


Article

A Novel Hierarchical Secret Image Sharing Scheme with Multi-Group Joint Management

Zhen Wu ^{1,†}, Yining Liu ^{1,2,*,†}  and Xingxing Jia ^{2,3,†}

¹ School of Information and Communication, Guilin University of Electronic Technology, Guilin 451000, China; wuzhen0610@gmail.com

² Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 451000, China

³ School of Mathematics and Statistics, Lanzhou University, Lanzhou 730000, China; jiaxx@lzu.edu.cn

* Correspondence: ynliu@guet.edu.cn

† These authors contributed equally to this work.

Received: 20 February 2020; Accepted: 16 March 2020; Published: 19 March 2020



Abstract: With the spread of the Internet, the speed of data spread is getting faster and faster. It benefits us a lot but also brings us many potential security problems, especially the problem of privacy leakage. For example, more and more people choose to store their private images in the cloud. Secret image sharing as a significant method has been widely applied in protecting images in the cloud, which reduces the risks of data leakage and data loss. Generally, the secret image sharing scheme would encrypt the secret image into a series of shares and then stored these shares in a cloud. However, when this cloud has been attacked, the secret may meet a risk of leakage. A solution to solve the problem is that the generated shares are distributed storage in multiple clouds. Each cloud is independent and all clouds can have a collaboration to manage the secret image. To address this issue, a novel hierarchical secret image sharing scheme with multi-group joint management is proposed in this paper, which is suitable for protecting the security of the secret image by distributed storage over multiple clouds. In the proposed scheme, the secret image would be shared among multiple groups with different thresholds. The number of each group's shareholders is determined by a sequence of thresholds. Therefore, the proposed scheme is a hierarchical secret image sharing scheme in which the secret image can be reconstructed if and only if the number of shares has met all threshold conditions. In addition, the generated shares have the same weight, which is more suitable for universal applicability. Both the system analysis and the simulation results prove that the proposed scheme is efficient and practical.

Keywords: hierarchical secret image sharing; multi-group joint management; interpolation algorithm; Birkhoff interpolation

1. Introduction

With the rapid development of information sciences, the speed of data spread is getting faster and faster. It benefits us a lot but also brings us many potential security problems in the aspect of privacy leakage. For example, the private photos disclosed on social networking sites [1–3], the electricity consumption data disclosed by a smart grid [4], the user's data in IoT [5,6] and so on. How to protect secret data transmitted in the network becomes an urgent problem.

Secret sharing (SS) is a significant encryption technology to protect secret data [7]. Generally speaking, the most commonly used secret sharing is the (t, n) SS scheme. It encrypts the secret data into n shares and then sent to n shareholders. Only no less than t shareholders with collaboration can decrypt and obtain the secret data. In this way, the secret data can be stored in

a distributed way, which is more secure than centralized storage. With the rapid development of multimedia technology, secret sharing is used in a vast range of multimedia and secret image sharing is one of its important applications. In 2002, Thien and Lin proposed a (t, n) secret image sharing (SIS) scheme to protect the secret image [8]. In Thien and Lin's scheme, a secret image is first permuted and then divided into several blocks. Each block has t non-overlapped pixels which would be used to construct a $(t - 1)$ degree sharing function $f(x)$. The pixel value in each share is $f(1), f(2), \dots, f(n)$, respectively. Finally, these random-looking shares would be sent to shareholders, respectively. In the reconstruction procedure, the secret image can be reconstructed based on Lagrange interpolation if and only if no less than t shareholders collaborate. Actually, all operations in Thien and Lin's scheme are over the finite field F_p , where p is a prime number and is usually selected as $p = 251$. Therefore, all pixel values larger than 250 in the secret image are truncated to 250, which would result in a distortion of the reconstructed secret image. Soon afterward, Wu and Kanso et al. attempted to improve the quality of the reconstructed secret image in different ways [9,10], respectively. However, the reconstructed secret image still has a distortion problem. In fact, the problem of distortion in an image is not allowed in many areas, such as medical images and military drawings. In order to solve this problem, a Galois Field $GF(p)$ would be employed in secret image sharing to acquire a lossless secret image. Recently, most of secret image sharing schemes [11–13] choose the finite field $GF(2^8)$ as the prime polynomial for a gray image, which corresponds to the irreducible polynomial is $x^8 + x^5 + x^3 + x^2 + 1$.

Except by Lagrange interpolation, secret sharing can also be realized in many ways. Yan et al. provided a secret image sharing with a general access structure based on Chinese remainder theorem (CRT) [14]. Jia et al. proposed a novel secret sharing scheme based on CRT in which the threshold is changeable [15]. Mashhadi and Samaneh proposed a secure publicly verifiable and proactive secret sharing scheme based on bilinear pairings and monotone span programs [16]. Deshmukh et al. proposed an efficient and secure multiple secret sharing scheme based on boolean XOR and arithmetic modulo [17].

All of the schemes discussed above require all shareholders belonging to a group, such as a party, a company or a government. Actually, the secret image may be managed jointly by multiple groups. For example, all the above schemes assume that each shareholder is considered to have the same priority. Actually, many scenarios require to assign different privileges to different participants. It is necessary to develop the secret image sharing such that the generated shares in several groups can be allocated with different weights. Hierarchical secret image sharing (HSIS) solves this problem. In 2007, Tassa provided a method for constructing a hierarchical secret sharing scheme which constructs a polynomial from a set of unstructured points and derivative values [18]. Employing Tassa's hierarchical secret sharing scheme, Guo et al. proposed a HSIS scheme in which the generated shares are partitioned into several levels, and the threshold access structure is determined by a sequence of threshold requirements [19]. However, Guo et al.'s scheme may arise a risk that the secret image would be partially reconstructed when some non-authorized shareholders attempt to attack the secret image. To overcome this drawback, Pakniat et al. proposed an improved HSIS scheme [20], which improves the level of security by utilizing the cellular automata and hash function. In 2018, Bhattacharjee et al. proposed a HSIS scheme which can generate fixable shares by utilizing the compressed sensing [21]. Besides, considered that some shareholders may not just be involved in a secret sharing scheme and assigned multiple shares, Jia et al. proposed collaborative secret sharing scheme in which each shareholder just keep only one share can participate in multiple secret sharing schemes [22].

Actually, even if the secret image has been processed in the above manner, the protection against the secret image leakage may not be achieved. Suppose that a provider of the cloud storage is dishonest. Then, it is possible for it to obtain the secret image by collecting enough shares. Thus, it is necessary that the generated shares can be distributed storage in multiple clouds. Therefore, a novel hierarchical secret image sharing scheme with multi-group joint management is proposed in this paper. The proposed scheme is more suitable for protecting the security of the secret image by distributed storage over multiple clouds, which can resist shares leakage from one cloud. In the proposed scheme, by combining

the threshold secret image sharing scheme and the derivation operation, the secret image would be shared among multiple groups with different thresholds. The proposed scheme is a hierarchical secret image sharing scheme in which the secret image can be reconstructed if and only if the number of shares has met each threshold. The highlights of this paper are as follows

1. The secret image can be jointly managed by multiple groups.
2. The proposed scheme has a hierarchical threshold access structure .
3. Shares have a same size and same weight.

The outline of this paper is organized as follows. Section 2 presents some basic descriptions of preliminaries. Section 3 presents the proposed scheme in detail. The security analysis of the proposed scheme is presented in Section 4. The simulations and comparison are presented in Section 5, and the conclusion of this paper is presented in Section 6.

2. Preliminaries

In this section, there are some preliminaries reviewed including Shamir's secret sharing scheme [7] and Guo's hierarchical threshold secret image sharing scheme [19].

2.1. Review of Secret Sharing

Shamir's secret sharing scheme is a (t, n) threshold scheme, which is based on the polynomial interpolation. All operations are performed over the finite field F_p , p is a secure big prime. In Shamir's scheme, the dealer encrypts a secret data s into n shares s_i , $i = 1, 2, \dots, n$, and sends these them to n shareholders U_i , respectively. The access structure refers to the qualified subset holding at least t shares which can recover the secret. Shamir's (t, n) secret sharing scheme includes two procedures: shares generation procedure and secret reconstruction procedure, which is introduced as follows.

2.1.1. Shares Generation Procedure

- Step 1.** Given a secret data s , the dealer chooses $t - 1$ random number r_1, r_2, \dots, r_{t-1} and a prime number p , where $s \in F_p$ and $r_1, r_2, \dots, r_{t-1} \in F_p$.
- Step 2.** Construct a $t - 1$ degree function $f(x) = s + r_1x + r_2x^2 + \dots + r_{t-1}x^{t-1} \bmod p$.
- Step 3.** The outputs $y_i = f(x_i)$ are regarded as shares S_i and assigned to the shareholders U_i in a secure channel.

2.1.2. Secret Reconstruction Procedure

- Step 1.** Given a subset of t disparate shares S_i , $i \in A$, $A = \{1, 2, \dots, t\}$, the $t - 1$ degree polynomial can be reconstructed by Lagrange interpolation as formula (1):

$$f(x) = \sum_{i=1}^t y_i \prod_{j=1, j \neq i}^t \frac{x - x_j}{x_i - x_j} \bmod p \quad (1)$$

- Step 2.** The secret data s can be reconstructed by calculating $s = f(0)$.

2.2. Birkhoff Interpolation

Definition 1. Defining that $X = \{x_1, x_2, \dots, x_k\}$, where $x_1 < x_2 < \dots < x_k$. E is a interpolation matrix with binary entries which is defined as $E = (e_{i,j})_{1 \leq i \leq k, 0 \leq j \leq l}$, where $I(E) = \{(i, j) : e_{i,j} = 1\}$ and $N = |I(E)|$. C is a set of N real values which is defined as $C = \{c_{i,j} : (i, j) \in I(E)\}$.

Birkhoff Interpolation Problem. The Birkhoff interpolation problem that corresponds to the triplet $\langle X, E, C \rangle$ is a problem of finding a polynomial $P(x) \in R_{N-1}[x]$ that satisfies the N equalities

$$P^{(j)}(x_i) = c_{i,j}(i, j) \in I(E) \quad (2)$$

where $P^{(j)}(x)$ is the j -th derivative of $P(x)$ and $R_{N-1}[x]$ is the set of all possible polynomials with degree at most $N - 1$.

Theorem 1. Let the Birkhoff interpolation problem that corresponds to the triple $\langle X, E, C \rangle$ be well posed. Then the entries of E satisfy the relation (3)

$$\forall t, (0 \leq t \leq l) : \sum_{j=0}^t \sum_{i=1}^k e_{i,j} \geq (t + 1) \quad (3)$$

where l is the highest derivative order in the data and k is the number of interpolating points [23].

Theorem 2. The interpolation problem (Definition 1) has a unique solution if the interpolation matrix E satisfies Theorem 1, and contains no supported l -sequences of odd length.

Theorem 3. The Birkhoff interpolation problem has a unique solution over the finite field $GF(q)$ if the conditions of the Theorem 2 and the following condition hold simultaneously:

$$q > 2^{-l+2} \times (l-1)^{(l-1)/2} \times (l-1)! \times x_k^{(l-1)(l-2)/2} \quad (4)$$

where l is the highest derivative order in the data.

2.3. Review of Guo's Hierarchical Threshold Secret Image Sharing

In Guo's (t, n) hierarchical threshold secret image sharing [19], the shares generated by the secret image are shared among a set of n shareholders with several levels. The number of each level's shareholders is determined by a sequence of thresholds. The secret image can be reconstructed if and only if the collected shares meet the following two conditions. First, the sum of collected shares is no less than t . Second, the number of the collected shares meets each level's threshold requirement. Guo's (t, n) hierarchical threshold secret image sharing scheme includes two procedures: shares generation procedure and secret image reconstruction procedure.

2.3.1. Shares Generation Procedure

- Step 1.** Given a secret image I , a cover image O sized $M \times N$, and a set of n shareholders $U = \{U_1, U_2, \dots, U_n\}$. The n shareholders are classified into $(m + 1)$ levels L_0, L_1, \dots, L_m with the corresponding threshold requirement $\{t_0, t_1, \dots, t_m\}$, where $t_m = t, 0 < t_0 < t_1 < \dots < t_m$.
- Step 2.** Every t_m non-lapped pixels $\{s_0, s_1, \dots, s_{t_m-1}\}$ in the secret image I are grouped as a section. For each section, a $(t - 1)$ degree function can be constructed as $f(x) = s_0 + s_1x + s_2x^2 + \dots + s_{t_m-1}x^{t_m-1} \bmod p$, the outputs are shadow images of the first level L_0 .
- Step 3.** The shadow images in the hierarchy L_r can be generated by computing $f^{(t_r-1)}(x)$.
- Step 4.** Denote the pixel values in the cover image O as o_j , where $j \in [1, M \times N]$. The dealer chooses a pair of parameters (k, σ) satisfying the relation:

$$\lfloor \frac{o_j}{k} \rfloor \times k + \sigma \leq 255 \quad (5)$$

- Step 5.** Each shadow image SH_i can be transformed a σ -bit stream as $SH_i = (y_{i,1}, y_{i,2}, \dots, y_{i,w})_\sigma$, where $w = \lceil \log_\sigma SH_i \rceil$. The w pixels $o_{i,j}, j \in [1, w]$ in stego images O_i can be generated by replacing w pixels $o_{i,j}$ as:

$$\begin{aligned}
o'_{i,1} &= \lfloor \frac{o_{i,1}}{k} \rfloor \times k + y_{i,1} \\
o'_{i,2} &= \lfloor \frac{o_{i,2}}{k} \rfloor \times k + y_{i,2} \\
&\dots \\
o'_{i,w} &= \lfloor \frac{o_{i,w}}{k} \rfloor \times k + y_{i,w}
\end{aligned} \tag{6}$$

Step 6. The generated n stego images O'_i are regarded as the n shares S_i , $i \in 1, 2, \dots, t$ and sent to shareholders, respectively.

2.3.2. Secret Image Reconstruction Procedure

Step 1. Given a subset of t disparate shares, the t disparate shadow images SH_i , can be extracted from shares S_i , $i \in 1, 2, \dots, t$, according the formula (7)

$$SH_i = y_{i,1} \parallel y_{i,2} \parallel \dots \parallel y_{i,w}. \tag{7}$$

Step 2. The secret image I can be reconstructed by employing Birkhoff interpolation with t disparate shadow images.

3. The Proposed Scheme

This section presents a novel hierarchical secret image sharing (HSIS) scheme with multi-group joint management in detail. The secret image in the proposed scheme is shared among multiple groups. Each group is independent and includes several shareholders. To protect the secret image, any group cannot reconstruct the secret image without other group's cooperation.

The definition of multiple groups, the threshold requirement of each group and the conditions of the number of collected shareholders in the secret image reconstruction procedure are presented as follows.

Definition 2. Given a secret image I , supposing that the secret image I is shared with two groups G_1 and G_2 . Suppose that G_1 consists of n_1 shareholders and G_2 consists of n_2 shareholders, which are denoted as $G_1 = \{U_i^1\}$, $G_2 = \{U_j^1\}$, $i \in [1, n_1]$, $j \in [1, n_2]$, $n = n_1 + n_2$. Besides, each group has a corresponding threshold requirement. Supposing the threshold requirement of G_1 is t_1 and the threshold requirement of G_2 is t_2 , where $t = t_1 + t_2$. Supposing that $|A|$ denotes the cardinality of any set A . To reconstruct the secret image, the number of collected shareholders must satisfy following conditions: (1) $|G_1| \geq t_1$; (2) $|G_2| \geq t_2$; (3) $|G_1| + |G_2| \geq t$. The proposed scheme includes two procedures: shares generation procedure and secret image reconstruction procedure.

3.1. Shares Generation Procedure

Step 1. Employ a reversible permutation operation on the secret image I to acquire a permuted secret image \hat{I} . It is necessary to reduce the association between adjacent pixels.

Step 2. Every t non-lapped pixels a_0, a_1, \dots, a_{t-1} are separated as a unit, and each unit can be used to construct a $t - 1$ degree function $f(x)$ as follows:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \bmod(2^8). \tag{8}$$

Step 3. Repeat the step 2 until all pixels have been processed, and the intermediate shadows T_i^1 for G_1 can be generated by computing $T_i^1 = f(i)$.

Step 4. Calculate t_1 -th derivative of $f(x)$ in the step 2, the derivation is shown as:

$$g(x) = f^{(t_1)}(x) = b_0 + b_1x + \dots + b_{t_2-1}x^{t_2-1} \bmod(2^8). \tag{9}$$

The results of $S_j^2 = g(j)$ are the pixel values in shares and the generated shares would be sent to the shareholders in G_2 .

Step 5. Obtain the mask shadow $R = b_0 \times b_1 \times \cdots \times b_{t_2-1} \bmod(2^8)$.

Step 6. The shares S_i^1 sent to G_1 can be generated by $S_i^1 = (T_i^1 + R) \bmod(2^8)$.

3.2. Shares Generation Procedure

Step 1. Given a subset of t disparate shares includes t_1 shares from G_1 and t_2 shares from G_2 . Using t_2 shares from G_2 , the coefficients of $g(x)$ can be reconstructed by Birkhoff interpolation and the mask shadow R can be obtained by $R = b_0 \times b_1 \times \cdots \times b_{t_2-1} \bmod(2^8)$.

Step 2. When G_2 has been calculated to generate the mask shadow R , the mask shadow R will be sent to G_1 , and the t_1 intermediate shadows $T = (S^1 - R) \bmod(2^8)$ in G_1 can be reconstructed.

Step 3. By utilizing t_1 shares from G_1 and t_2 shares from G_2 , the permuted secret image \hat{I} can be reconstructed by employing Birkhoff interpolation.

Step 4. The secret image I can be reconstructed by employing the corresponding inverse-permutation on the permuted secret image \hat{I} .

4. Security Analysis

The security of the proposed scheme is mainly focuses on the security of the secret image. We will analyse the security of the secret image when the number of collected shareholders whether or not satisfy the threshold conditions: (1) $|G_1| \geq t_1$; (2) $|G_2| \geq t_2$; (3) $|G_1| + |G_2| \geq t$. The entire analysis process consists of the following three scenarios:

Case 1: $|G_1| < t_1, |G_2| \geq t_2, |G_1| + |G_2| \geq t$;

Case 2: $|G_1| \geq t_1, |G_2| < t_2, |G_1| + |G_2| \geq t$;

Case 3: $|G_1| \geq t_1, |G_2| \geq t_2, |G_1| + |G_2| \geq t$;

Case 1. When $|G_1| < t_1, |G_2| \geq t_2, |G_1| + |G_2| \geq t$, the secret image cannot be reconstructed.

Proof. Supposing $|G_1| = l_1 < t_1, |G_2| = l_2 \geq t_2$ and $|G_1| + |G_2| = l_1 + l_2 \geq t$. In the secret image reconstruction procedure, first $l_2 (l_2 \geq t_2)$ collected shareholders in G_2 can reconstruct the function $g(x) = f^{(t_1)}(x) = b_0 + b_1x + \cdots + b_{t_2-1}x^{t_2-1} \bmod(2^8)$ based on the Birkhoff interpolation. As the coefficients $b_0, b_1, \dots, b_{t_2-1}$ can deduce t_2 coefficients $a_{t_1}, a_{t_1+1}, \dots, a_{t-1}$ in $f(x)$, and the number of coefficients in $f(x)$ is $t = t_1 + t_2$, there still t_1 coefficients in $f(x)$ are unknown. Meanwhile, the mask shadow R can be acquired as $R = b_0 \times b_1 \times \cdots \times b_{t_2-1} \bmod(2^8)$, and then G_2 will send the mask shadow to the involved l_1 shareholders in G_1 . For $|G_1| = l_1 < t_1$ less than t_1 intermediate shadows can be reconstructed, the function $f(x)$ cannot be reconstructed correctly. Therefore, even $|G_2|$ meet the threshold condition, the secret image cannot be reconstructed. \square

Case 2. When $|G_1| \geq t_1, |G_2| < t_2, |G_1| + |G_2| \geq t$, the secret image cannot be reconstructed.

Proof. Supposing $|G_1| = l_1 \geq t_1, |G_2| = l_2 < t_2$ and $|G_1| + |G_2| = l_1 + l_2 \geq t$. Since there are only l_2 shareholders in G_2 participating in reconstructing the secret image, the function $g(x)$ cannot be reconstructed. Therefore, the mask shadow R also cannot be obtained. Therefore, even there are l_1 shareholders in G_1 participating the secret image reconstruction procedure, the secret image still cannot be reconstructed. Therefore, only $|G_1|$ meets the threshold condition, the secret image cannot be reconstructed. \square

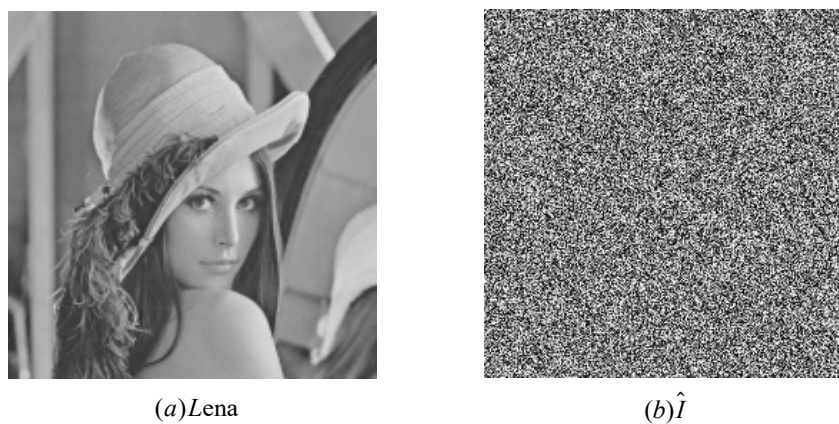
Case 3. When $|G_1| \geq t_1, |G_2| \geq t_2, |G_1| + |G_2| \geq t$, the secret image can be reconstructed.

Proof. Supposing $|G_1| = l_1 \geq t_1, |G_2| = l_2 \geq t_2$ and $|G_1| + |G_2| = l_1 + l_2 \geq t$. In the secret image reconstruction procedure, $l_2 (l_2 \geq t_2)$ collected shareholders in G_2 can reconstruct the function $g(x) = f^{(t_1)}(x) = b_0 + b_1x + \cdots + b_{t_2-1}x^{t_2-1} \bmod(2^8)$ based on the Birkhoff interpolation. Since t_2 coefficients $b_0, b_1, \dots, b_{t_2-1}$ can deduce t_2 coefficients $a_{t_1}, a_{t_1+1}, \dots, a_{t-1}$ in $f(x)$, and the number of coefficients in $f(x)$ is $t = t_1 + t_2$, there still t_1 coefficients in $f(x)$ are unknown. Meanwhile, the mask shadow R can

be acquired as $R = b_0 \times b_1 \times \cdots \times b_{t_2-1} \bmod(2^8)$, and then the mask shadow would be sent to the involved l_1 shareholders in G_1 , and G_1 can reconstruct l_1 intermediate shadows. All l_1 intermediate shadows and $g(x)$ can be used to reconstruct $f(x)$, thus, permuted secret image can be recovered. The secret image can be reconstructed after performing the reversible permutation operation on permuted secret image. Therefore, only when both G_1 and G_2 meet the threshold condition, the secret image can be reconstructed. \square

5. Simulation and Comparison

Supposing there are two independent groups G_1 and G_2 , where G_1 consists of three shareholders and G_2 consists of four shareholders. Denoting $G_1 = \{U_i^1\}$, $G_2 = \{U_j^2\}$, $i \in [1, 3]$, $j \in [1, 4]$, $n = 7$. Besides, each group has its corresponding threshold requirement. Suppose the threshold of G_1 is $t_1 = 2$ and the threshold of G_2 is $t_2 = 2$, where $t = t_1 + t_2 = 4$, the simulation results are shown in Figure 1.



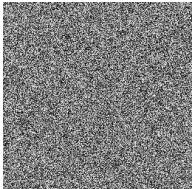
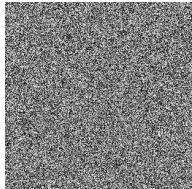
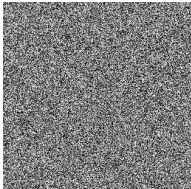
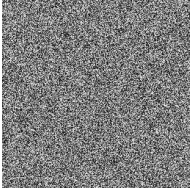
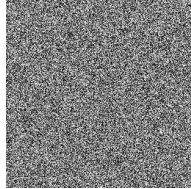
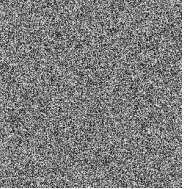
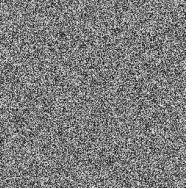
			
G_1	$(c-1)S_1^1$	$(c-2)S_2^1$	$(c-3)S_3^1$
			
G_2	$(d-1)S_1^2$	$(d-2)S_2^2$	$(d-3)S_3^2$
			

Figure 1. (a) the test secret image “Lena”, (b) the permuted secret image, (c) the generated shares sent to G_1 , (d) the generated shares sent to G_2 .

Figure 1a shows the test secret image I named “Lena” with 512×512 pixels and Figure 1b shows the permuted secret image \hat{I} . The generated shares according to the proposed scheme are shown in

Figure 1c,d, where Figure 1c presents three shares sent to G_1 and Figure 1d presents four shares sent to G_2 . As we can see, each shares has the same size with 256×256 pixels.

5.1. The Security

There are some simulation results to prove the security of the secret image in the proposed scheme. According to the security analysis in Section 4, we conduct three experiments as examples to demonstrate the proposed scheme, and the simulation results are presented in Figure 2.

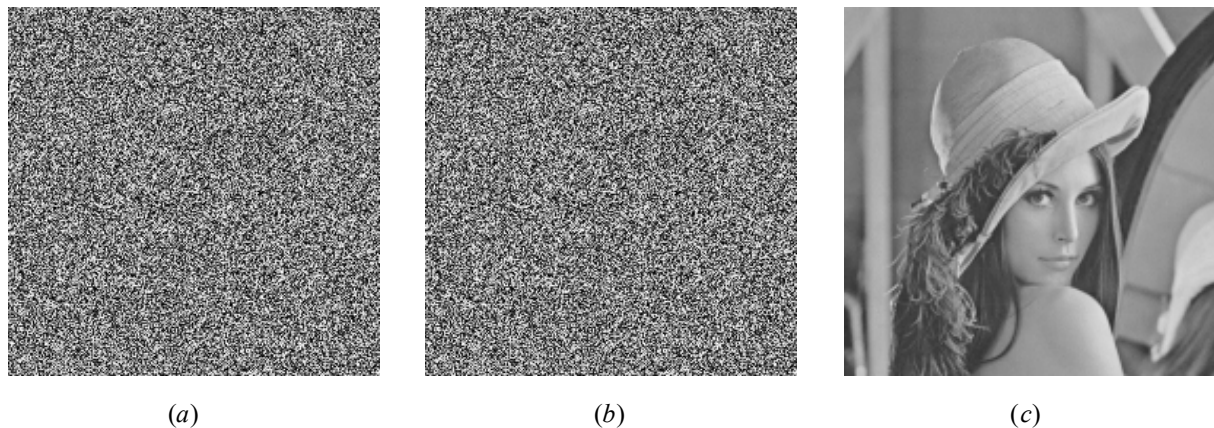


Figure 2. The simulation results in Examples 1, 2, 3, (a) the reconstructed image in Example 1 (b) the reconstructed image in Example 2 (c) the reconstructed image in Example 3.

Example 1. Assume that the collected shares in the secret image reconstruction procedure satisfy $|G_1| < 2$, $|G_2| \geq 2$, $|G_1| + |G_2| \geq 4$. Considering that there are four shares including one share from G_1 and three shares from G_2 . The simulation result is shown in Figure 2a. As we can see, when the collected shares cannot reach the threshold condition in G_1 , the reconstructed image is a random-looking image which can prove the security of the secret image in Case 1.

Example 2. Assume that the collected shares in the secret image reconstruction procedure satisfy $|G_1| \geq 2$, $|G_2| < 2$, $|G_1| + |G_2| \geq 4$. Considering that there are four shares including three shares from G_1 and one shares from G_2 . The simulation result is shown in Figure 2b. As we can see, when the collected shares against the threshold condition in G_2 , the reconstructed image is a random-looking image which can prove the security of the secret image in Case 2.

Example 3. Assume that the collected shares in the secret image reconstruction procedure satisfy $|G_1| \geq 2$, $|G_2| \geq 2$, $|G_1| + |G_2| \geq 4$. Considering that there are four shares including two share from G_1 and two shares from G_2 . The simulation result is shown in Figure 2c. For the collected shares satisfied both the threshold condition in G_1 and the threshold condition in G_2 , the original secret image can be reconstructed.

5.2. Histogram Analysis

The purpose of analysing an image's histogram is to measure the intensity level of this image. Usually, the pixel values in a random gray image are uniformly distributed in the range $[0, 255]$, and it is better when the generated shares have the feature of a random image.

We analyse the histograms of the test secret image and the generated shares in each group to prove that the security of the proposed scheme, and the results are presented in Figure 3. Figure 3a shows the histogram of the test secret image "Lena". The histogram of shares in G_1 and G_2 are shown in Figure 3b,c, respectively. As we can see from Figure 3, the pixel values in generated shares are almost uniformly distributed, so that the visible pattern cannot acquire meaningful information about the secret image.

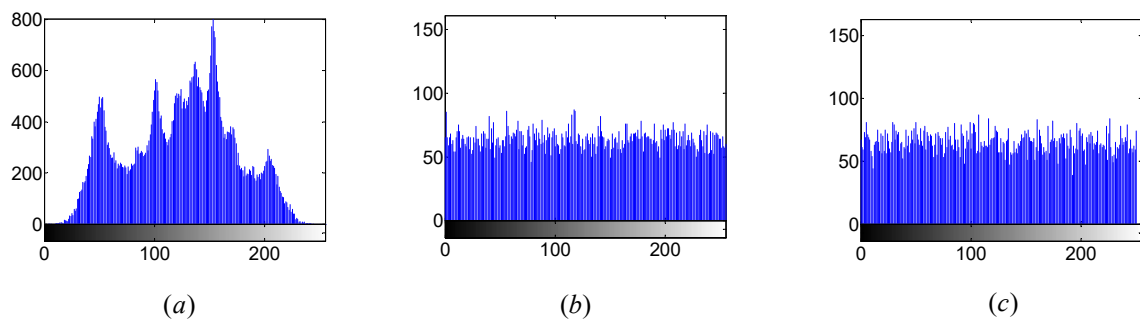


Figure 3. Histograms of Lena and the generated shares. (a) The histogram of “Lena” (b) the histogram of shares in G_1 (c) the histogram of shares in G_2 .

5.3. Correlation of Adjacent Pixels Analysis

If there is a strong correlation with the adjacent pixels in the shares, which would attract the attention of the attacker and would reveal some meaningful information of the secret image. Therefore, it shows a better security when the correlation between adjacent pixels is as little as possible in the generated shares. Mathematically, the correlation P_{xy} is represented by the formula (10).

$$P_{xy} = \frac{E[(x - C(x))(y - C(y))]}{\sqrt{D(x)D(y)}}, \quad (10)$$

$$C(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad (11)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - C(x)]^2. \quad (12)$$

where $C(x)$, $C(y)$ and $D(x)$, $D(y)$ are noted as the mean value and the standard variance of a sequence x and a sequence y , respectively, which are represented by the Formula (11) and Formula (12). And x , y represented as data sequences of two adjacent pixels in an image. When there is a strong correlation with the adjacent pixels, the value of P_{xy} approaches 1, otherwise, the value of P_{xy} approaches 0.

Table 1 shows the horizontal, vertical, and diagonal correlation coefficients in the secret test image “Lena” and two generated shares from G_1 and G_2 , respectively. It can be seen that the all correlation coefficients of the shares S_1^1 and S_1^2 are close to zero, which illustrate that the generated shares seems as random images. Besides, the correlation coefficients also can be evaluated from the plots. Usually, the stronger correlation between the adjacent pixels, the closer the points accumulating along the line $y = x$. The plots of the intensity values in horizontally adjacent pixels from “Lena”, and the shares S_1^1 , S_1^2 are shown in Figure 4a–c, respectively.

Table 1. The average correlation coefficients of shadows in $((1,4),4,4,8)$ -PESIS scheme.

	Lena	S_1^1	S_1^2
Horizontal	0.9746	−0.0130	−0.0131
Vertical	0.9539	−0.0089	−0.0028
Diagonal	0.9494	−0.0101	−0.0088

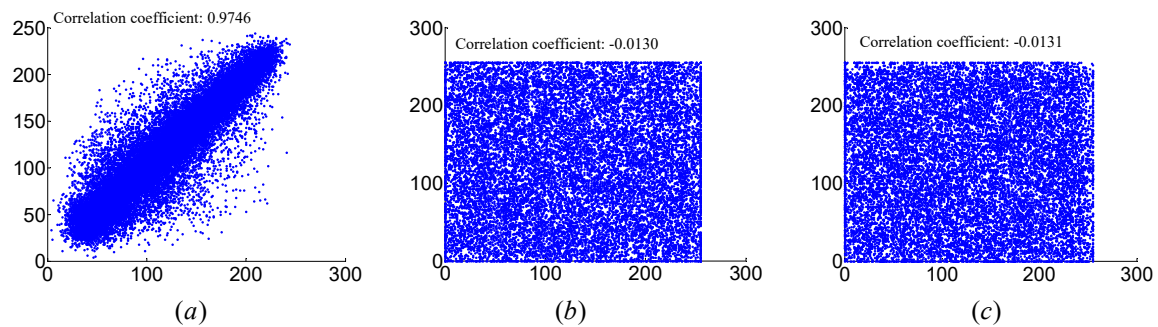


Figure 4. Histograms of Lena and the generated shares. (a) The histogram of “Lena” (b) the histogram of shares in G_1 (c) the histogram of shares in G_2 .

5.4. Resisting Noise Analysis

The shares would be polluted with some noise during being transmitted to shareholders, which would impact the quality of the reconstructed image. It is better the secret image can be reconstructed when shares are exposed to noise pollution in different degree. We add some different percentages Gaussian noise into each share and the results are presented in Figure 5. Figure 5a shows the share with the share with 1% Gaussian noise and the decrypted image. Figure 5b shows the share with the share with 5% Gaussian noise and the decrypted image. Figure 5c shows the share with the share with 10% Gaussian noise and the decrypted image. Figure 5d shows the share with the share with 15% Gaussian noise and the decrypted image. The value of peak-signal-to-noise-ratio ($PSNR$) is used to evaluate the visual quality of the decrypted image. Mathematically, $PSNR$ is represented by the Formula (13).

$$PSNR = 10 \times \lg \frac{255^2}{MSE} dB, \quad (13)$$

where MSE is the mean square error and represented as the Formula (14)

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N (O_{xy} - R_{xy})^2 \quad (14)$$

and $M \times N$ is the size of the original image, O_{xy} and R_{xy} are pixel values in the original image and decrypted image, respectively.

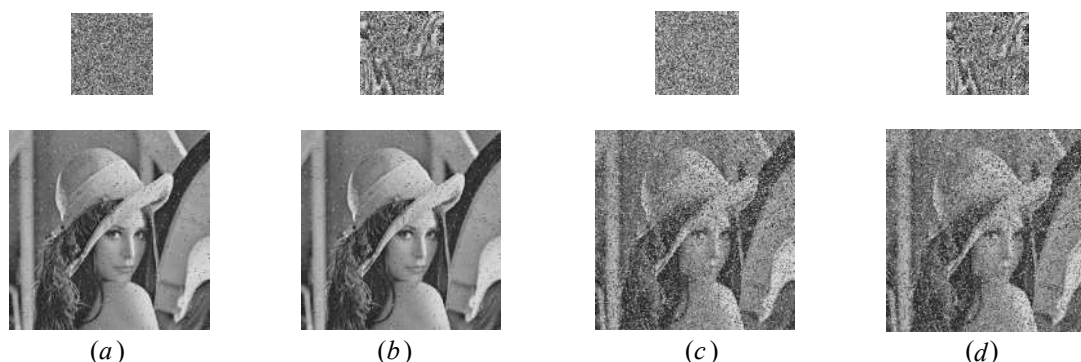


Figure 5. The results of resisting Gaussian noise. (a) the share with 1% Gaussian noise and the decrypted result (b) the share with 5% Gaussian noise and the decrypted result (c) the share with 10% Gaussian noise and the decrypted result (d) the share with 15% Gaussian noise and the decrypted result.

5.5. Comparison

Table 2 presents the comparison between some related hierarchical secret image sharing schemes and the proposed scheme.

Table 2. Comparisons between proposed scheme and some existing HSIS schemes.

Functionality	Level of Security	Shares Characteristic	Characteristic of Shareholders
Scheme [19]	Low	Different importance	A group
Scheme [20]	High	Different importance	A group
Scheme [21]	High	Same importance	A group
The Proposed scheme	High	Same importance	Multiple groups

First, there is a comparison of the level of security. As shown in the first row in Table 2, the proposed scheme is better than Guo et al.'s scheme in the aspect of the security. Actually in Guo et al. scheme [19], the embedded secret pixel values into all coefficients of a polynomial may be leading some non-authorized shareholders to partially restore the secret image, so that there is a low level of security in Guo et al.'s scheme. While in the proposed scheme, the secret image is permuted as a chaotic secret image, which improves the level of security of the secret image.

Second, there is a comparison of the characteristic of the generated shares. As shown in the second row in Table 2, the generated shares in Guo et al.'s scheme [19] and Pakniat et al.'s scheme [20] have different importance. While the generated shares in the proposed scheme have the same importance, which is more suitable for jointly managing the secret image by multiple groups.

Third, there is a comparison of the characteristic of shareholders. As shown in the third row in Table 2, the participated shareholders are from a common group in the schemes [19–21], so that the secret image is managed by one group. Actually, in the real world, the secret image needs to be managed by multiple groups jointly. Therefore, the scheme which the shareholders are from multiple groups is more suitable for a hierarchical secret image sharing scheme with multi-group joint management.

6. Conclusions

In this paper, a novel hierarchical secret image sharing scheme with multi-group joint management is proposed, which is suitable for protecting the security of the secret image by distributed storage over multiple clouds. In the proposed scheme, the secret image is managed by multiple groups rather than one group. By combining secret image sharing and Birkhoff interpolation algorithm, the secret image would be shared among multiple groups with different thresholds. Besides, the generated shares have the same weight, which is more suitable for the applicability. In addition, the proposed scheme would be applied in other related fields, such as image encryption in the Internet of things, multi-secret sharing in ad hoc networks, and so on.

Author Contributions: Methodology, Z.W.; Project administration, Y.L.; Writing—original draft, Z.W.; Writing—review and editing, X.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partly supported by National Natural Science Foundation of China under grant No. 61662016, the National Natural Science Foundation No. 61902164, Key projects of Guangxi Natural Science Foundation under grant No. 2018JJD170004, Guangxi Key Laboratory of Trusted Software No. KX201907.

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

References

1. Pares-Pulido, C.; Agudo, I. LockPic: Privacy Preserving Photo Sharing in Social Networks. In *Data Privacy Management, and Security Assurance*; Springer: Berlin, Germany, 2015; pp. 281–290.
2. Sun, W.; Zhou, J.; Zhu, S.; Tang, Y.Y. Robust privacy-preserving image sharing over online social networks (OSNs). *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2018**, *14*, 14. [[CrossRef](#)]

3. Xu, L.; Bao, T.; Zhu, L.; Zhang, Y. Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks. *IEEE Trans. Multimed.* **2019**, *21*, 591–602. [[CrossRef](#)]
4. Song, J.; Liu, Y.; Shao, J.; Tang, C. A dynamic membership data aggregation (DMDA) protocol for smart grid. *IEEE Systems Journal* **2020**, *14*, 900–908. [[CrossRef](#)]
5. Liu, Y.; Zhao, Q. E-voting scheme using secret sharing and K-anonymity. *World Wide Web* **2019**, *22*, 1657–1667. [[CrossRef](#)]
6. Chen, J.; Liu, G.; Liu, Y. Lightweight Privacy-preserving Raw Data Publishing Scheme. *IEEE Trans. Emerg. Top. Comput.* **2020**, doi:10.1109/TETC.2020.2974183. [[CrossRef](#)]
7. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [[CrossRef](#)]
8. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [[CrossRef](#)]
9. Wu, K.S. A secret image sharing scheme for light images. *EURASIP J. Adv. Signal Process.* **2013**, *2013*, 49. [[CrossRef](#)]
10. Kansa, A.; Ghebleh, M. An efficient (t, n) -threshold secret image sharing scheme. *Multimed. Tools Appl.* **2017**, *76*, 16369–16388. [[CrossRef](#)]
11. Yan, X.; Lu, Y.; Liu, L. A general progressive secret image sharing construction method. *Signal Process. Image Commun.* **2019**, *71*, 66–75. [[CrossRef](#)]
12. Chen, C.C. Essential secret image sharing scheme with equal-sized shadows generation. *J. Vis. Commun. Image Represent.* **2018**, *52*, 143–150. [[CrossRef](#)]
13. Wu, Z.; Liu, Y.N.; Wang, D.; Yang, C.N. An Efficient Essential Secret Image Sharing Scheme Using Derivative Polynomial. *Symmetry* **2019**, *11*, 69. [[CrossRef](#)]
14. Yan, X.; Lu, Y. Generalized general access structure in secret image sharing. *J. Vis. Commun. Image Represent.* **2019**, *58*, 89–101. [[CrossRef](#)]
15. Jia, X.; Wang, D.; Nie, D.; Luo, X.; Sun, J.Z. A new threshold changeable secret sharing scheme based on the Chinese Remainder Theorem. *Inf. Sci.* **2019**, *473*, 13–30. [[CrossRef](#)]
16. Mashhadi, S. Secure publicly verifiable and proactive secret sharing schemes with general access structure. *Inf. Sci.* **2017**, *378*, 99–108. [[CrossRef](#)]
17. Deshmukh, M.; Nain, N.; Ahmed, M. Efficient and secure multi secret sharing schemes based on boolean XOR and arithmetic modulo. *Multimed. Tools Appl.* **2018**, *77*, 89–107. [[CrossRef](#)]
18. Tassa, T. Hierarchical threshold secret sharing. *J. Cryptol.* **2007**, *20*, 237–264. [[CrossRef](#)]
19. Guo, C.; Chang, C.C.; Qin, C. A hierarchical threshold secret image sharing. *Pattern Recognit. Lett.* **2012**, *33*, 83–91. [[CrossRef](#)]
20. Pakniat, N.; Noroozi, M.; Eslami, Z. Secret image sharing scheme with hierarchical threshold access structure. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1093–1101. [[CrossRef](#)]
21. Bhattacharjee, T.; Maity, S.P.; Islam, S.R. Hierarchical secret image sharing scheme in compressed sensing. *Signal Process. Image Commun.* **2018**, *61*, 21–32. [[CrossRef](#)]
22. Jia, X.; Song, Y.; Wang, D.; Nie, D.; Wu, J. A collaborative secret sharing scheme based on the Chinese Remainder Theorem. *Math. Biosci. Eng.* **2019**, *16*, 1280. [[CrossRef](#)] [[PubMed](#)]
23. Schoenberg, I.J. On Hermite-Birkhoff interpolation. *J. Math. Anal. Appl.* **1966**, *16*, 538–543. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).