symmetry

MDPI

Article

Verifiable (2, *n*) Image Secret Sharing Scheme Using Sudoku Matrix

Yi-Hui Chen [1,2], Jia-Ye Lee [1], Min-Hsien Chiang [3] and Shih-Hsin Chen [4,*]

[1] Department of Information Management, Chang Gung University, Taoyuan City 33302, Taiwan; cyh@gap.cgu.edu.tw (Y.-H.C.); jiaye418@gmail.com (J.-Y.L.)
[2] Kawasaki Disease Center, Kaohsiung Chang Gung Memorial Hospital, Kaohsiung 83301, Taiwan
[3] Department of Computer Science, National Chengchi University, Taipei City 11605, Taiwan; brian295639@gmail.com
[4] Department of Computer Science and Information Engineering, Tamkang University, New Taipei City 251301, Taiwan
* Correspondence: shchen@mail.tku.edu.tw

Abstract: As Internet technology continues to profoundly impact our lives, techniques for information protection have become increasingly advanced and become a common discussion topic. With the aim to protect private images, this paper splits a secret image into *n* individual shares using a Sudoku matrix with authentication features. Later, the shares can be compiled to completely reconstruct the secret image. The shares are meaningful ones in order to avoid detection and suspicion among malicious users. Our proposed matrix is unique because the embedding rate of the secret data is very high, while the visual quality of the shares can be well guaranteed. In addition, the embedded authentication codes can be retrieved to authenticate the integrity of the secret image. Experimental results prove the advantages of our approach in terms of visual quality and authentication ability.

Keywords: Sudoku; secret image sharing; data hiding; image authentication

Citation: Chen, Y.-H.; Lee, J.-Y.; Chiang, M.-H.; Chen, S.-H. Verifiable (2, *n*) Image Secret Sharing Scheme Using Sudoku Matrix. *Symmetry* **2022**, *14*, 1445. https://doi.org/10.3390/sym14071445

Academic Editor: José Carlos R. Alcantud

Received: 1 June 2022
Accepted: 9 July 2022
Published: 14 July 2022

1. Introduction

As Internet technology becomes more sophisticated, users have grown accustomed to backing up digital content, such as text files, photos, and videos, to cloud platforms. These technologies allow users to easily access their photos from anywhere; however, if the platform is not trustworthy, personal privacy can be jeopardized. Image encryption [1,2] is a reliable tool for traditional information security. Files containing sensitive data are usually encrypted prior to uploading. However, traditional encryption methods face shortcomings; for instance, an encrypted image is meaningless and thus easily attracts the attention of hackers, who try to decrypt them through data analysis and data mining. The meaningless content is difficult to manage. In order to facilitate management, image information can be carried under the encrypted image [3–28], so as to identify the content according to the extracted information later. However, since traditional data are hidden in a single carrier, once the carrier is discovered, the probability of the code being cracked greatly increases. In order to reduce the risk that comes from using a single carrier, Shamir and Blakley [29] proposed a (t, n) threshold secret sharing approach that first decomposes the secret into n parts, which then jointly provide their share to reconstruct the secret, where t is less than or equal to n. It then distributes them to different participants of n. Afterward, participants are greater than $t-1$. However, the shares are still meaningless to users, which arouses the suspicion of malicious attackers. Therefore, secure Internet usage and data privacy have become major issues and given rise to various data-hiding technologies that embed shared content into images.

Chang et al. [30] proposed a reversible secret image sharing system (SIS) using an exploiting modification direction (EMD) matrix. The shared images are embedded into the

cover images as stego images. After embedding, the stego image has high visual quality. The shared image can be extracted, and then the secret image can be reconstructed through calculation. To improve the visual quality, Chang et al. [31] proposed an SIS scheme based on the Sudoku matrix and Lagrange polynomial. Later, Yan et al. proposed a reversible image secret sharing scheme [32]. To guarantee the integrity of the shares, the authentication mechanism authenticates which pixels are modified or lost during transmission. In 2018, Liu and Chang [33] proposed applying the authentication mechanism to secret sharing to authenticate whether the shadow images have been tampered with (modified) or not. In 2021, Gao et al. [34] proposed a high-capacity secret sharing scheme with an authentication mechanism. To achieve reversibility, a reversible and verifiable SIS scheme has also been proposed. Gao et al. [35] designed a stick insect matrix to verify the shared image, and embedded the verification code and the secret image into the shared image. However, the shared images generated by these reversible SIS schemes rely on a single cover image, which may increase the possibility that confidential images may be identified through statistical analysis of subtle differences between share images. In order to prevent the discovery of secret images by statistical analysis, Liu et al. [36] and Chang et al. [37] generated shares from different cover images. Nevertheless, these methods cannot construct secret images losslessly.

In this paper, we encode a secret image into n shares using the concept of Sudoku. The schemes [33–36,38] are not allowed more than three participants. The scheme allows n joint participants, so it is more flexible than the above schemes. To achieve a flexible secret sharing scheme, we encode the shares by using simultaneous algebraic equations, in which the parameters are a hybrid of the secret pixels and the corresponding authentication codes. Later, the shares are embedded into the cover images. The cover images can be different individually. Any two cover images can be combined together to completely restore the secret image. If the pixels in the cover image are missing or have been modified, an authentication mechanism indicates the untrue locations. During the embedding process, the cover image is only slightly modified due to the concept of Sudoku. Therefore, it is difficult to identify the difference between the original cover image and the hidden image, which helps protect the secret image from detection by malicious users. When compared with Gao et al.'s method [34,35], as summarized in Section 4, the proposed approach achieves superior performance in terms of visual quality, hiding capacity, and authentication ability.

The structure of this paper is organized as follows. First, we briefly present the Sudoku matrix in Section 2. Next, we describe our proposed scheme in Section 3, followed by the experimental results and analysis in Section 4. Finally, our conclusions are summarized in Section 5.

2. Sudoku Matrix

This section introduces the concept of the Sudoku matrix M [39], which represents the core of our solution. The size of the Sudoku matrix M is 256×256, as shown in Figure 1, calculated using Equation (1), where $n = 2$. As can be seen in the Figure 1, each pixel pair, represented by α_1 and α_2, can be mapped to a core digit. Based on the core number, there are eight different independent numbers surrounding the core number without any repeated numbers. For example, if $\alpha_1 = 5$ and $\alpha_2 = 2$, as shown in Figure 1, the core digit is 2, the surrounding eight neighboring digits are different from each other, and the range is between 0 and 8, excluding the number 2. By using the Sudoku matrix M, a pixel pair can be moved to a new pixel pair, which is represented by α_1' and α_2' according to the hidden number d. For example, if $d = 5$, α_1' and α_2', obtained through Equation (2), will be 5 and 3, respectively. The maximum distortion of a pixel is 1 in order to maintain good visual quality after secret embedding.

$$\alpha = \sum_{i=1}^{n} 3^{i-1} \alpha_i \bmod 3^n \tag{1}$$

$$d = f(\alpha'_1, \alpha'_2) = \alpha'_1 + 3 \times \alpha'_2 \bmod 9 \tag{2}$$

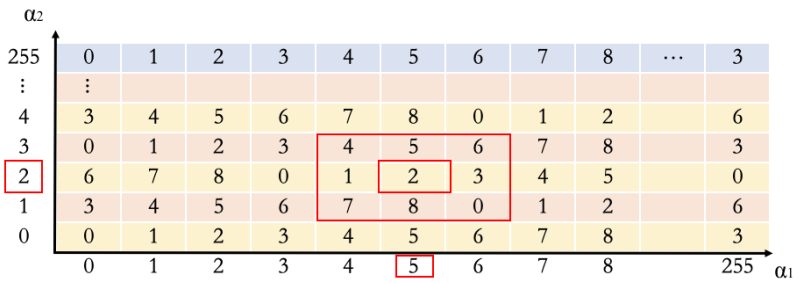


Figure 1. An example of Sudoku matrix M, where $w = 2$, $\alpha_1 = 5$ and $\alpha_2 = 2$.

3. Research Methods

In this section, we propose a (t, n)-threshold secret sharing scheme using the Sudoku matrix, where $t \leq n$. The secret image can be distributed to n different participants. After this, any t participants together can completely reconstruct the secret image, except in the case where participants whose number of shares minus the result is a multiple of three. An authentication mechanism is also proposed to authenticate the integrity of the proposed scheme. The new proposed Sudoku matrix can markedly improve the embedding capacity of secret data. The proposed approach can be divided into the following parts: (1) the procedure for hiding and extracting secret images, (2) the authentication mechanism, and (3) the reconstruction of the secret image and authentication.

Based on the (t, n)-threshold secret sharing method put forth by Shamir and Blakley in 1979, the matrix that we propose incorporates this concept as a $(2, n)$-SIS scheme. In our method, there is no limit on the number of shareholders, and each two of the holders can completely retrieve secret data. As the overflow shows in Figure 2a, there can be several cover images to embed secret data, while the same number of shares are produced. Any two of the shares can reconstruct the secret image. For example, as shown in Figure 2b, if n is 29, we select two of the shares, such as the first and the last ones, to reconstruct the secret image.

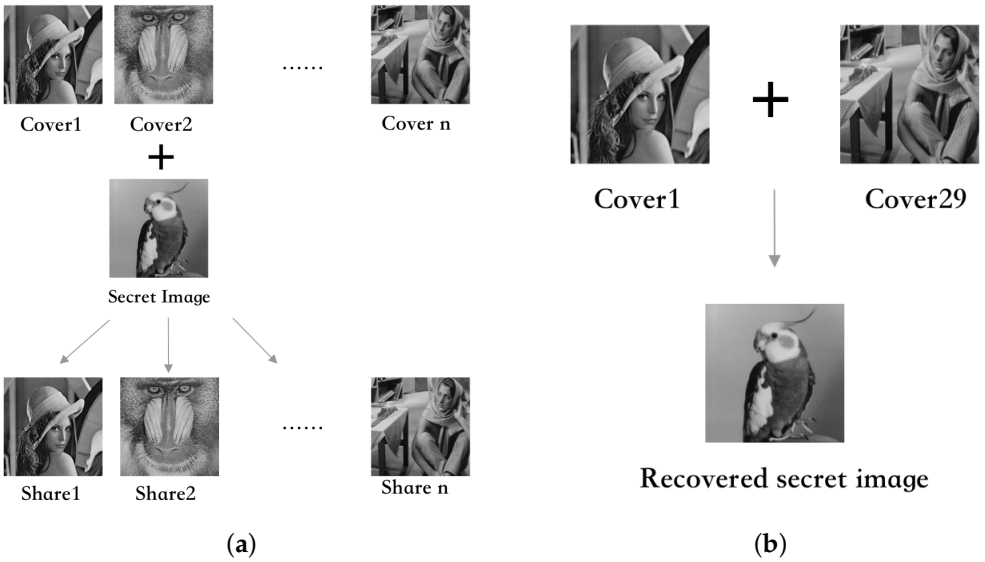


Figure 2. Schematic diagram of the proposed $(2, n)$-SIS scheme. (**a**) Secret sharing process. (**b**) Recovery process.

If two of the random shares are real, as shown in Figure 3a,b, the secret data can be recovered completely, as in Figure 3c. On the contrary, if any one of the shares is fake, as in

Figure 3e, the secret data cannot be retrieved, and the image in the authentication result will appear incomplete, as shown in Figure 3f.

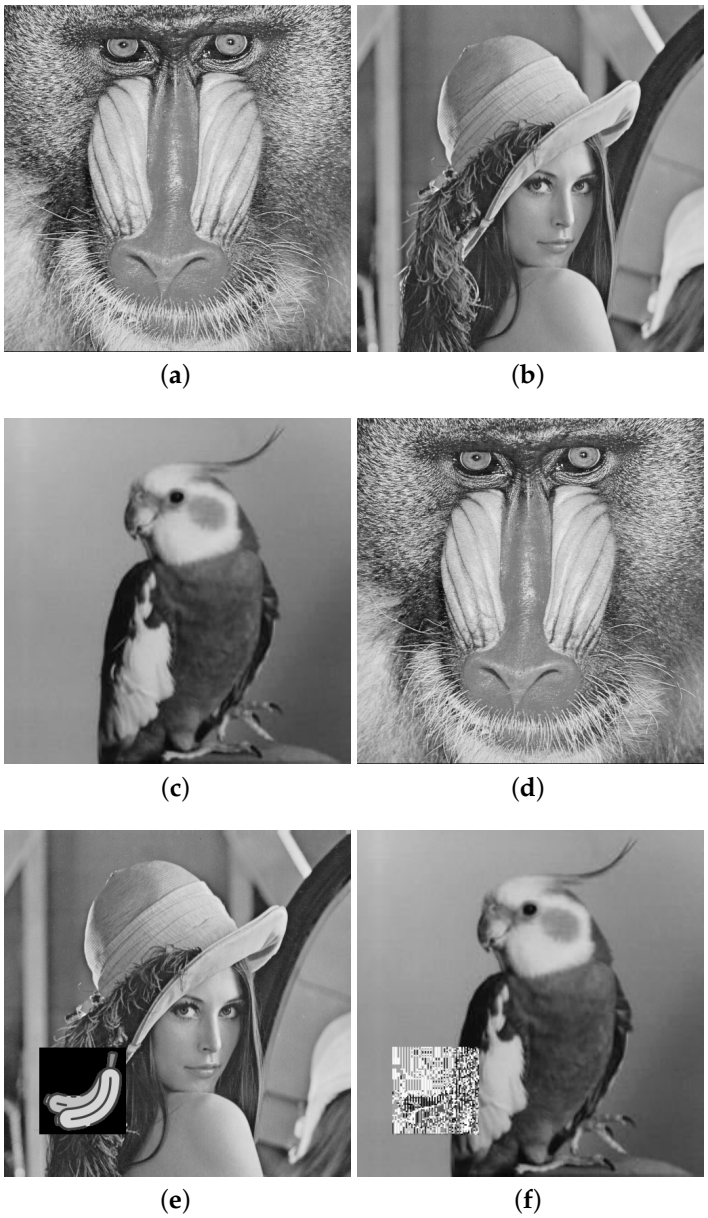


Figure 3. An example of our schematic diagram. (**a**) Real share 1. (**b**) Real share 2. (**c**) Authentication result—fully recovered. (**d**) Real share 1. (**e**) Fake share 2. (**f**) Authentication result—not recovered completely.

3.1. The Procedure of Hiding Secret Image and Authentication Codes to Cover Images

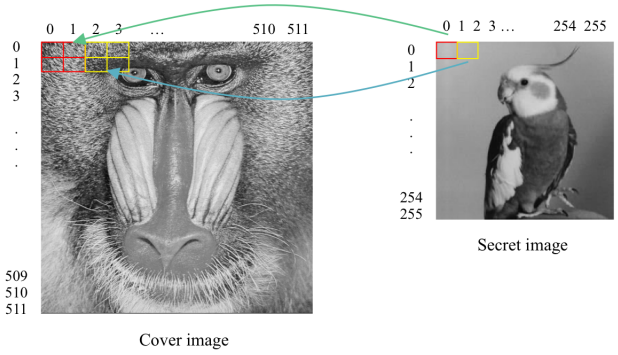
We adopt Equations (3) and (4), to describe the secret image divided into n shadows and the corresponding authentication codes hidden back into the shadows, respectively. There is a secret image of size $n \times n$ to be hidden, while there can be several cover images of size $2n \times 2n$ depending on the numbers of shareholders participating in hiding the secret data. There are two square pixels of each cover image to hide two pixels of secret data values and the corresponding authentication codes, as shown in Figure 4a. Each square pixel consists of four pixels. The first square pixel, denoted by B_1, and the second square pixel, denoted by B_2, are used to embed the first pixel, denoted by p_1, and the second secret pixel, denoted by p_2, of the secret image in different colors, as shown in Figure 4b. Here,

for B_j ($j \in \{1,2\}$), the original pixel values of the four pixels, located in the upper-left pixel, the upper-right pixel, the bottom-left pixel, and the bottom-right pixel, are represented as B_j^1, B_j^2, B_j^3, and B_j^4, respectively.

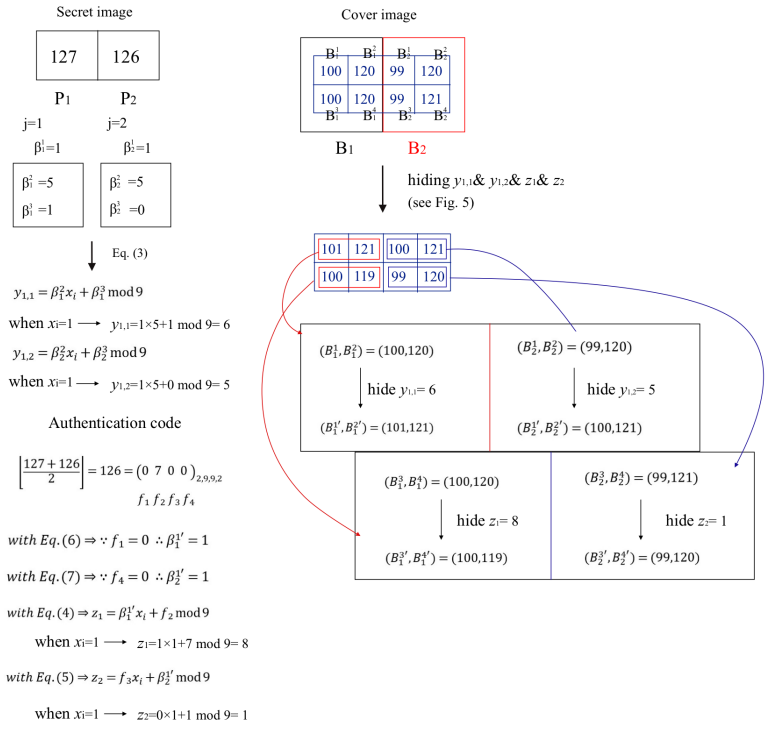
During the secret sharing procedure, first, the pixel value in the secret image needs to be converted to a base value of 9, denoted by $(\beta_j^1 \beta_j^2 \beta_j^3)_9$, where β_j^1 is in the range of 0 and 3, and β_j^2 and β_j^3 are in the range of 0 and 8, and j are equal to 1 and 2 if the digits are generated by pixels p_1 and p_2, respectively. Secondly, the β_j^2 and β_j^3 are embedded into the top two pixels (B_j^1 and B_j^2) of the cover images with Equation (3). Here, the x_i represents the ID number of the cover image.

$$y_{i,j} = \beta_j^2 x_i + \beta_j^3 \mod 9 \tag{3}$$

$$z_1 = \beta_1^{1\prime} x_i + f_2 \mod 9 \tag{4}$$



(**a**)



(**b**)

Figure 4. Schematic diagram of secret data embedded into a cover image. (**a**) Schematic diagram. (**b**) An embedding example.

An embedding example is shown in Figure 4b, prior to undergoing the embedding procedure. We suppose that the first pixel value p_1 in the pixel pair retrieved by the secret image is 127, for which the ID of the cover image is $x_i = 1$, and the converted value is $(151)_9$, indicated as β_1^1, β_1^2, β_1^3, from left to right, respectively. With Equation (3), the y_i is 6 because the equation is generated as $y_{i,1} = 5x_i + 1 \bmod 9$ if $x_i = 1$. Suppose that the original pixel values of B_1^1 and B_1^2 are 100 and 120, respectively. To hide the $y_{i,1}$ value, the pixels B_1^1 and B_1^2 are changed as stego pixels $B_1^{1\prime}$ and $B_1^{2\prime}$, respectively. After embedding $y_{i,1}$ ($y_{i,1} = 6$ in the example), the values $B_1^{1\prime}$ and $B_1^{2\prime}$ will be 101 and 121, respectively, as shown in Figure 5. In the same way, the digits β_2^2 and β_2^3 generated by the secret pixel p_2 can be hidden as B_2^1 and B_2^2 to generate the stego pixels $B_2^{1\prime}$ and $B_2^{2\prime}$. For example, if p_2 is equal to 126, the values of β_2^2 and β_2^3 are 5 and 0, respectively. After the hiding procedure, the stego pixels $B_2^{1\prime}$ and $B_2^{2\prime}$ are 100 and 121, respectively.

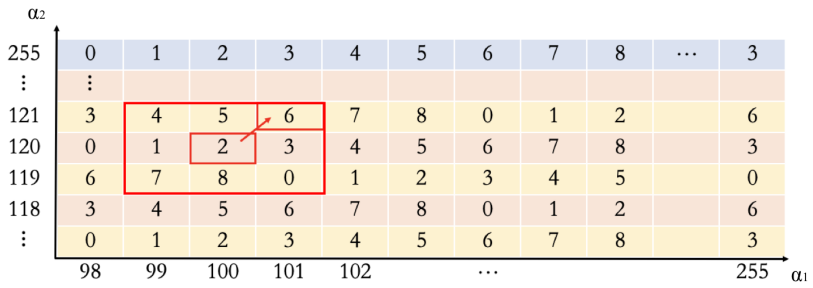


Figure 5. Data embedding example with hidden number 6 changing α_1 and α_2 to 101 and 121.

The authentication codes, denoted by f_1, f_2, f_3, and f_4, are the average of pixels p_1 and p_2 and transformed into $(f_1 f_2 f_3 f_4)_{2,9,9,2}$ via a multiple notation system. Later, the digits β_1^1 and β_2^1 are hybridized with the authentication codes for embedding into pixels B_1^3, B_1^4, B_2^3, and B_2^4 based on Equations (4) and (5). Here, the values $\beta_1^{1\prime}$ and $\beta_2^{1\prime}$ are generated according to Equations (6) and (7), respectively.

$$z_2 = f_3 x_i + \beta_2^{1\prime} \bmod 9 \tag{5}$$

$$\beta_1^{1\prime} = \begin{cases} \beta_1^1 & \text{if } f_1 = 0 \\ \beta_1^1 + 4 & \text{if } f_1 = 1 \end{cases} \tag{6}$$

$$\beta_2^{1\prime} = \begin{cases} \beta_2^1 & \text{if } f_4 = 0 \\ \beta_2^1 + 4 & \text{if } f_4 = 1 \end{cases} \tag{7}$$

As for embedding the hybrid authentication codes, the pixel pairs (B_1^3, B_1^4) and (B_2^3, B_2^4) are used to embed the digits z_1 and z_2, respectively, using the Sudoku matrix as denoted by ($B_1^{3\prime}$, $B_1^{4\prime}$) and ($B_2^{3\prime}$, $B_2^{4\prime}$). For example, we assume that the two secret pixels p_1 and p_2 are 127 and 126. The average value is 126. The generated authentication codes f_1, f_2, f_3, and f_4 are 0, 0, 7, and 0, respectively. Since the values of f_1 and f_4 are all 0 s, the values of $\beta_1^{1\prime}$ and $\beta_2^{1\prime}$ will be 1 and 1, respectively. The two equations are composed as $z_1 = x_i + 7$ mod 9 and $z_2 = 0x_i + 1$ mod 9. If x_i equals 1, z_1 and z_2 are 8 and 1, respectively. After hiding the authentication codes, the stego pixels ($B_1^{3\prime}$, $B_1^{4\prime}$) and ($B_2^{3\prime}$, $B_2^{4\prime}$) are (100, 119) and (99, 120), respectively.

3.2. The Procedure of Secret Image Reconstruction and Authentication

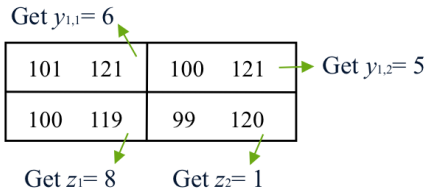
During secret image reconstruction and authentication extraction, we can retrieve the $y_{i,j}$ value according to the stego pixels $B_j^{1\prime}$ and $B_j^{2\prime}$. Equation (3) can be reconstructed when participant *id* as x_i is inputted as the participant ID. For example, in the previous example, $y_{i,1}$ can be obtained by mapping the pixels $B_1^{1\prime}$ and $B_1^{2\prime}$ to indicate the digit 6 using a Sudoku matrix. Thus, Equation (3) can be reconstructed as $6 = \beta_1^2 + \beta_1^3 \bmod 9$.

Any two participants can resolve the parameters β_1^2 and β_1^3. Using the same process, the parameters β_2^2 and β_2^3 can be extracted by the stego pixels $B_2^{1\prime}$ and $B_2^{2\prime}$.

The values of z_1 and z_2 in Equations (4) and (5) can be reconstructed by mapping the stego pixel pairs ($B_1^{3\prime}$, $B_1^{4\prime}$) and ($B_2^{3\prime}$, $B_2^{4\prime}$). For the previous example, as shown in Figure 6, when inputting the participant *id* $x_i = 1$, two equations can be reconstructed as $1 = \beta_1^{1\prime} + f_2 \bmod 9$ and $8 = f_3 + \beta_2^{1\prime} \bmod 9$. With any two participants, the parameters $\beta_1^{1\prime}$, f_2, f_3, and $\beta_2^{1\prime}$ can be extracted. The values f_1 and f_4 can be computed with Equations (8) and (9), respectively.

$$f_1, \beta_1^1 = \begin{cases} 0, \beta_1^{1\prime}, & \text{if } \beta_1^{1\prime} < 4 \\ 1, \beta_1^{1\prime} - 4, & \text{otherwise.} \end{cases} \tag{8}$$

$$f_4, \beta_2^1 = \begin{cases} 0, \beta_2^{1\prime}, & \text{if } \beta_2^{1\prime} < 4 \\ 1, \beta_2^{1\prime} - 4, & \text{otherwise.} \end{cases} \tag{9}$$



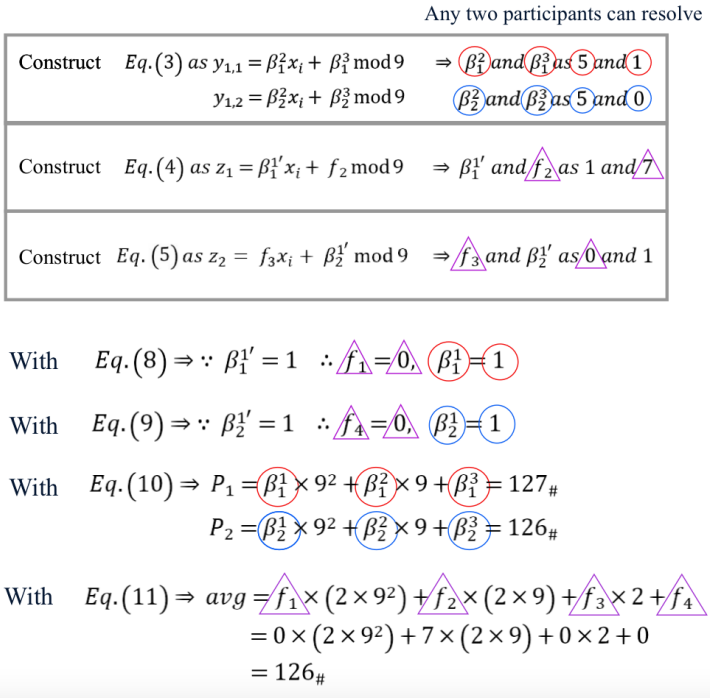


Figure 6. Example of secret pixel reconstruction and authentication code extraction, where the same shape is used for the same parameters in the analytical equation

After this, the secret pixels p_1 and p_2 can be reconstructed with Equation (10). Moreover, the average pixel, denoted by avg, can be obtained via Equation (11). The reconstructed pixels p_1 and p_2 can be computed as an average value, denoted by avg'. The pixel is judged as authentic if the value avg' is equal to avg; otherwise, it is labeled inauthentic.

$$p_j = \beta_j^1 \times 9^2 + \beta_j^2 \times 9 + \beta_j^3. \tag{10}$$

$$avg = f_1 \times (2 \times 9^2) + f_2 \times (2 \times 9) + f_3 \times 2 + f_4. \tag{11}$$

4. Experimental Results

In the experiment, two secret images of size 256 × 256 pixels, as shown in Figure 7a,b, and four cover images of size 512 × 512 pixels, as shown in Figure 7c–f, were used. During the retrieval and authentication procedure, if the cover images were real, without evidence of tampering, we could reconstruct the full secret images completely, as shown in Figure 8a,b. To measure the visual quality of the cover images and reconstructed secret image, PSNR (peak signal-to-noise ratio) was used with Equation (12), where MSE (mean-squared error) was calculated with Equation (13), in which $I(i,j)$ and $K(i,j)$ were the values of the original pixel and that of the stego pixel located at location (i,j), and m and n were the size (height and width) of the image. Generally, the higher the PSNR value is, the better the visual quality will be. Furthermore, we evaluated the visual quality between the cover image and the shared image using the structural similarity (SSIM) of Equation (14), where μ_x and μ_y are the averages of x and y; σ_x and σ_y are the standard deviation values of x and y; and values c_1 and c_2 are two constant values, which are set to 1s. If the SSIM value equals 1, it means that the two images are identical without any distortion. Visual quality comparisons of the shadow images shown in Table 1 demonstrate high visual quality. It is difficult to recognize the differences between cover images and share images.

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

$$MSE = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2 \tag{13}$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(\sigma_x y + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{14}$$

Table 1. Visual quality of shadow images when embedding different secret images.

Secret Images	Lena		Baboon		Pepper		Zelda	
	PSNR	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**
Bird	49.88	0.993	49.88	0.998	49.88	0.993	49.89	0.990
Jet(F16)	49.88	0.994	49.89	0.998	49.88	0.993	49.88	0.990

(**a**) (**b**)

Figure 7. *Cont.*

(**c**) (**d**)

(**e**) (**f**)

Figure 7. Secret images and cover images. (**a**) Secret image "Bird". (**b**) Secret image "Jet(F16)". (**c**) Cover image "Lena". (**d**) Cover image "Baboon". (**e**) Cover image "Pepper". (**f**) Cover image "Zelda".

(**a**) (**b**)

Figure 8. Reconstructed secret images. (**a**) Recovered image "Bird" (PSNR = ∞). (**b**) Recovered image "Jet(F16)" (PSNR = ∞).

We also compared several additional features listed in Table 2, which shows that our proposed scheme achieved high performance and met all requirements.

Table 2. Comparison to other methods.

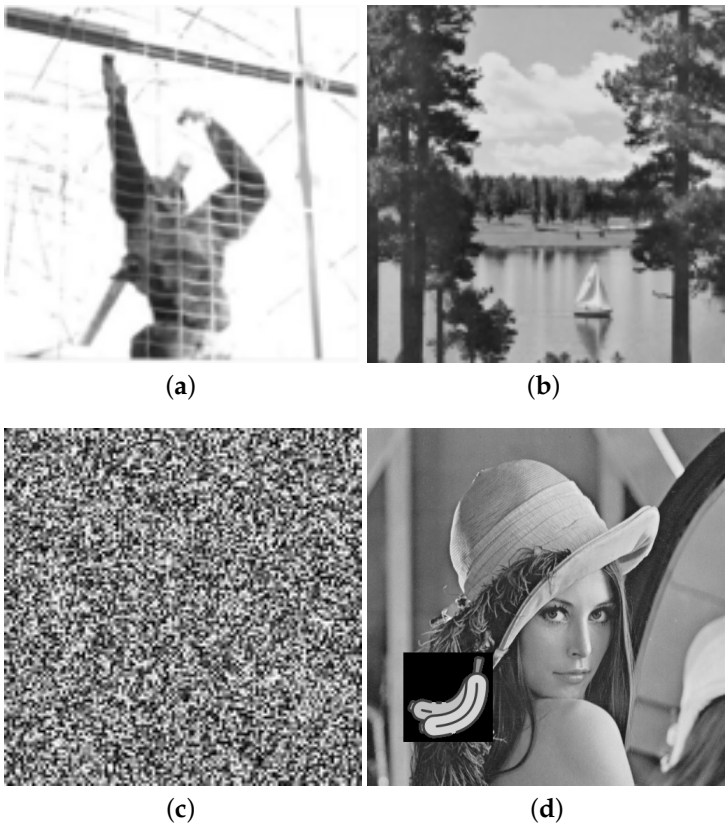
Features	Gao et al.'s Scheme [35]	Li et al.'s Scheme [38]	Liu et al.'s Scheme [33]	Liu et al.'s Scheme [36]	Gao et al.'s Scheme [34]	Proposed Scheme
Meaningful shares	Yes	Yes	Yes	Yes	Yes	Yes
Reversibility	Yes	Yes	Yes	-	-	Yes
Different cover images	-	-	-	Yes	Yes	Yes
(k,n)-SIS	(2,2)-SIS	(3,3)-SIS	(2,2)-SIS	(2,2)-SIS	(2,3)-SIS	(2, n)-SIS
Fault tolerance	Yes	-	-	-	Yes	Yes
Average PSNR	32.96	49.07	48.72	41.71	40.41	49.88
Embedding capacity (bits)	786,432	624,215	524,288	785,525	1,310,720	786,432

There were three fake logos, as shown in Figure 9a–c, which were replaced with the content of stego images. If a stego image had been modified (tampered with), as shown in Figure 9d (128 × 128 in size), the secret image could not be completely reconstructed, as shown in Figure 9f. Figure 9g demonstrates the authentication results; the modified region is shown in black, while the unmodified area is in white. The accuracy rate of detecting an inauthentic region was depicted by BER (Bit Error Rate) using Equation (15). The BER of Figure 9g was 99.50% on average. The BER value was much higher for our approach than for [work] as shown in Table 3, in which the first column shows the detection results for Gao et al.'s method, where the two shadow images join in the authentication procedure, and the second column shows the results that incorporate three shadow images.

$$BER = \frac{\text{the number of truly detected pixels}}{\text{the number of fake pixels}} \times 100\%. \quad (15)$$

Table 3. BER values compared to Gao et al.'s approach.

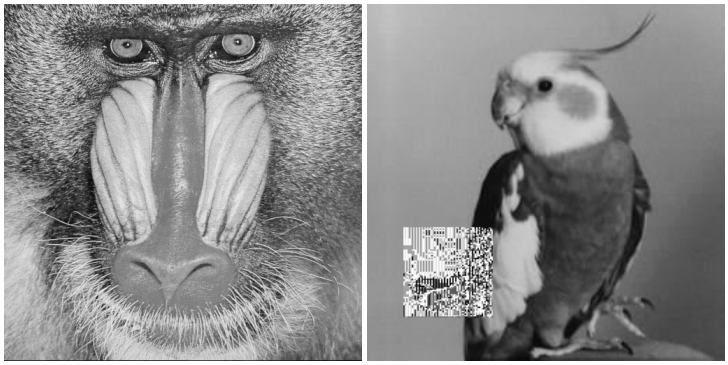
Tampered Image	Gao et al.'s Scheme [34]		Proposed Scheme
Special image	0.684	0.942	0.997
Standard image	0.084	0.834	0.995
Uniform noise	0.097	0.836	0.995



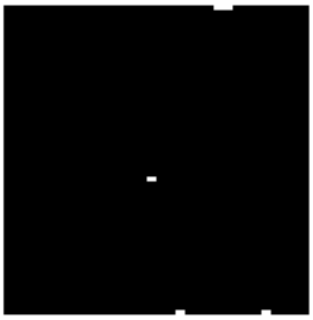
(**a**) (**b**)

(**c**) (**d**)

Figure 9. *Cont.*



(**e**) (**f**)



(**g**)

Figure 9. An authentication example. (**a**) Special image (fake logo). (**b**) Standard image (fake logo). (**c**) Uniform noise (fake logo). (**d**) Image with tampering (fake cover). (**e**) Image without tampering (real cover). (**f**) Reconstructed secret image. (**g**) Detected inauthentic region (painted in black).

5. Conclusions

This paper proposes a verifiable image secret sharing method that can divide a secret image into several shares, and then embed the shares containing authentication codes into cover images as stego images. Later, the secret image can be completely reconstructed, and the authentication codes can be extracted via any two stego images. Experiments show that the hiding capacity of the proposed method exceeds that of other approaches for both smooth and complex types of images. Moreover, the visual quality of the stego images in our approach is superior to that found in the experiments, while the BER values are much higher than those achieved.

Author Contributions: Methodology, Y.-H.C. and M.-H.C.; formal analysis and validation, Y.-H.C., M.-H.C. and J.-Y.L.; writing—original draft preparation, Y.-H.C., J.-Y.L. and S.-H.C.; writing—review and editing, Y.-H.C. and S.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: The work was supported in part by the Ministry of Science and Technology of the Republic of China, Taiwan, under Grant MOST 110-2221-E-182-026-MY3, and in part by the Kaohsiung Chang Gung Memorial Hospital, with grant number CMRPD3M0011.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Li, X.; Xiao, D.; Mou, H.; Lu, D.; Peng, M. A compressive sensing based image encryption and compression algorithm with identity authentication and blind signcryption. *IEEE Access* **2020**, *8*, 211676–211690. [CrossRef]
2. Sasaki, M.; Watanabe, Y. Visual secret sharing schemes encrypting multiple images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 356–365. [CrossRef]
3. Cao, X.; Du, L.; Wei, X.; Meng, D.; Guo, X. High capacity reversible data hiding in encrypted images by patch-level sparse representation. *IEEE Trans. Cybern.* **2015**, *46*, 1132–1143. [CrossRef] [PubMed]
4. Chen, K.; Chang, C.C. High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement. *J. Vis. Commun. Image Represent.* **2019**, *58*, 334–344. [CrossRef]
5. Chen, Y.C.; Shiu, C.W.; Horng, G. Encrypted signal-based reversible data hiding with public key cryptosystem. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1164–1170. [CrossRef]
6. Chen, Y.H.; Lin, P.Y.; Wu, H.P.; Chen, S.H. Joint hamming coding for high capacity lossless image encryption and embedding scheme. *Appl. Sci.* **2022**, *12*, 1966. [CrossRef]
7. Hong, W.; Chen, T.S.; Wu, H.Y. An improved reversible data hiding in encrypted images using side match. *IEEE Signal Process. Lett.* **2012**, *19*, 199–202. [CrossRef]
8. Huang, F.; Huang, J.; Shi, Y.Q. New framework for reversible data hiding in encrypted domain. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2777–2789. [CrossRef]
9. Liao, X.; Shu, C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. *J. Vis. Commun. Image Represent.* **2015**, *28*, 21–27. [CrossRef]
10. Ma, K.; Zhang, W.; Zhao, X.; Yu, N.; Li, F. Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 553–562. [CrossRef]
11. Puteaux, P.; Puech, W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1670–1681. [CrossRef]
12. Qian, Z.; Zhang, X.; Feng, G. Reversible data hiding in encrypted images based on progressive recovery. *IEEE Signal Process. Lett.* **2016**, *23*, 1672–1676. [CrossRef]
13. Qian, Z.; Zhang, X.; Wang, S. Reversible data hiding in encrypted JPEG bitstream. *IEEE Trans. Multimed.* **2014**, *16*, 1486–1491. [CrossRef]
14. Qian, Z.; Zhang, X. Reversible data hiding in encrypted images with distributed source encoding. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *26*, 636–646. [CrossRef]
15. Wu, X.; Sun, W. High-capacity reversible data hiding in encrypted images by prediction error. *Signal Process.* **2014**, *104*, 387–400. [CrossRef]
16. Xu, D.; Wang, R. Separable and error-free reversible data hiding in encrypted images. *Signal Process.* **2016**, *123*, 9–21. [CrossRef]
17. Yi, S.; Zhou, Y. Binary-block embedding for reversible data hiding in encrypted images. *Signal Process.* **2017**, *133*, 40–51. [CrossRef]
18. Yi, S.; Zhou, Y. Separable and reversible data hiding in encrypted images using parametric binary tree labeling. *IEEE Trans. Multimed.* **2019**, *21*, 51–64. [CrossRef]
19. Yin, Z.; Abel, A.; Tang, J.; Zhang, X.; Luo, B. Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification. *Multimed. Tools Appl.* **2017**, *76*, 3899–3920. [CrossRef]
20. Yin, Z.; Xiang, Y.; Zhang, X. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding. *IEEE Trans. Multimed.* **2020**, *22*, 874–884. [CrossRef]
21. Zhang, X. Reversible data hiding in encrypted image. *IEEE Signal Process. Lett.* **2011**, *18*, 255–258. [CrossRef]
22. Zhang, X. Separable reversible data hiding in encrypted image. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 826–832. [CrossRef]
23. Zhang, W.; Ma, K.; Yu, N. Reversibility improved data hiding in encrypted images. *Signal Process.* **2014**, *94*, 118–127. [CrossRef]
24. Zhang, X.; Qian, Z.; Feng, G.; Ren, Y. Efficient reversible data hiding in encrypted images. *J. Vis. Commun. Image Represent.* **2014**, *25*, 322–328. [CrossRef]
25. Zhang, X.; Long, J.; Wang, Z.; Cheng, H. Lossless and reversible data hiding in encrypted images with public-key cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *26*, 1622–1631. [CrossRef]
26. Zhang, W.; Wang, H.; Hou, D.; Yu, N. Reversible data hiding in encrypted images by reversible image transformation. *IEEE Trans. Multimed.* **2016**, *18*, 1469–1479. [CrossRef]
27. Zheng, S.; Li, D.; Hu, D.; Ye, D.; Wang, L.; Wang, J. Lossless data hiding algorithm for encrypted images with high capacity. *Multimed. Tools Appl.* **2016**, *75*, 13765–13778. [CrossRef]
28. Zhou, J.; Sun, W.; Dong, L.; Liu, X.; Au, O.C.; Tang, Y.Y. Secure reversible image data hiding over encrypted domain via key modulation. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 441–452. [CrossRef]
29. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
30. Chang, C.C.; Kieu, T.D.; Chou, Y.C. Reversible data hiding scheme using two steganographic images. In Proceedings of the TENCON 2007–2007 IEEE Region 10 Conference, Taipei, Taiwan, 30 October–2 November 2007; pp. 1–4.
31. Chang, C.C.; Lin, P.Y.; Wang, Z.H.; Li, M. A sudoku-based secret image sharing scheme with reversibility. *J. Commun.* **2010**, *5*, 5–12. [CrossRef]
32. Yan, X.; Lu, Y.; Liu, L.; Song, X. Reversible image secret sharing. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3848–3858. [CrossRef]

33. Liu, Y.; Chang, C.C. A turtle shell-based visual secret sharing scheme with reversibility and authentication. *Multimed. Tools Appl.* **2018**, *77*, 25295–25310. [CrossRef]
34. Gao, K.; Horng, J.H.; Chang, C.C. An authenticatable (2, 3) secret sharing scheme using meaningful share images based on hybrid fractal matrix. *IEEE Access* **2021**, *9*, 50112–50125. [CrossRef]
35. Gao, K.; Horng, J.H.; Liu, Y.; Chang, C.C. A reversible secret image sharing scheme based on stick insect matrix. *IEEE Access* **2020**, *8*, 130405–130416. [CrossRef]
36. Liu, Y.; Chang, C.C.; Huang, P.C. Security protection using two different image shadows with authentication. *Math. Biosci. Eng.* **2019**, *16*, 1914–1932. [CrossRef]
37. Chang, C.C.; Horng, J.H.; Shih, C.S.; Chang, C.C. A maze matrix-based secret image sharing scheme with cheater detection. *Sensors* **2020**, *20*, 3802. [CrossRef]
38. Li, X.S.; Chang, C.C.; He, M.X.; Lin, C.C. A lightweight authenticable visual secret sharing scheme based on turtle shell structure matrix. *Multimed. Tools Appl.* **2020**, *79*, 453–476. [CrossRef]
39. Lin, C.C.; Chen, Y.H.; Chang, C.C. LSB-based high-capacity data embedding scheme for digital images. *Int. J. Innov. Comput. Inf. Control* **2009**, *5*, 4283–4289.