An Authenticatable (2, 3) Secret Sharing Scheme Using Meaningful Share Images Based on Hybrid Fractal Matrix

KAI GAO\(^1\), JI-HWEI HORNG\(^2\), AND CHIN-CHEN CHANG\(^1\), (Fellow, IEEE)

\(^1\)Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan
\(^2\)Department of Electronic Engineering, National Quemoy University, Kinmen 89250, Taiwan

Corresponding authors: Ji-Hwei Horng (horng@email.nqu.edu.tw) and Chin-Chen Chang (alan3c@gmail.com)

ABSTRACT

Secret image sharing (SIS) scheme is an important technology to protect secret information. It distributes the secret data into multiple shares so that the participants can obtain the embedded secret by sharing their authenticated shares. Through a simple process of these shares, the secret data can be extracted. In this paper, we propose a (2, 3) SIS scheme based on a fractal matrix. Through guidance of the proposed fractal matrix, the secret data can be distributed into three shares which are indistinguishable from their corresponding cover images. Any two of the three distinct shares can cooperate to extract the exact secret data. Moreover, we devise two authentication mechanisms to prevent from tampering. Experimental results show that our proposed scheme can provide efficient payloads with shares of good visual quality. The authentications are also effective and easy to implement.

INDEX TERMS

Secret image sharing, fractal matrix, data hiding, steganography, authentication.

I. INTRODUCTION

Nowadays, with the rapid development of the Internet, people can continuously enjoy the fruits of the latest technological revolution. More and more information is transmitted through the Internet. However, network viruses, Trojan horses, and illegal organizations that steal information all pose serious threats to information security. Thus, the security of information transmission has become particularly important, especially in the political, military, and commercial fields. Although traditional encryption can ensure information security to a certain extent, this type of technology does not conceal the content of the information. On one hand, the secret keys generated in order to hide information are often unordered symbols, which will arouse the interest of the attacker, thereby increasing the risk of exposure. This has become the biggest weakness of traditional encryption algorithms. On the other hand, with the rising sharply use of digital media, protecting intellectual property rights in digital media, preventing illegal copying and dissemination of intellectual property products, and ensuring information security have also become more and more urgent. In order to solve the above-mentioned series of problems, information hiding [1] technology was born.

Information hiding is mainly divided into two categories: reversible information hiding [2], [3] and irreversible information hiding [4], [5]. In reversible information hiding, the recipient can restore the original carrier losslessly after extracting the secret data embedded by the sender, while after irreversible information hiding, one cannot restore the original carrier. Based on these two categories of information hiding methods, it can be subdivided into the following four types: information hiding based on spatial domain [6]–[12], information hiding based on frequency domain [13]–[15], information hiding based on encryption domain [16]–[19], and information hiding based on compressed domain [20], [21].

Traditional information hiding schemes have an obvious common disadvantage: only a single carrier is used to embed information. Once the carrier is targeted by an attacker, the possibility of the information being attacked increases greatly. To solve this shortcoming, Shamir [22] and Blakley [23] proposed a (k, n)-threshold secret sharing scheme in 1979. Their scheme pioneered the concept of secret sharing. It distributes the secret data into n parts and deals them to n participants. When extracting the secret data, only k
In 1994, Naor and Shamir [24] applied the concept of secret sharing to images and proposed the visual secret sharing (VSS) scheme. But their scheme produces binary shares and these shares look meaningless. A meaningless share is easily noticed by an attacker during transmission. Covering the secret data with a regular image can effectively reduce the risk of being suspected. To solve these disadvantages of the original VSS scheme, many improved VSS methods [25]–[28] have been proposed.

In 2006, Chang et al. [29] proposed a reversible secret image sharing (SIS) scheme using the exploiting modification direction (EMD) reference matrix. After embedding, two steganographic images with high visual quality are generated. The main difference between VSS and SIS is the visual perceptibility. Traditional VSS (including visual cryptography [25], extended visual cryptography [26], and color extended visual cryptography [27], [28]) reconstruct images by mixing gray levels or colors through stacking. The SIS scheme proposed in [29] extracts the secret data by computation. In this modern age of consumer electronics, portable devices are popular. Therefore, thin client computing is now more feasible than stacking transparencies. The SIS scheme became a new hot issue.

In 2010, Chang et al. [30] proposed a reversible SIS scheme based on the Sudoku matrix and Lagrange polynomial. In 2018 and 2019, reversible and authenticatable SIS schemes were proposed based on the turtle shell matrix [31], [32]. In 2020, Gao et al. [33] designed a new reference matrix called the stick insect matrix to further improve the SIS schemes. These reversible SIS schemes use only a single cover image to generate multiple shares, where each share has a very slight and invisible difference.

Although the shares generated from a single cover image look the same, they are vulnerable to steganalysis. By analyzing the differences between shares, camouflage can easily be detected. In 2019 and 2020, SIS schemes using different cover images were proposed [34], [35]. However, these schemes are irreversible: the cover images cannot be reconstructed after extraction of the secret data.

With irreversibility comes the problem that when one of the shares is tampered with, the secret data cannot be recovered at all, even though the share is authenticatable. In order to reduce the risk of tampering attacks, Gao et al. [36] proposed a (2, 3) reversible SIS scheme based on the fractal matrix. Through ingenious design of the fractal matrix, any two out of the three shares can cooperate to retrieve the secret data. However, this scheme uses a single cover image to generate two shares and suffers from the steganalysis risk mentioned above.

In this paper, we propose a (2, 3) SIS scheme which is based on the new fractal reference matrix and which uses three distinct share images. In our SIS scheme, three shares that are indistinguishable from their corresponding cover images are generated and any two shares can cooperate to retrieve the secret data. Our scheme also provides two effective authentication mechanisms and a large payload. The experimental results show that the embedding capacity of our scheme is larger than those of related works, and that the visual quality of the shares is satisfactory.

The rest of this paper is as follows. Section 2 briefly introduces the new proposed fractal matrix. The share generation, authentication, and data extraction processes are proposed in Section 3. Section 4 presents the experimental results and discussions. Finally, conclusions and prospects are presented in Section 5.

II. THE PROPOSED FRAC TAL MATRIX

In this section, we briefly introduce the fractal matrix proposed by Gao et al. in [36]. Then, a modified fractal matrix based on the same concept is proposed to fit our new problem formulation.

A. BRIEF INTRODUCTION OF THE FRAC TAL MATRIX

The fractal matrix was first proposed by Gao et al. [36]. It is a special type of reference matrix which is applied to guide the production of shares in their secret sharing scheme. A fractal matrix is constituted by a lot of fundamental three-dimensional structures called fractal models. Two types of fractal models sized $2^n \times 2^n$ and $3^n \times 3^n$ are shown in Figs. 1(a) and 1(b), respectively. In each model, the colored boxes represent the fractal elements in the model. There are four and nine elements in Figs. 1(a) and 1(b), respectively. Following the spatial self-similarity property of fractals, a fractal group can be constructed using fractal models as basic elements. As shown in Fig. 2, the fractal matrix proposed in [36] contains a long series of concatenated fractal groups on its main diagonal.

The elements in a fractal model are so ingeniously arranged that the projections of all elements in a fractal group onto each axial plane constitute a perfect square matrix. In other words, each element in the fractal group is unique and indispensable. This property was exploited to design the (2, 3) SIS scheme in [36]. To achieve a similar purpose, the fractal matrix proposed in this paper is a modified version of the above matrix and will be described in the next subsection.

B. THE NEWLY PROPOSED FRAC TAL MATRIX

As discussed in the previous subsection, two fractal models, see Fig. 1, are applicable to construct a fractal group. Two factors to be considered are the embedding capacity and...
we apply a secret key to initialize the random number size 3 × 3 cubic space sized 6.

Eq. (3) determines whether $M$ (1) and (2) determine the outer and inner coordinates. Eq. (3) determines whether $M$ (x, y, z) is an element of the outer fractal model, while Eq. (4) determines whether $M$ (x, y, z) is an element of the inner fractal model. Both conditions should be valid to conclude that $M$ (x, y, z) is an element of the proposed fractal group.

$$x_0 = \lfloor x/3 \rfloor; \quad y_0 = \lfloor y/3 \rfloor; \quad z_0 = \lfloor z/3 \rfloor.$$  (1)

$$x_I = x \mod 3; \quad y_I = y \mod 3; \quad z_I = z \mod 3.$$  (2)

$$y_0 = (-x_0 + z_0 + 1) \mod 2,$$  (3)

$$y_I = (-x_I + z_I + 1) \mod 3.$$  (4)

After determining the configuration of the fractal group, we apply a secret key to initialize the random number generator and start the numbering process. First, we assign a random permutation of 0 to 7 into all elements of each fractal model $F_I$ except for the central element, which is reserved for authentication purpose. Next, we assign a random permutation of 0 to 3 to each $F_O$ inside the fractal group. For instance, $F_O(1, 0, 0) = 0, F_O(0, 1, 0) = 1, F_O(0, 0, 1) = 3$, and $F_O(1, 1, 1) = 2$ as shown in the figure. So there are a total of $2^3 \times 2^2$ elements in a fractal group.

The arrangement of fractal groups in the new fractal matrix is quite different from the arrangement in the original version proposed in [36]. The new fractal matrix is illustrated in Fig. 4. The duplicated fractal groups are compactly stacked to constitute a huge cube of $[(255)/6] \times [(255)/6] \times [(255)/6] = 42 \times 42 \times 42 = 74088$ fractal groups in total, where $\lfloor \cdot \rfloor$ denotes the floor operation. The rest elements outside the range of [0 : 251, 0 : 251, 0 : 251] covered by the fractal groups are left unassigned for authentication.

### III. THE PROPOSED (2, 3) SECRET IMAGE SHARING SCHEME

In this section, we first take an overview on the proposed scheme. Then, the production process of shares, authentication mechanisms, and data extraction process are introduced sequentially.

#### A. OVERVIEW

The schematic diagram of the proposed (2, 3)-SIS scheme is illustrated in Fig. 5. The data hider uses three distinct cover images to embed secret image or data and generates three shares, which are visually indistinguishable from their corresponding cover images. The three shares are then distributed to three participants. To recover the secret data, any two of the participants who combine their shares can completely decrypt the secret. We provide an authentication mechanism to detect tampered shares and prevent from cheating events, to be used before the decryption. When all three shares can be obtained, an even stricter authentication mechanism is available.

#### B. PRODUCTION OF THE SHARES

Assume that the secret data to be shared is converted into a long stream of binary segments denoted by
For each binary segment, $s_k^{1-2}$ and $s_k^{3-5}$ denotes the front 2 bits and the rear 3 bits, respectively. Three grayscale cover images with size $H \times W$ are rearranged and denoted as $I_1 = \{p_{3i}|i = 1, 2, \ldots, H \times W\}$, $I_2 = \{p_{2i}|i = 1, 2, \ldots, H \times W\}$ and $I_3 = \{p_{3i}|i = 1, 2, \ldots, H \times W\}$, respectively. The shares to be generated are denoted by $\hat{I}_1$, $\hat{I}_2$, and $\hat{I}_3$, which are the same size as the original cover images and are represented by $\hat{I}_1 = \{\hat{p}_{3i}|i = 1, 2, \ldots, H \times W\}$, $\hat{I}_2 = \{\hat{p}_{2i}|i = 1, 2, \ldots, H \times W\}$, and $\hat{I}_3 = \{\hat{p}_{3i}|i = 1, 2, \ldots, H \times W\}$, respectively. In this share generation phase, firstly, the three-dimensional fractal matrix $M$ is constructed. Then, the pixels in cover images are processed in the prearranged order. Each time, we apply a pixel triplet $(p_{3i}, p_{2i}, p_{3i})$ as the coordinates and map to the elements in the fractal matrix $M(p_{3i}, p_{2i}, p_{3i})$. Locate its mother fractal group $F_G$ and the precisely mapped fractal element by Eqs. (5-8).

$$Q_s = \left[p_{1i}/6\right]; \quad Q_y = \left[p_{2i}/6\right]; \quad Q_z = \left[p_{3i}/6\right]. \quad (5)$$

$$x_i = p_{1i} \mod 6; \quad y_i = p_{2i} \mod 6; \quad z_i = p_{3i} \mod 6. \quad (6)$$

$$x_O = \left[x_i/3\right]; \quad y_O = \left[y_i/3\right]; \quad z_O = \left[z_i/3\right]. \quad (7)$$

$$x_l = x_i \mod 3; \quad y_l = y_i \mod 3; \quad z_l = z_i \mod 3. \quad (8)$$

Its mother fractal group, outer fractal element, and inner fractal element are denoted by $F_G(Q_s, Q_y, Q_z)$, $F_O(x_O, y_O, z_O)$, and $F_I(x_l, y_l, z_l)$, respectively, where $0 \leq Q_s, Q_y, Q_z < 41$, $0 \leq x_O, y_O, z_O < 2$, $0 \leq x_l, y_l, z_l < 3$. To embed a secret segment $s_k$, we search the mother fractal group $F_G(Q_s, Q_y, Q_z)$ to find an outer fractal element $F_O(\hat{x}_O, \hat{y}_O, \hat{z}_O)$ and an inner fractal element $F_I(\hat{x}_I, \hat{y}_I, \hat{z}_I)$ such that $F_O(\hat{x}_O, \hat{y}_O, \hat{z}_O) = s_k^{1-2}$ and $F_I(\hat{x}_I, \hat{y}_I, \hat{z}_I) = s_k^{3-5}$. Then, calculate the share pixel triplet $(\hat{p}_{1i}, \hat{p}_{2i}, \hat{p}_{3i})$ by

$$\hat{p}_{1i} = 6 \times Q_s + 3 \times \hat{x}_O + \hat{x}_I; \quad (9)$$

$$\hat{p}_{2i} = 6 \times Q_y + 3 \times \hat{y}_O + \hat{y}_I; \quad (10)$$

$$\hat{p}_{3i} = 6 \times Q_z + 3 \times \hat{z}_O + \hat{z}_I. \quad (11)$$

The share pixel triplet is continually recorded to the shares $\hat{I}_1$, $\hat{I}_2$, and $\hat{I}_3$ as the embedding is proceeded.

For example, as shown in Fig. 6, suppose the original pixel triplet is $(0, 2, 5)$ and the secret segment $s_k = (10111)_2$. The mother fractal group, outer fractal element, and inner fractal element are $F_G(0, 0, 0)$, $F_O(0, 0, 1)$, and $F_I(0, 2, 2)$, respectively. To embed secret bits $s_k^{1-2} = (10)_2 = 2$ and $s_k^{3-5} = (111)_2 = 7$, we can find $F_O(1, 1, 1) = 2$ and $F_I(2, 2, 0) = 7$ that satisfy our embedding rule. The share pixel triplet is therefore $(0 + 3 + 2, 0 + 3 + 2, 0 + 3 + 0) = (5, 5, 3)$ as illustrated in Fig. 6.

For the special cases of $Q = \left[p/6\right] = 42$, i.e., $252 \leq p \leq 255$, the mapped matrix element does not belong to any fractal group. To embed data with a minimal distortion, we round it to the nearest index of $Q = 41$. The share production algorithm is summarized as follows.
C. AUTHENTICATION OF THE SHARES

As discussed in Section 3.1, any two of the participants can recover the secret data by sharing their shares. In order to prevent cheating, two authentication mechanisms are provided.

1) AUTHENTICATION WITH TWO SHARES

Referring to Section 2.2, the central element of each fractal model and the residual space resulted from fractal group stacking are left unnumbered. Projection of the fractal matrix on the xy-plane is illustrated in Fig. 7. Since the fractal groups are duplications of a fundamental fractal group, the overlapped fractal elements at a particular position corresponds to a same element in the fundamental group. Thus a unique secret binary segment can be determined. The positions marked by ‘x’ are vacated in the fractal matrix. Therefore, a proper secret embedded share triplet must project to a color position. A share pixel pair \((p_{1i}, p_{2i})\) which maps to an ‘x’-marked position indicates the existence of a tampered pixel. This principle is valid for projections on all axial planes. An authentication mechanism is devised according to this principle and given as follows.

2) AUTHENTICATION WITH THREE SHARES

When we can obtain all the three shares, more information can be applied to detect a tampered share. A secret embedded share pixel triplet must be the coordinates of a fractal element. Otherwise, a tampering event is detected. Under such circumstances, we can authenticate the three shares pairwise. When a pair has passed the authentication, the remaining one is a

---

**Algorithm 1 Production of the Shares**

| Input: | Cover images \(I_1, I_2, I_3\), where \(I_m = \{p_{mi}\} = 1, 2, \ldots, H \times W\), Secret data \(S = \{s_k\} = 1, 2, \ldots, n\) Secret key \(K\). |
|---|---|
| Output: | shares \(\hat{I}_1, \hat{I}_2, \hat{I}_3\), where \(\hat{I}_m = \{\hat{p}_{mi}\} = 1, 2, \ldots, H \times W\). |
| 1: | Construct the fractal matrix (see Section 2.2) using secret key \(K\). |
| 2: | For each pixel triplet \((p_{1i}, p_{2i}, p_{3i})\), |
| 3: | Retrieve a data segment \(s_k\). |
| 4: | Calculate \(Q_x, Q_y, Q_z\) by Eq. (5). |
| 5: | For all \(Q\), |
| 6: | If \(Q = 42\), modify to \(Q = 41\). |
| 7: | End |
| 8: | Search in the fractal group \(F_G(Q_x, Q_y, Q_z)\) to find \((\hat{\chi}_0, \hat{\gamma}_0, \hat{\zeta}_0)\) and \((\hat{x}_1, \hat{y}_1, \hat{z}_1)\), such that \(F_0(\hat{\chi}_0, \hat{\gamma}_0, \hat{\zeta}_0) = s_k^{1-2}\) and \(F_1(\hat{x}_1, \hat{y}_1, \hat{z}_1) = s_k^{0-5}\). |
| 9: | Calculate the share pixel triplet \((\hat{p}_{1i}, \hat{p}_{2i}, \hat{p}_{3i})\) by Eqs. (9-11). |
| 10: | Record \((\hat{p}_{1i}, \hat{p}_{2i}, \hat{p}_{3i})\) to shares \(\hat{I}_1, \hat{I}_2, \hat{I}_3\). |
| 11: | End |
| 12: | Output shares \(\hat{I}_1, \hat{I}_2, \hat{I}_3\). |
Algorithm 2 Authentication With Two Shares

Input: Shares $\hat{I}_1$, $\hat{I}_2$, where $\hat{I}_m = [\hat{p}_{mi}]i = 1, 2, \ldots, H \times W$. 
Output: Number of tampered pixel pairs $N_F$. 
1: $N_F = 0$. 
2: For each pixel pair $(\hat{p}_{1i}, \hat{p}_{2i})$, 
3: \quad If $(\hat{p}_{1i} \text{ or } \hat{p}_{2i} > 251)$, $F^*$ check boundary */ 
4: \quad \quad $N_F = N_F + 1$. 
5: Else 
6: \quad If $\hat{p}_{1i} \text{mod} 3 = 1 \text{ and } \hat{p}_{2i} \mod 3 = 1$, 
\quad \quad $F^*$ check central element */ 
7: \quad \quad $N_F = N_F + 1$. 
8: End 
9: End 
10: End 
11: Print $N_F$. 
12: If $N_F = 0$, Print “authentication passed.” End

Algorithm 3 Authentication With Three Shares

Input: Shares $\hat{I}_1$, $\hat{I}_2$, and $\hat{I}_3$, where $\hat{I}_m = [\hat{p}_{mi}]i = 1, 2, \ldots, H \times W$. 
Output: Number of tampered pixel triplets $N_F$. 
1: $N_F = 0$. 
2: For each pixel triplet $(\hat{p}_{1i}, \hat{p}_{2i}, \hat{p}_{3i})$, 
3: \quad If $(p_{1i} \text{ or } p_{2i} \text{ or } p_{3i} > 251)$, 
\quad \quad $F^*$ check boundary */ 
4: \quad \quad $N_F = N_F + 1$. 
5: Else 
6: \quad Substitute $(\hat{p}_{1i}, \hat{p}_{2i}, \hat{p}_{3i})$ into Eqs. (5-8) in order to obtain $F_0(x_0, y_0, z_0)$ and $F_1(x_1, y_1, z_1)$ \quad \quad $F_0^*$ \quad $F_1^*$ 
7: \quad If $y_0 = (-x_0 + z_0 + 1)$ mod 2, $F_0^*$ check $F_0^*$/ 
8: \quad \quad If $(y_1 \neq -x_1 + z_1 + 1)$ mod 3 or $(x_1 = y_1 = z_1 = 1)$, $F_1^*$ $F_1^*$ 
9: \quad \quad $N_F = N_F + 1$. 
10: End 
11: Else 
12: \quad $N_F = N_F + 1$. 
13: End 
14: End 
15: End 
16: Print $N_F$. 
17: If $N_F = 0$, Print “authentication passed.” End

Algorithm 4 Extraction of Secret Data

Input: Shares $\hat{I}_a$ and $\hat{I}_b$, where $\hat{I}_m = [\hat{p}_{mi}]i = 1, 2, \ldots, H \times W$, Secret key $K$. 
Output: Secret data $S = [s_k]k = 1, 2, \ldots, n$. 
1: Construct the fractal matrix (see Section 2.2) using secret key $K$. 
2: Project $F_0(x_0, y_0, z_0)$ and $F_1(x_1, y_1, z_1)$ onto $ab$-plane to obtain $F_{Oab}(\hat{a}_0, \hat{b}_0)$ and $F_{lab}(\hat{a}_1, \hat{b}_1)$. 
3: For each pixel pair $(\hat{p}_{ai}, \hat{p}_{bi})$, 
4: \quad Substitute $(\hat{p}_{ai}, \hat{p}_{bi})$ into Eqs. (4)-(6) to obtain $(\hat{a}_0, \hat{b}_0), (\hat{a}_1, \hat{b}_1)$. 
5: Extract secret digits by $s_k^{5-2} = F_{Oab}(\hat{a}_0, \hat{b}_0), s_k^{3-5} = F_{lab}(\hat{a}_1, \hat{b}_1)$. 
6: Record $s_k$ to $S$. 
7: End 
8: Output $S$. 

tampered share. When there are no pairs of shares that can pass the authentication, it indicates that at least two shares are tampered with and that the secret is lost. The details of the algorithm are given as follows.

D. EXTRACTION OF SECRET DATA

Any two shares that have been passed the authentication can cooperate to extract secret data. Each corresponding pixel pair retrieved from the two shares can be applied to extract a secret segment. The extraction algorithm is provided as follows.

IV. EXPERIMENTAL RESULTS

In this experimental section, we will evaluate the performance of our SIS scheme. The 12 standard gray images of size $512 \times 512$ used in our experiment are shown in Fig. 8. All programs are implemented with MATLAB R2018a.

A. VISUAL QUALITY

In order to evaluate the visual quality of the shares generated by our SIS scheme, we use two evaluation indicators, PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity). The formula for PSNR is as follows:

$$PSNR = 10 \log_{10} \left( \frac{255^2 \times H \times W}{\sum_{H \times W} (p_i - p_j)^2} \right) \text{ (dB)},$$

(12)

where $H$ and $W$ represent the height and width of the two images, and $p_i$ and $p_j$ represent the corresponding pixels in the two images. In general, if the PSNR value of the share and the cover image exceeds 30dB, it is difficult for human eyes to distinguish the difference between two images.

The formula for SSIM is as follows:

$$SSIM \left( P, P^* \right) = \frac{(2\mu_P \mu_{P^*} + c_1)(2\sigma_{PP} + c_2)}{\left( \mu_{P}^2 + \mu_{P^*}^2 + c_1 \right) \left( \sigma_{P}^2 + \sigma_{P^*}^2 + c_2 \right)},$$

(13)

where $P$ and $P'$ represent the cover image and the share, respectively; $\mu_P$ and $\mu_{P'}$ represent the average of $P$ and $P'$, respectively; $\sigma_P^2$ is the variance of $P$, $\sigma_{PP}$ is the variance of $P'$ and $\sigma_{PP'}$ is the covariance of $P$ and $P'$; and $c_1$ and $c_2$ are constants used to maintain stability of the formula. $c_1$ and $c_2$ can be obtained by Eqs. (14) and (15), respectively, where $L$
is the dynamic range of pixel values, $k_1 = 0.01$, $k_2 = 0.03$.

\begin{align*}
  c_1 &= (k_1L)^2, \\
  c_2 &= (k_2L)^2.
\end{align*}

Since the three shares generated by our SIS scheme are only minor modifications to the pixels of the three cover images, the image quality of the shares should be excellent in theory. To confirm this, Fig. 9 shows the first experimental results. The secret image “Airplane” with a size of $256 \times 256$ (see Fig. 9(a)) is embedded into three cover images “Coach”, “Lena” and “Barbara” with the size of $512 \times 512$ (see Fig. 9(b)-(d)). After full embedding, the three high-quality shares are generated with $PSNR$ values of $44.36 \, dB$, $44.39 \, dB$ and $44.39 \, dB$, respectively (see Figs. 9(e)-(g)). As shown in Fig. 9(h), the secret image can be recovered losslessly as long as there are no tampered shares.

The visual quality of the shares generated by our SIS scheme are listed in Table 1, where random bit streams are used as the secret data. In this case, the $PSNR$ value is
The embedding capacity is increased to 5 bits per cover pixel pair with only a slight reduction in the quality of the shares. Table 2 compares the features of our scheme with other SIS schemes. SIS schemes based on modern lightweight computing focus on generating meaningful shares with good visual quality and large embedding capability. As shown in the table, the features of reversibility and different cover images are mutually contradictory. To recover distinct cover images requires three times the information of a single cover image. It is not worth doing, since the cover images are just used for covering the secret transmission. In addition, the attacker can analyze information from the difference of secret shares generated with a single cover image. Therefore, the single cover image-based schemes are more vulnerable under steganalysis. Our proposed scheme provides three most striking features are the complete difference of the cover images, the extremely high embedding capacity and the (2, 3) secret sharing.
An advantage of our scheme is that, if one of the shares is invalid, we can use the other two shares to completely recover the secret data, but in the traditional SIS scheme, the secret data cannot be recovered at all. Therefore our scheme provides fault tolerance that the traditional SIS schemes do not have.
In order to test the authentication ability of the two authentication mechanisms proposed in our scheme, we assume that three shares 1, 2 and 3 are distributed to participants 1, 2 and 3, respectively. Suppose the share of participant 1 is fake, and the shares of participant 2 and 3 are real. When participants 1 and 2 want to cooperate to retrieve the secret data, participant 2 can verify whether participant 1 is dishonest. Here, we use the $DR$ (detection rate) to measure the authentication ability of the two authentication mechanisms. The formula of $DR$ is defined as:

$$DR = \frac{N_d}{N_t},$$  \hspace{1cm} (16)

where $N_d$ represents the number of illegal pixels detected by the authentication mechanism, and $N_t$ represents the total number of illegal pixels.

Next, we use two examples to illustrate the two authentication mechanisms which are proposed in our scheme. Referring to Fig. 10, a hostile image “Airplane” (see Fig. 10(a)) is inserted into share 1 in “Coach” (see Fig. 10(b)). The result

| Features                        | Gao et al.’s scheme [36] | Chang et al.’s scheme [29] | Li et al.’s scheme [32] | Liu et al.’s scheme [31] | Liu et al.’s scheme [34] | Proposed scheme |
|---------------------------------|---------------------------|----------------------------|-------------------------|--------------------------|--------------------------|----------------|
| Meaningful shares               | Yes                       | Yes                        | Yes                     | Yes                      | Yes                      | Yes            |
| Reversibility                   | Yes                       | -                          | Yes                     | Yes                      | -                        | -              |
| Different cover images          | -                         | Yes                        | -                       | -                        | Yes                      | Yes            |
| $(k, n)$ - SIS                  | (2, 3) - SIS              | (2, 2) - SIS               | (3, 3) - SIS            | (2, 2) - SIS             | (2, 2) - SIS             | (2, 3) - SIS   |
| Fault tolerance                 | Yes                       | -                          | -                       | -                        | -                        | Yes            |
| Average PSNR                    | 32.96                     | 39.88                      | 49.07                   | 48.72                    | 41.71                    | 40.41          |
| Embedding capacity(bits)        | 786432                    | 1048576                    | 624215                  | 524288                   | 785525                   | 1310720        |
of using real share 2 “Lena” (see Fig. 10(c)) to verify the share 1, the result is shown in Fig. 10(d). The black pixels represent the ones where tampering has been detected.

The second example is shown in Fig. 11, where the hostile image and the tampered share are shown in Figs. 11(a) and (b), respectively. With the help of two real shares (see Figs. 11(c) and (d)), the detection result is shown in Fig. 11(e). From the results, we can see that our scheme has a good ability to detect tampering.

When we can obtain all three shares, more information can be applied to detect a tampered share. A secret embedded share pixel triplet must be the coordinates of a fractal
element. Otherwise, a tampering event is detected. Under such circumstances, we can authenticate the three shares pairwise. As shown in Fig. 12, when a pair has passed the authentication, the remaining one is a tampered share. When there are no pairs of shares that can pass the authentication, it indicates that at least two shares are tampered with and that the secret is lost.

To investigate the authentication ability of the proposed mechanisms, the DR values for different experimental image sets (see Fig. 13) are listed in Table 3. Since there is a trade-off between embedding capacity and authentication ability for reference matrix-based schemes, the detection rate for authentication with two shares is relatively low. However, the authentication is processed pixel-wise. A small tampering patch consists of hundreds or even thousands of pixels. It is almost impossible to pass the authentication. When all three shares can be obtained, the detection rate can be greatly improved. In fact, the third pixel value of a triplet can be uniquely determined within the whole space of a particular fractal group.
C. SECURITY ANALYSIS

In order to analyze the security of the proposed scheme, pixel-value differencing steganalysis [37] is applied. The histograms of pixel-value difference are shown in Figs. 14, where the test cover images are ‘Baboon’, ‘Lena’, and ‘Zelda’. The histograms of the fully embedded stego-images are very close to the histograms of the cover images, which indicates that the proposed scheme is secure under the steganalysis of pixel-value differencing.

V. CONCLUSION

In this paper, a novel (2, 3) SIS scheme based on three distinct cover images and the fractal matrix has been proposed. Our scheme has good security and authentication ability. The scheme has the following features: (1) the three shares are generated based on the three distinct cover images, (2) the shares generated by our scheme have high visual quality, (3) it provides two effective authentication mechanisms, and (4) any two of the three shares can cooperate to extract the secret data losslessly. Experimental results show that the proposed (2, 3) SIS scheme can achieve good embedding capacity with a satisfactory visual quality of the shares.

Our future work will try to generalize the (2, 3) SIS scheme into a \((k, n)\) SIS scheme of arbitrary selected parameter set, where \(k < n\). The principle is to choose a set of elements within a properly sized \(n\)-dimensional matrix in a way that their projections into any \(k\)-dimensional subspace are not overlapped. This set of elements can be applied as a group for embedding, which guarantees extractable using arbitrarily selected \(k\) shares.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Syst. J., vol. 35, nos. 3–4, pp. 313–336, 1996.

[2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[3] C.-C. Chang, “Adversarial learning for invertible steganography,” IEEE Access, vol. 8, pp. 198425–198435, Oct. 2020.

[4] M. He, Y. Liu, C.-C. Chang, and M. He, “A mini-Sudoku matrix-based data embedding scheme with high payload,” IEEE Access, vol. 7, pp. 141414–141425, 2019.

[5] J.-H. Horng, S. Xu, C.-C. Chang, and C.-C. Chang, “An efficient data-hiding scheme based on multidimensional mini-Sudoku,” Sensors, vol. 20, no. 9, p. 2739, May 2020.

[6] C.-C. Chang, C.-T. Li, and Y.-Q. Shi, “Privacy-aware reversible watermarking in cloud computing environments,” IEEE Access, vol. 6, pp. 70720–70733, 2018.

[7] X. Gao, Z. Pan, E. Gao, and G. Fan, “Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction,” Signal Process., vol. 173, Aug. 2020, Art. no. 107579.

[8] C.-C. Chang, C.-T. Li, and K. Chen, “Privacy-preserving reversible information hiding based on arithmetic of quadratic residues,” IEEE Access, vol. 7, pp. 54117–54132, 2019.

[9] C.-C. Chang and Y. Liu, “Fast turtle shell-based data embedding mechanisms with good visual quality,” J. Real-Time Image Process., vol. 16, no. 3, pp. 589–599, Jun. 2019.

[10] S. Weng, Y. Shi, W. Hong, and Y. Yao, “Dynamic improved pixel value ordering reversible data hiding,” Inf. Sci., vol. 489, pp. 136–154, Jul. 2019.

[11] C.-C. Chang, T.-C. Lu, G. Horng, Y.-H. Huang, and Y.-M. Hsu, “A high payload data embedding scheme using dual stego-images with reversibility,” in Proc. 9th Int. Conf. Inf., Commun. Signal Process., Tainan, Taiwan, Dec. 2013, pp. 1–5.

[12] C. C. Chang, Y. Liu, and T. S. Nguyen, “A novel turtle shell based scheme for data hiding,” in Proc. 10th Int. Conf. Inf., Intern. Hiding Multimedia Signal Process., Kita Kyushu, Japan, Aug. 2014, pp. 89–93.

[13] F. Li, Q. Mao, and C.-C. Chang, “A reversible data hiding scheme based on IWT and the SuDoku method,” Int. J. Netw. Secur., vol. 18, no. 3, pp. 410–419, 2014.

[14] H. Zhang and L. T. Hu, “A data hiding scheme based on multidirectional line encoding and integer wavelet transform,” Signal Process., Image Commun., vol. 78, pp. 331–344, Oct. 2019.

[15] C.-Y. Yang and W.-C. Hu, “Reversible data hiding in the spatial and frequency domains,” Int. J. Image Process., vol. 3, no. 6, pp. 373–384, 2010.

[16] X.-Z. Xie, C.-C. Chang, and K. Chen, “A high-embedding efficiency RDH in encrypted image combining MSB prediction and matrix encoding for non-volatile memory-based cloud service,” IEEE Access, vol. 8, pp. 52028–52040, 2020.

[17] M. Long, Y. Zhao, X. Zhang, and F. Peng, “A separable reversible data hiding scheme for encrypted images based on tremolo scrambling and adaptive pixel value ordering,” Signal Process., vol. 176, Nov. 2020, Art. no. 107703.

[18] Z. Qian, X. Zhang, and S. Wang, “Reversible data hiding in encrypted JPEG bitstream,” IEEE Trans. Multimedia, vol. 16, no. 5, pp. 1486–1491, Aug. 2014.

[19] Z. Qian, H. Xu, X. Luo, and X. Zhang, “New framework of reversible data hiding in encrypted JPEG bitstreams,” IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 351–362, Feb. 2019.

[20] F. Huang, X. Qu, H. Kim, and J. Huang, “Reversible data hiding in JPEG images,” IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 9, pp. 1610–1621, Sep. 2016.

[21] X. Wang, C.-C. Chang, and C.-C. Lin, “Adaptive reversible data hiding scheme for AMBTC compressed images,” Multimedia Tools Appl., vol. 79, nos. 9–10, pp. 6547–6568, Mar. 2020.

[22] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[23] G. R. Blakley, “Safeguarding cryptographic keys,” in Proc. Int. Workshop Meeting Requirements Know., (MARK), New York, NY, USA, Jun. 1979, pp. 313–317.

[24] M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 950, A. De Santis, Ed. Berlin, Germany: Springer, 1995, doi: 10.1007/BFb0053419.

[25] K. Jainti and P. Prabhu, “A novel cryptographic technique that emphasis visual quality and efficiency by Floyd steinberg error diffusion method,” Int. J. Res. Eng. Technol., vol. 4, no. 2, pp. 428–439, 2015.

[26] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” J. WSCG, vol. 10, nos. 1–2, pp. 303–310, 2002.

[27] I. Kang, G. R. Arce, and H.-K. Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.

[28] S. Patil and J. Rao, “Extended visual cryptography for color shares using random number generators,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 1, no. 6, pp. 399–410, 2012.

[29] C.-C. Chang, T. Kieu, and Y.-C. Chou, “Reversible data hiding scheme using two steganographic images,” in Proc. IEEE Region 10 Conf. (TENCON), Taipei, Taiwan, Oct. 2007, pp. 1–4.

[30] C.-C. Chang, P.-Y. Lin, Z. H. Wang, and M. C. Li, “A SuDoku-based secret image sharing method with reversibility,” J. Commun., vol. 5, no. 1, pp. 12–19, 2010.

[31] Y. Liu and C.-C. Chang, “A turtle shell-based visual secret sharing scheme with reversibility and authentication,” Multimedia Tools Appl., vol. 77, no. 19, pp. 25295–25310, Oct. 2018.

[32] X.-S. Li, C.-C. Chang, M.-X. He, and C.-C. Lin, “A lightweight authenticable visual secret sharing scheme based on turtle shell structure matrix,” Multimedia Tools Appl., vol. 79, nos. 1–2, pp. 453–476, Jan. 2020.

[33] H. Qiao, J.-H. Horng, Y. Liu, and C.-C. Chang, “A reversible secret image sharing scheme based on stick insect matrix,” IEEE Access, vol. 8, pp. 130405–130416, 2020.

[34] Y. J. Liu, C.-C. Chang, and P. C. Huang, “Security protection using two different image shadows with authentication,” Math. Biosci., vol. 16, no. 4, pp. 1914–1932, 2009.

[35] C.-C. Chang, J.-H. Horng, C.-S. Shih, and C.-C. Chang, “A maze matrix-based secret image sharing scheme with cheater detection,” Sensors, vol. 20, no. 15, p. 3802, Jul. 2020.
K. Gao, J.-H. Horng, and C.-C. Chang, “A novel (2, 3) reversible secret image sharing based on fractal matrix,” IEEE Access, vol. 8, pp. 174325–174341, 2020.

X. Zhang and S. Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security,” Pattern Recognit. Lett., vol. 25, no. 3, pp. 331–339, Feb. 2004.

KAI GAO received the B.S. degree in software engineering from Fujian Normal University, Fuzhou, China, in 2018. He is currently pursuing the Ph.D. degree with Feng Chia University. His current research interests include information security and information hiding.

JI-HWEI HORNG received the B.S. degree from the Department of Electronic Engineering, Tamkang University, Taipei, Taiwan, in 1990, and the M.S. and Ph.D. degrees from the Department of Electrical Engineering, National Taiwan University, Taipei, in 1992 and 1996, respectively. He was a Professor and the Chairman of the Department of Electronic Engineering, from 2006 to 2009, and the Dean of the College of Science and Engineering, from 2011 to 2014, with National Quemoy University (NQU), Kinmen, Taiwan. He is currently the Vice President of the Academic Affairs with NQU. His research interests include image processing, pattern recognition, information security, and artificial intelligence.

CHIN-CHEN CHANG (Fellow, IEEE) received the B.S. degree in applied mathematics and the M.S. degree in computer and decision sciences from National Tsing Hua University, and the Ph.D. degree in computer engineering from National Chiao Tung University. From 1989 to 2005, he was with the National Chung Cheng University. He is currently the Chair Professor of the Department of Information Engineering and Computer Science, Feng Chia University. Prior to joining Feng Chia University, he was an Associate Professor with National Chiao Tung University, a Professor with National Chung Hsing University, and the Chair Professor with National Chung Cheng University. He has been a Visiting Researcher with The University of Tokyo, Japan, and a Visiting Scientist with Kyoto University, Japan. During his service in National Chung Cheng University, he served as the Chairman for the Institute of Computer Science and Information Engineering, the Dean for the College of Engineering, a Provost, the Acting President for National Chung Cheng University, and the Director for Advisory Office in Ministry of Education, Taiwan. His current research interests include database design, computer cryptography, image compression, and data structures. He has won many research awards and has honorary positions in prestigious organizations both nationally and internationally. Since his early years of career development, he has consecutively won awards, including the Outstanding Talent in Information Sciences of the R.O.C., the Acer Dragon Award of the Ten Most Outstanding Talents, the Outstanding Scholar Award of the R.O.C., the Outstanding Engineering Professor Award of the R.O.C., the Distinguished Research Awards of National Science Council of the R.O.C., and the Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software. On numerous occasions, he has been invited to serve as a visiting professor, the chair professor, the honorary professor, the honorary director, the honorary chairman, the distinguished alumnus, the distinguished researcher, and a research fellow by various universities and research institutes.

* * *

VOLUME 9, 2021