedding capacity of 1.5 bpp and a PSNR of 49.76dB. There are two other steganographic schemes that can change the traversal area. The experimental results of the turtle shell magic matrix-based image steganography are listed in Table 1.

Table 1. Experimental results of turtle shell magic matrix-based image steganography.

Cover Image	Chang et al.′s Scheme (TDH)		Low-Com-Cost-2020		Low-Com-Cost_TS	
	EC (bpp)	PSNR (dB)	EC (bpp)	PSNR (dB)	EC (bpp)	PSNR (dB)
Airplane	1.5	49.76	1.5	50.17	1.5	49.2
Baboon	1.5	49.76	1.5	50.17	1.5	49.2
Boat	1.5	49.76	1.5	50.17	1.5	49.24
House	1.5	49.75	1.5	50.17	1.5	49.2
Paper	1.5	49.76	1.5	50.17	1.5	49.2
Average	1.5	49.76	1.5	50.17	1.5	49.21

4.2. 4 × 4 Magic Matrix-Based Image Steganography

Table 2 lists the experimental results of the 4 × 4 magic matrix-based image steganography. As shown by the example of a 4 × 4 magic matrix in Figure 6, four images are processed by steganography. According to the experimental results, this scheme can achieve an embedding capacity of 2 bpp and a PSNR of 46.36 dB, able to maintain good image quality.

Table 2. Experimental results of 4 × 4 magic matrix-based image steganography.

Cover Image	ER (bpp)	PSNR (dB)	Hiding Duration	Extraction Duration
Baboon	2	46.3651	0.0256	0.0121
Paper	2	46.3604	0.0282	0.0137
Airplane	2	46.3658	0.0266	0.0135
House	2	46.3583	0.0305	0.0128
Avg	2	46.3624	0.0277	0.0130

⋮	⋮										
9	8	6	5	11	8	6	5	11	8	6	
8	3	13	14	0	3	13	14	0	3	13	
7	15	1	2	12	15	1	2	12	15	1	
6	4	10	9	7	4	10	9	7	4	10	
5	8	6	5	11	8	6	5	11	8	6	
4	3	13	14	0	3	13	14	0	3	13	
3	15	1	2	12	15	1	2	12	15	1	
2	4	10	9	7	4	10	9	7	4	10	
1	8	6	5	11	8	6	5	11	8	6	
0	3	13	14	0	3	13	14	0	3	13	⋯
	0	1	2	3	4	5	6	7	8	9	⋯

Figure 6. Example of 4 × 4 Magic Matrix.

4.3. 4-2 Double-Layer Magic Matrix-Based Image Steganography

Table 3 lists the experimental results of the 4-2 double-layer magic matrix-based image steganography. Four images are processed by steganography using the structure of the double-layer magic matrix shown in Figure 3. According to the experimental results, this scheme can achieve an embedding capacity of 3 bpp and a PSNR of 40.73dB.

Table 3. Experimental results of 4-2 double-layer magic matrix-based image steganography.

Cover Image	ER (bpp)	PSNR (dB)	Hiding Duration	Extraction Duration
Airplane	3	40.73	0.041	0.0188
Baboon	3	40.731	0.0417	0.0221
Boat	3	40.725	0.0419	0.0187
House	3	40.727	0.0429	0.0193
Paper	3	40.728	0.0421	0.0185
Avg	3	40.728	0.0419	0.0195

In order to improve stego-image quality and steganography efficiency [35,36], the paper redesigns the hidden manner of secret information. Therefore, this scheme can achieve the corresponding secret information steganography. Abundant experimental comparison analyses show that this scheme can realize secret information hidden for different steganography capacity requirements. Moreover, it can improve the quality of steganography images under the same steganography capacity.

The paper describes the three image information hidden schemes in terms of the design theory and steganographic process. It analyzes steganography efficiency, steganography image quality, steganography capacity, and security through simulation experiments. Experimental results show that, compared with the previous schemes, the three schemes have some advantages in terms of steganography capacity and steganography image quality.

5. Conclusions

In the magic matrix-based data hiding methods proposed in the previous researches, the embedding capacity can reach 3bpp if the image maintains good quality. In this paper, a larger embedding capacity is achieved utilizing the double-layer magic matrix.

As one of the indicators, image quality is used to verify data embedding. With the same embedding capacity, constructing magic matrices and designing traversal areas for special magic matrices can improve the image quality and the efficiency of data embedding.

Based on the 16 × 16 Sudoku magic matrix, this paper proposes image steganography to improve algorithm security. The double-layer magic matrix-based image steganography is applied to improve the embedding capacity. A method for determining a new traversal area is designed to improve the image quality and reduce the computation complexity. A number of magic matrix-based data hiding methods have been implemented. On such a basis, it is practicable to implement a data hiding system for newly designed magic matrices.

Focusing on the security of the information transmitted on the Internet, this paper presents the data hiding scheme, which apply many technologies such as Magic Matrix. The scheme inspired from the Sudoku use a magic matrix generated by a Double-layer numeral system function to guide cover pixels' modification and fully explores embedding space in the magic matrix. This information hiding scheme gets very large embedding capacity with good security at the same time.

Author Contributions: Conceptualization, T.-C.H. and D.-X.L.; Methodology, T.-C.H. and D.-X.L.; Software development, D.-X.L.; Formal analysis, T.-C.H. and C.-C.C.; Writing—Original draft preparation, T.-C.H. and T.-L.C.; Writing—Review and editing, T.-C.H. and C.-C.C.; Funding acquisition, T.-C.H. and T.-L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Projects of Natural Science Foundation of Fujian Province of China (Nos. 2017J01109), Science and Technology Planning Fund of Quanzhou (Nos. 2016T009), and Xiamen Key Laboratory of Data Security and Blockchain Technology.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: This work was supported by the Natural Science Foundation of Fujian Province of China (Nos. 2017J01109) and Science and Technology Planning Fund of Quanzhou (Nos. 2016T009).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M.G. Information hiding-a survey. *Proc. IEEE* **1999**, *87*, 1062–1078. [CrossRef]
2. Sreejith, R.; Senthil, S. A novel tree based method for data hiding and integrity in medical images. In Proceedings of the IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), Karur, India, 27–28 April 2017; pp. 1–4.
3. Bender, W.; Gruhl, D.; Morimoto, N. Techniques for data hiding. *IBM Syst. J.* **1996**, *35*, 313–336. [CrossRef]
4. Chang, C.C.; Lin, C.C.; Tseng, C.S. Reversible hiding in DCT-based compressed images. *Inf. Sci.* **2007**, *177*, 2768–2786. [CrossRef]
5. Lu, T.C.; Leng, H.S. Reversible dual-image-based hiding scheme using block folding technique. *Symmetry* **2017**, *9*, 223. [CrossRef]
6. Liu, W.L.; Leng, H.S.; Huang, C.K. A block-based division reversible data hiding method in encrypted images. *Symmetry* **2017**, *9*, 308. [CrossRef]
7. Lin, C.C.; Shiu, P.F. High capacity data hiding scheme for DCT-based images. *J. Inf. Hiding Multimed. Signal Process.* **2010**, *1*, 220–240.
8. Abdelwahab, A.A.; Hassaan, L.A. A discrete wavelet transform based technique for image data hiding. In Proceedings of the 2008 National Radio Science Conference, Tanta, Egypt, 18–20 March 2008; pp. 1–9.
9. Liu, H.; Liu, J.; Huang, J. A robust DWT-based blind data hiding algorithm. In Proceedings of the IEEE International Symposium on Circuits & Systems, Phoenix-Scottsdale, AZ, USA, 26–29 May 2002; Volume 2, p. II.
10. Chang, C.C.; Wu, W.C. Hiding secret data adaptively in vector quantization index tables. *IEE Proc.-Vis. Image Signal Process.* **2006**, *153*, 889–897. [CrossRef]
11. Hu, Y.C. High-capacity image hiding scheme based on vector quantization. *Pattern Recognit.* **2006**, *39*, 1715–1724. [CrossRef]
12. Chang, C.C.; Kieu, T.D.; Wu, W.C. A lossless data embedding technique by joint neighboring coding. *Pattern Recognit.* **2009**, *42*, 1597–1603. [CrossRef]
13. Pizzolante, R.; Carpentieri, B.; Castiglione, A. The AVQ algorithm: Watermarking and compression performances. In Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 30 November–2 December 2011; pp. 698–702.
14. Wang, R.Z.; Lin, C.F.; Lin, J.C. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognit.* **2001**, *34*, 671–683. [CrossRef]
15. Mielikainen, J. LSB matching revisited. *IEEE Signal Process. Lett.* **2006**, *13*, 285–287. [CrossRef]
16. Ker, A.D. Improved detection of LSB steganography in grayscale images. In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 97–115.
17. Sahu, A.K.; Swain, G. A novel n-rightmost bit replacement image steganography technique. *3D Res.* **2019**, *10*, 2. [CrossRef]
18. Sahu, A.K.; Swain, G. A novel multi stego-image based data hiding method for gray scale image. *Pertanika J. Sci. Technol.* **2019**, *27*, 753–768.
19. Sahu, A.K.; Swain, G.; Babu, E.S. Digital image steganography using bit flipping. *Cybern. Inf. Technol.* **2018**, *18*, 69–80. [CrossRef]
20. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
21. Kim, H.J.; Kim, C.; Choi, Y. Improved modification direction methods. *Comput. Math. Appl.* **2010**, *60*, 319–325. [CrossRef]
22. Liu, Y.; Chang, C.C.; Huang, P.C.; Hsu, C.Y. Efficient Information Hiding Based on Theory of Numbers. *Symmetry* **2018**, *10*, 19. [CrossRef]
23. Chang, C.C.; Chou, Y.C.; Kieu, T.D. An information hiding scheme using Sudoku. In Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control, Dalian, China, 18–20 June 2008; p. 17.
24. Hong, W.; Chen, T.S.; Shiu, C.W. A minimal Euclidean distance searching technique for Sudoku steganography. In Proceedings of the 2008 International Symposium on Information Science and Engineering, Shanghai, China, 20–22 December 2008; Volume 1, pp. 515–518.
25. Kieu, T.D.; Wang, Z.H.; Chang, C.C. A Sudoku Based Wet Paper Hiding Scheme. *Int. J. Smart Home* **2011**, *3*, 1–12.
26. Chang, C.C.; Liu, Y.; Nguyen, T.S. A novel turtle shell based scheme for data hiding. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, 27–29 August 2014; pp. 89–93.
27. Liu, Y.; Chang, C.C.; Nguyen, T.S. High capacity turtle shell-based data hiding. *IET Image Process.* **2016**, *10*, 130–137. [CrossRef]

28. Jin, Q.; Li, Z.; Chang, C.C. Minimizing Turtle-Shell Matrix Based Stego Image Distortion Using Particle Swarm Optimization. *IJ Netw. Secur.* **2017**, *19*, 154–162.
29. Liu, L.; Chang, C.C.; Wang, A. Data hiding based on extended turtle shell matrix construction method. *Multimed. Tools Appl.* **2017**, *76*, 12233–12250. [CrossRef]
30. Xie, X.Z.; Lin, C.C.; Chang, C.C. Data hiding based on a two-layer turtle shell matrix. *Symmetry* **2018**, *10*, 47. [CrossRef]
31. He, M.; Liu, Y.; Chang, C.C. A mini-Sudoku matrix-based data embedding scheme with high payload. *IEEE Access* **2019**, *7*, 141414–141425. [CrossRef]
32. Horng, J.H.; Xu, S.; Chang, C.C. An Efficient Data-Hiding Scheme Based on Multidimensional Mini-SuDoKu. *Sensors* **2020**, *20*, 2739. [CrossRef]
33. Chen, W.; Chang, C.C.; Weng, S. Multi-Layer Mini-Sudoku Based High-Capacity Data Hiding Method. *IEEE Access* **2020**, *8*, 69256–69267. [CrossRef]
34. USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 13 December 2020).
35. Carpentieri, B.; Castiglione, A.; Santis, A.D.; Palmieri, F.; Pizzolante, R. One-pass lossless data hiding and compression of remote sensing data. *Future Gener. Comput. Syst.* **2019**, *90*, 222–239. [CrossRef]
36. Kumar, R.; Jung, K.H. Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context. *Inf. Sci.* **2020**, *536*, 101–119. [CrossRef]