Hindawi
Security and Communication Networks
Volume 2021, Article ID 9960998, 14 pages
https://doi.org/10.1155/2021/9960998

Research Article

An Intragroup and Intergroup Multiple Secret Images' Sharing Scheme with Each Participant Holding One Shadow Image

Jiayu Wang, Xuehu Yan, Jia Chen, and Yongqiang Yu

National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Xuehu Yan; publictiger@126.com

Received 1 April 2021; Accepted 20 June 2021; Published 2 July 2021

Academic Editor: Zhili Zhou

In some particular situations, participants need to recover different secrets both within a group (i.e., intragroup) and between two groups (i.e., intergroup). However, most of the existing multilevel secret sharing (MLSS) and multigroup secret sharing (MGSS) schemes mainly focus on how to protect a secret between one or more groups. In this paper, we propose a polynomial-based scheme to share multiple secret images both within a group and between groups. The random elements' utilization model of integer linear programming is used to find polynomial coefficients that meet certain conditions so that each participant holds only one shadow image and some of them can recover secrets of both intergroup and intragroup. In addition, our scheme based on polynomials has the advantage of low computational complexity. Theoretical analysis and experiments show that the proposed scheme is feasible and effective.

1. Introduction

With the popularization of digital media technology, the transmission of information is more and more convenient and fast. At the same time, many malicious participants appear on the network to intercept or tamper with the information. So how to safely transmit secret information has become a problem of increasing concern. With the development of cloud technology, more and more attention has been paid to information security, especially image security. The secret image sharing (SIS) technique is an excellent way to keep secret images secure among specific participants.

The (k, n) threshold SS scheme was firstly proposed by Adi [1] and Blakley [2], respectively. In Shamir's scheme, the secret is shared into n shadow images and distributed to n participants. At least k participants are needed to recover the secret, while less than k participants cannot obtain any information of the secret. The Lagrange interpolation method is used to recover the secret. The SS scheme based on polynomial can be applied to SIS for grayscale images and color images.

The technology of visual cryptography (VC) has gradually developed as digital images are used more and more widely in daily life. This technique is also known as visual secret sharing (VSS). The visual cryptography scheme was first proposed by Noar and Shamir [3] in 1995. In their scheme, the secret can be revealed by a human visual system without any cryptographic computations, and the scheme is very useful when there is no lightweight computation device. The secret image can be recovered by stacking shares, and when the computation device is available, we can also choose the XOR operation to recover the secret image in a lossless manner [4, 5]. At present, the research on VC is mainly divided into basis matrix based [3, 6, 7] and random grid based [8–10]. However, the image quality recovered by this scheme is poor [11], so we choose a polynomial-based scheme as our scheme.

In 2002, Thien and Lin [12] firstly applied the polynomial-based SS technique to SIS. In their scheme, instead of setting the coefficients to be random, they embedded the secret image pixel values into all the coefficients. In order to avoid information leakage, the scheme permuted the secret image. Later, many people studied the polynomial-based SIS (PSIS) scheme from different perspectives. Li et al. [13] proposed an SIS scheme using derivative polynomial and Birkhoff interpolation. Kanso and Ghebleh [14] improved Thien and Lin's [12] scheme by cyclically shifting the bits of

the secret image; and there are some studies on essential SIS [15–17].

In some practical application scenarios, secret recovery requires a hierarchical limit of participants. Some multilevel secret sharing (MLSS) schemes were proposed [18–20]. The MLSS schemes are also called schemes with hierarchical threshold access structure. In MLSS, shares are divided into different levels. Shadow images of different levels will reach different thresholds to recover the secret image. Guo et al. [21] proposed an MLSS scheme based on Tassa's [18] hierarchical SIS scheme. Pakniat et al. [22] improved the security of the scheme proposed by Guo et al.

For sharing secrets in groups, there are lots of multigroup secret sharing (MGSS) schemes. Li et al. [23] proposed a threshold MGSS scheme based on the Chinese Remainder Theorem (CRT). In their scheme, secrets of multiple groups are packed into a group of large secrets and shared with participants. Wu et al. [24] proposed a hierarchical SIS scheme with multigroup joint management. In their scheme, participants in different groups have to meet different threshold conditions to recover the secret, while all of the shadow images have the same weight. Meng et al. [25] proposed an MGSS scheme without hierarchy. A secret is shared between groups and all the participants are equal. A tightly coupled SS scheme proposed by Meng et al. can resist illegal participant attacks and share capture attacks.

However, all of the above schemes mainly focus on how to keep one secret image secure between one or more groups. Yang et al. [26] proposed a multiple secret images sharing (MSIS) scheme between multiple groups for the first time. They constructed a base matrix to embed the information of multiple secret images into the coefficients of m polynomials. However, participants in their scheme are required to hold more than one shadow image.

In practical applications, a participant may need to participate in intragroup and intergroup SS. Holding multiple shadow images is not convenient for the distribution and transmission of the shadow images. Consider the following application scenario. In the professional field, often some experts' research fields are crossed, and the number of experts in some fields is limited. Two groups of engineering designers have designed two kinds of products, respectively, and each of the two teams holds a draft of a product. At the same time, some members of the first group work with some members of the second group to design a third product. In this case, intragroup designers should be able to restore their own group's draft; intergroup designers working on two products should be able to restore both drafts. The intragroup recovery and the intergroup recovery should be distinct. Designers working on only one product cannot restore the intergroup secret image.

In order to realize MSIS within one group and between groups and to transmit and save shadow images more conveniently in practical application, we propose an intragroup and intergroup MSIS scheme with each participant holding one shadow image. Our scheme is based on the polynomial; and we use the random elements utilization model to screen the coefficients of the sharing polynomial. The coefficients satisfying the condition can be solved by solving the matrix equation. The contributions of our work are as follows:

(1) Multiple secret images can be shared within a group and between groups

(2) Each participant holds only one shadow image

(3) Our scheme has low computational complexity

The structure of this paper is as follows. In Section 2, we present the PSIS scheme and the concepts of intragroup and intergroup SIS. In Section 3, we describe the sharing and restoring processes of the proposed scheme in detail and take the value of a pixel as an example to illustrate the scheme. Related theoretical analyses are given in Section 4. In Section 5, we present the experimental results and comparison. Finally, conclusions are drawn in Section 6.

2. Preliminaries

In this section, we review the PSIS scheme and then introduce the concepts of intragroup and intergroup SIS.

2.1. Polynomial-Based SIS Scheme. Shamir proposed a (k, n) threshold secret sharing scheme based on the polynomial and it can be applied to SIS. The PSIS scheme shares a secret image into n shadow images and distributes them to n participants. When k or more participants participate in the recovery, the secret image can be recovered. The specific implementation principle is as follows. For secret a_0, construct a polynomial in equation (1). $a_1, a_2, \ldots, a_{k-1}$ are random numbers taken in the prime number field p, and all operations are carried out in the field of GF(p). The value of $f(x)$ is the value of the shadow pixel.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \ (\underline{\mathrm{mod}}\ p). \quad (1)$$

When recovering the secret, at least k participants are needed, for there are k unknown coefficients and we need k equations. The Lagrange interpolation method shown in (2) is used to recover the secret $(x_i \neq x_j, i, j = 1, 2, \ldots, n)$. The secret can be recovered by calculating $a_0 = f(0)$.

$$f(x) = \sum_{i=1}^{k} f(x_i) \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} (\underline{\mathrm{mod}}\ p). \quad (2)$$

In the PSIS scheme, the influence of the coefficient value on the shadow image can be seen intuitively. In order to screen the coefficients more intuitively and find the appropriate combination of coefficients in the solution space, we adopted the PSIS scheme. We can list the conditions that need to be satisfied for the coefficients of the polynomial and solve the matrix equation to find the values of the coefficients. What is more, we choose to operate on the field of GF(251), for it has low computational complexity. However, the pixel value between 251 and 255 is changed to 250, and the scheme is lossy.

2.2. Intragroup and Intergroup SIS. As mentioned in the application scenario, the secret recovery involves recovering the secret across groups. Intragroup SIS means sharing and

recovering a secret image within a group; intergroup SIS means sharing and recovering a secret image between two groups.

In our scheme, there is no hierarchy between the groups or the participants. There are two groups in our scheme. Every participant can participate in the intragroup secret recovery of his own group, and some predetermined participants can participate in the intergroup secret recovery.

Participants who are authorized to participate in the intergroup secret recovery can participate in the recovery of two different secret images with the one shadow image in their hands. Participants within one group cannot recover intergroup secrets, and participants without permissions cannot participate in the intergroup secret recovery. Secret recovery within one group and that between groups do not affect each other.

Take the intragroup (3, 4) and intergroup (4, 4) thresholds scheme as an example. P_1, P_2, P_3, P_4 in G_1 can participate in the recovery of S_1; P_5, P_6, P_7, P_8 in G_2 can participate in the recovery of S_2; P_1, P_2, P_5, P_6 can participate in the recovery of $S_{1,2}$. The relationship between the participants and the groups is shown in Figure 1.

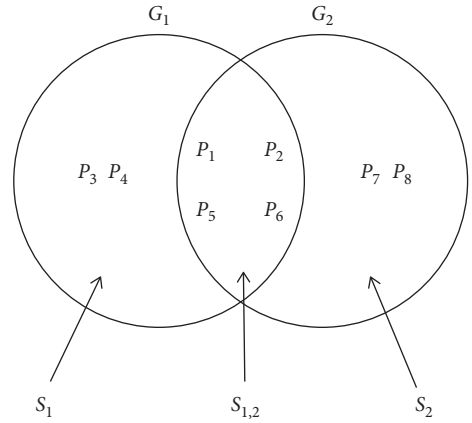

Figure 1: The relationship between the participants and the groups.

3. The Proposed Scheme

In this section, we propose an intragroup and intergroup SIS scheme with each participant holding one shadow image. Secret images are shared into multiple shadow images by the random elements utilization model. Participants who can participate in the recovery of the secret between groups are identified in advance.

A participant who is authorized to participate in intergroup secret recovery can recover the intergroup secret together with other participants according to the shadow image he holds; he could use the same shadow image to recover the group's secret image with the intragroup participants. Intragroup and intergroup secrets are different and independent. Participants who do not have permission to participate in intergroup secret recovery have no access to get the intergroup secret image; they can only recover the intragroup secret together with intragroup participants. Those who participate in the secret image recovery within their own group are called local participants, while those who participate in the secret recovery between groups are called shared participants. The meanings of each symbol are shown in Table 1. The process of sharing and restoring is shown in Figure 2.

3.1. The Sharing Phase. The sharing process is based on the PSIS scheme proposed by Shamir. The random elements utilization model is used to screen the polynomial coefficients that satisfy specific conditions. All the following operations are performed in the field of GF(251). Assume that the size of the secret image is $A \times B$. The steps are shown in Algorithm 1.

For the shared participants, the shadow images obtained by this method satisfy both the intragroup sharing polynomials and the intergroup sharing polynomials. As a result, a shared participant can join in the intragroup and intergroup secret recovery with the same shadow image. It is worth noting that the shared participants are assigned in advance.

To find a suitable combination of the coefficients, the brute-force cracking method can be used, in which we traverse the solution space for all possible values until we find a solution that satisfies the condition. Obviously, this algorithm has high time complexity. We adopt the random elements utilization model of integer linear programming and find the solution by multiplying inverse matrix, and the calculation efficiency is greatly improved.

3.2. The Recovery Phase. In the recovery phase, we adopt Lagrangian interpolation to obtain the pixel values of the secret images. At least k_1 (k_2) local participants in G_1 (G_2) are required to recover S_1 (S_2); at least k_3 shared participants between G_1 and G_2 are required to recover $S_{1,2}$. The steps are shown in Algorithm 2.

When recovering the intergroup secret image, we require a dealer to collect shadow images from participants and recover the secret image. This is to prevent intergroup participants from gaining access to intragroup secret information of the other group. For example, intergroup participants in G_1 cannot obtain the shadow image of participants in G_2.

3.3. An Example of a Pixel. In this section, we give an example of the sharing and recovery processes of a pixel. a_0 is the value of a pixel in S_1, b_0 is the pixel value of the corresponding position in S_2, and c_0 is the pixel value of the corresponding position in $S_{1,2}$. The secret pixel values are $[a_0, b_0, c_0] = [123, 135, 146]$. Intragroup (3, 4) and intergroup (4, 4) thresholds are assumed. P_1, P_2, P_3, P_4 are the local participants in G_1 and P_5, P_6, P_7, P_8 are the local participants in G_2. We designate that P_1, P_2, P_5, P_6 can participate in the recovery of secret images between groups in advance. The order numbers of P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8 are $1, 2, 3, 4, 5, 6, 7, 8$, that is, $(x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, y_1 = 5, y_2 = 6, y_3 = 7, y_4 = 8)$. The sharing polynomials of the secret images are shown as follows:

Table 1: Meanings of the symbols.

Symbol	Meaning
$G_i\,(i = 1, 2)$	Group 1, Group 2
$P_i\,(i = 1, \ldots, n_1 + n_2)$	The participant
x_i, y_i, z_i	The order number of P_i
$SC_i\,(i = 1, \ldots, n_1 + n_2)$	The shadow image held by P_i
$S_i\,(i = 1, 2)$	The intragroup secret image of G_i
$S_{1,2}$	The intergroup secret image of Group 1 and Group 2
$S_i'\,(i = 1, 2)$	The recovered intragroup secret image of G_i
$S_{1,2}'$	The recovered intergroup secret image of Group 1 and Group 2
$(k_i, n_i)\,(i = 1, 2)$	The threshold of intragroup SIS of G_i
(k_3, n_3)	The threshold of intergroup SIS of Group 1 and Group 2
a_0	A pixel value of S_1
b_0	A pixel value of S_2
c_0	A pixel value of $S_{1,2}$

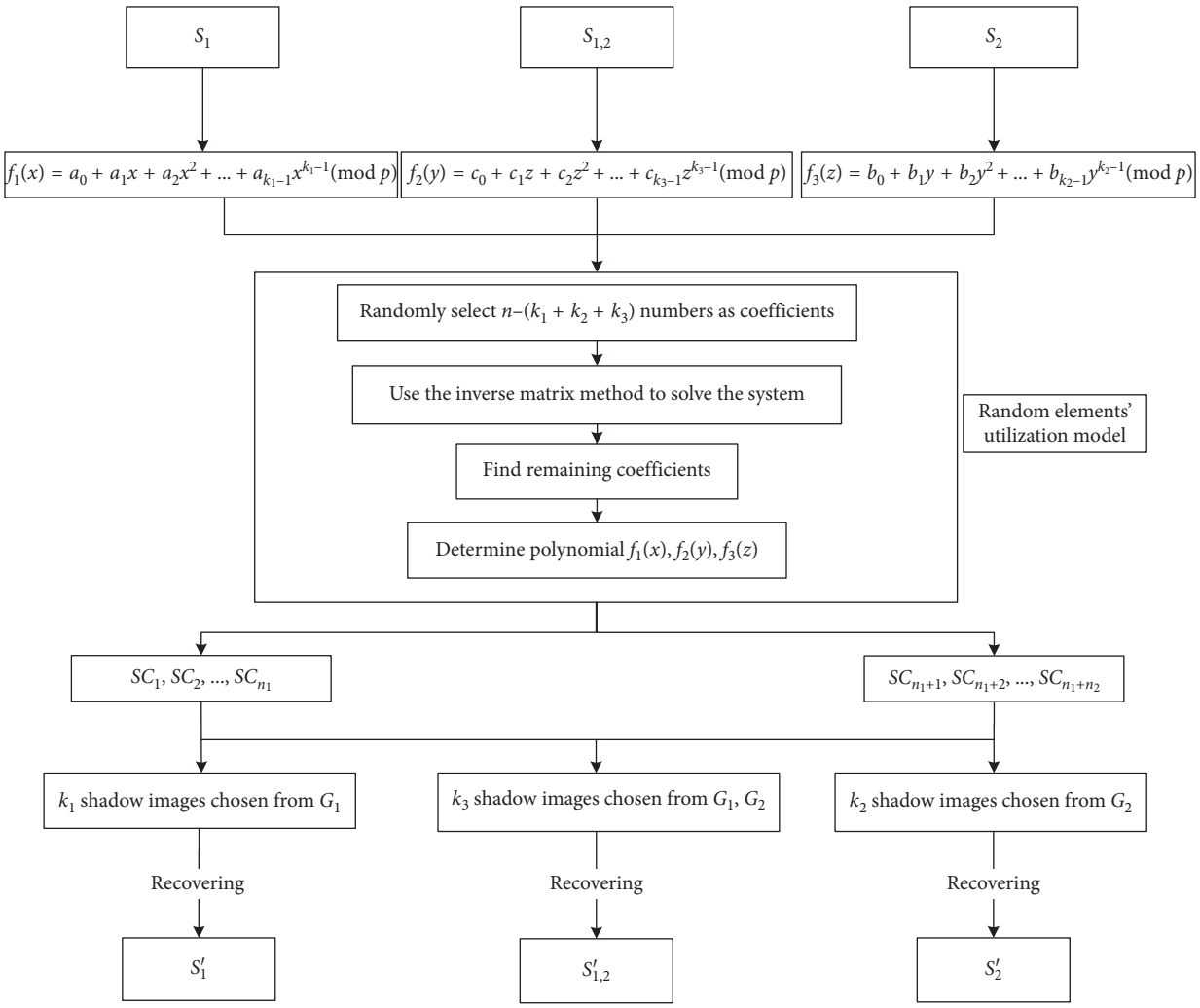

Figure 2: The flowchart of our proposed scheme.

Input: the secret images $S_1, S_2, S_{1,2}$ and the order numbers of the participants $x_i\,(i = 1, 2, \ldots, n_1 + n_2)$
Output: the shadow images $SC_i\,(i = 1, 2, \ldots, n_1 + n_2)$
Step 1: repeat Steps 2–7 for each pixel of the secret images $S_1\,(a, b), S_2\,(a, b)$, and $S_{1,2}\,(a, b)$, where $(a, b) \in \{(a, b)|1 \le a \le A, 1 \le b \le B\}$
Step 2: write the polynomial expressions for SIS within and between groups
Step 3: find the equations that the sharing coefficients need to satisfy
Step 4: count the variables $(k_1 + k_2 + k_3 - 3)$ and the number of equations that need to be satisfied (n_3)
Step 5: pick $n_3 - (k_1 + k_2 + k_3 - 3)$ coefficients randomly and assign them to a random number between 0 and 250
Step 6: use the inverse matrix method to solve the system and find the values of the remaining unspecified coefficients
Step 7: calculate the values of the shadow pixel based on the sharing polynomial, in which the polynomial coefficients are known

Algorithm 1: The shadow image generation process of SIS within one group and between groups.

Input: the shadow images $SC_i\,(i = 1, 2, \ldots, n_1 + n_2)$, the order numbers of the participants $x_i\,(i = 1, 2, \ldots, n_1 + n_2)$ and the order numbers of the authorized shared participants.
Output: the recovered images $S_1', S_2', S_{1,2}'$
Step 1: determine the shadow images participating in the recovery of $S_1, S_2, S_{1,2}$, respectively.
Step 2: repeat Steps 3 and 4 for each pixel of the corresponding shadow images in each group.$SC_i\,(a, b)\,(i = 1, \ldots, n_1)$ $(SC_i\,(a, b)\,(i = n_1 + 1, \ldots, n_2))$ are used to recover $S_1\,(S_2)$; intergroup shadow images are used to recover $S_{1,2}$, where $(a, b) \in \{(a, b)|1 \le a \le A, 1 \le b \le B\}$.
Step 3: calculate $f\,(x)$ in the field of GF(251) by the Lagrange interpolation formula $f\,(x) = \sum_{i=1}^{k} f\,(x_i) \prod_{j=1, j\neq i}^{k} ((x - x_j)/x_i - x_j)$.
Step 4: set $x = 0$ to calculate the recovered secret pixel value in each group.
Step 5: output the recovered images $S_1', S_2', S_{1,2}'$.

Algorithm 2: The recovery process of the SIS within one group and between groups.

$$
\begin{aligned}
S_1 &\begin{cases} f_1(x_1) = a_0 + a_1 x_1 + a_2 x_1^2 \,(\mathrm{mod}\, 251), \\ f_1(x_2) = a_0 + a_1 x_2 + a_2 x_2^2 \,(\mathrm{mod}\, 251), \\ f_1(x_3) = a_0 + a_1 x_3 + a_2 x_3^2 \,(\mathrm{mod}\, 251), \\ f_1(x_4) = a_0 + a_1 x_4 + a_2 x_4^2 \,(\mathrm{mod}\, 251), \end{cases} \\
S_2 &\begin{cases} f_2(y_1) = b_0 + b_1 y_1 + b_2 y_1^2 \,(\mathrm{mod}\, 251), \\ f_2(y_2) = b_0 + b_1 y_2 + b_2 y_2^2 \,(\mathrm{mod}\, 251), \\ f_2(y_3) = b_0 + b_1 y_3 + b_2 y_3^2 \,(\mathrm{mod}\, 251), \\ f_2(y_4) = b_0 + b_1 y_4 + b_2 y_4^2 \,(\mathrm{mod}\, 251), \end{cases} \\
S_{1,2} &\begin{cases} f_3(z_1) = c_0 + c_1 z_1 + c_2 z_1^2 + c_3 z_1^3 \,(\mathrm{mod}\, 251), \\ f_3(z_2) = c_0 + c_1 z_2 + c_2 z_2^2 + c_3 z_2^3 \,(\mathrm{mod}\, 251), \\ f_3(z_3) = c_0 + c_1 z_3 + c_2 z_3^2 + c_3 z_3^3 \,(\mathrm{mod}\, 251), \\ f_3(z_4) = c_0 + c_1 z_4 + c_2 z_4^2 + c_3 z_4^3 \,(\mathrm{mod}\, 251), \end{cases}
\end{aligned}
\tag{3}
$$

where z_1, z_2, z_3, z_4 represent the order numbers of the participants of the intergroup, which are the same as the order numbers of the selected participants from G_1 and G_2.

The polynomial coefficients need to satisfy (4). The random elements utilization model of integer linear programming is shown in equation (5).

$$\begin{aligned}
a_0 + a_1x_1 + a_2x_1^2 &\equiv c_0 + c_1x_1 + c_2x_1^2 + c_3x_1^3 \,(\mathrm{mod}\, 251),\\
a_0 + a_1x_2 + a_2x_2^2 &\equiv c_0 + c_1x_2 + c_2x_2^2 + c_3x_2^3 \,(\mathrm{mod}\, 251),\\
b_0 + b_1y_1 + b_2y_1^2 &\equiv c_0 + c_1y_1 + c_2y_1^2 + c_3y_1^3 \,(\mathrm{mod}\, 251),\\
b_0 + b_1y_2 + b_2y_2^2 &\equiv c_0 + c_1y_2 + c_2y_2^2 + c_3y_2^3 \,(\mathrm{mod}\, 251),
\end{aligned} \tag{4}$$

$$\text{s.t.}\begin{cases}
f_1(x_i) = f_3(x_i), & i = 1,2\\
f_2(y_i) = f_3(y_i), & i = 1,2,\\
a_l, b_m, c_n \in z,\\
a_l, b_m, c_n \in [0,250],\\
l = 1,2,\\
m = 1,2,\\
n = 1,2,3.
\end{cases} \tag{5}$$

There are four equations and seven variables. We choose to assign values for $3(7-4=3)$ variables: c_1, c_2, c_3. The values assigned are randomly selected between 0 and 250 and the result is $[c_1, c_2, c_3] = [35, 163, 5]$. After c_1, c_2, and c_3 are determined as constants, we can obtain (6) by placing the constant terms in the equation on one side and obtain (7) by putting the values of the parameters into the equation and writing it in matrix form.

$$\begin{aligned}
a_1x_1 + a_2x_1^2 &\equiv -\left(a_0 + c_0 + c_1x_1 + c_2x_1^2 + c_3x_1^3\right) (\mathrm{mod}\, 251),\\
a_1x_2 + a_2x_2^2 &\equiv -\left(a_0 + c_0 + c_1x_2 + c_2x_2^2 + c_3x_2^3\right) (\mathrm{mod}\, 251),\\
b_1y_1 + b_2y_1^2 &\equiv -\left(b_0 + c_0 + c_1y_1 + c_2y_1^2 + c_3y_1^3\right) (\mathrm{mod}\, 251),\\
b_1y_2 + b_2y_2^2 &\equiv -\left(b_0 + c_0 + c_1y_2 + c_2y_2^2 + c_3y_2^3\right) (\mathrm{mod}\, 251),
\end{aligned} \tag{6}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0\\ 2 & 4 & 0 & 0\\ 0 & 0 & 5 & 25\\ 0 & 0 & 6 & 36 \end{bmatrix} \begin{bmatrix} a_1\\ a_2\\ b_1\\ b_2 \end{bmatrix} = \begin{bmatrix} 226\\ 32\\ 117\\ 141 \end{bmatrix}. \tag{7}$$

In equation (7), we can multiply both sides of the equation by the inverse of the coefficient matrix on the left-hand side, and we get that the values of a_1, a_2, b_1, b_2 are $185, 41, 48, 226$. So far, we have determined all the coefficients of the sharing polynomial. We can get the value of the shadow pixels by putting the values of the coefficients and the order numbers of the participants into equation (3). The results are as follows: the shadow pixel values of G_1 are $98, 155, 43, 13$ and the shadow pixel values of G_2 are $1, 25, 250, 174$.

When recovering the secrets, we use the Lagrange interpolation method. We chose P_2, P_3, P_4 to recover a_0, P_6, P_7, P_8 to recover b_0, and P_1, P_2, P_5, P_6 to recover c_0. The results are $123, 135, 146$, which are equal to a_0, b_0, c_0, respectively.

4. Theoretical Analysis

In this section, we give the feasibility and security analysis of the proposed scheme and give the conditions for each parameter to be satisfied.

4.1. Feasibility and Security Analysis

4.1.1. Feasibility Analysis. The following details are the sharing process of one pixel. a_0, b_0, c_0 are the secret pixels to be shared. The three pixels are shared into shadow image pixels as shown in (8)–(10):

$$S_1\begin{cases}
f_1(x_1) = a_0 + a_1x_1 + \cdots + a_{k_1-1}x_1^{k_1-1} \,(\mathrm{mod}\, 251),\\
f_1(x_2) = a_0 + a_1x_2 + \cdots + a_{k_1-1}x_2^{k_1-1} \,(\mathrm{mod}\, 251),\\
\vdots\\
f_1\left(x_{n_1}\right) = a_0 + a_1x_{n_1} + \cdots + a_{k_1-1}x_{n_1}^{k_1-1} \,(\mathrm{mod}\, 251),
\end{cases} \tag{8}$$

$$S_2\begin{cases}
f_2(y_1) = b_0 + b_1y_1 + \cdots + b_{k_2-1}y_1^{k_2-1} \,(\mathrm{mod}\, 251),\\
f_2(y_2) = b_0 + b_1y_2 + \cdots + b_{k_2-1}y_2^{k_2-1} \,(\mathrm{mod}\, 251),\\
\vdots\\
f_2\left(y_{n_2}\right) = b_0 + b_1y_{n_2} + \cdots + b_{k_2-1}y_{n_2}^{k_2-1} \,(\mathrm{mod}\, 251),
\end{cases} \tag{9}$$

$$S_{1,2}\begin{cases}
f_3(z_1) = c_0 + c_1z_1 + \cdots + c_{k_3-1}z_1^{k_3-1} \,(\mathrm{mod}\, 251),\\
f_3(z_2) = c_0 + c_1z_2 + \cdots + c_{k_3-1}z_2^{k_3-1} \,(\mathrm{mod}\, 251),\\
\vdots\\
f_3\left(z_{n_3}\right) = c_0 + c_1z_{n_3} + \cdots + c_{k_3-1}z_{n_3}^{k_3-1} \,(\mathrm{mod}\, 251).
\end{cases} \tag{10}$$

In the basic sharing scheme, the polynomial coefficients are random. We use the randomness to make the coefficients meet certain conditions, so that the shadow images can carry more information. The shadow pixel value held by local participants in G_1 participating in intergroup secret sharing shall satisfy equations (8) and (10), while the shadow pixel value held by local participants in G_2 participating in intergroup secret sharing shall satisfy equations (9) and (10). So, the coefficients shall satisfy equation (11). The random elements utilization model of integer linear programming is shown in equation (12).

$$\begin{aligned}
a_0 + a_1 x_1 + \cdots + a_{k_1-1} x_1^{k_1-1} &\equiv \left(c_0 + c_1 x_1 + \cdots + c_{k_3-1}\right) x_1^{k_3-1} \,(\mathrm{mod}\, 251),\\
a_0 + a_1 x_2 + \cdots + a_{k_1-1} x_2^{k_1-1} &\equiv \left(c_0 + c_1 x_2 + \cdots + c_{k_3-1}\right) x_2^{k_3-1} \,(\mathrm{mod}\, 251),\\
&\vdots\\
b_0 + b_1 x_{n_3-1} + \cdots + b_{k_2-1} x_{n_3-1}^{k_2-1} &\equiv \left(c_0 + c_1 x_{n_3-1} + \cdots + c_{k_3-1}\right) x_{n_3-1}^{k_3-1} \,(\mathrm{mod}\, 251),\\
b_0 + b_1 x_{n_3} + \cdots + b_{k_2-1} x_{n_3}^{k_2-1} &\equiv \left(c_0 + c_1 x_{n_3} + \cdots + c_{k_3-1}\right) x_{n_3}^{k_3-1} \,(\mathrm{mod}\, 251),
\end{aligned} \tag{11}$$

$$\text{s.t.} \begin{cases}
f_1(x_i) = f_3(x_i),\\
f_2(y_i) = f_3(y_i), \quad i = 1, 2, \ldots, n_3,\\
x_i, y_i \in Z\\
x_i, y_i \in [0, 250],\\
a_l, b_m, c_n \in Z,\\
a_l, b_m, c_n \in [0, 250],\\
l = 1, 2, \ldots, k_1 - 1,\\
m = 1, 2, \ldots, k_2 - 1,\\
n = 1, 2, \ldots, k_3 - 1.
\end{cases} \tag{12}$$

We write equation (11) as matrix multiplication, as shown in the following equation:

$$\begin{bmatrix}
x_1 & x_1^2 & \ldots & x_1^{k_1-1} & 0 & 0 & \ldots & 0 & -x_1 & -x_1^2 & \ldots & -x_1^{k_3-1}\\
x_2 & x_2^2 & \ldots & x_2^{k_1-1} & 0 & 0 & \ldots & 0 & -x_2 & -x_2^2 & \ldots & -x_2^{k_3-1}\\
 & & \vdots & & & & & & & & & \\
0 & 0 & \ldots & 0 & x_{n_3} & x_{n_3}^2 & \ldots & x_{n_3}^{k_2-1} & -x_{n_3} & -x_{n_3}^2 & \ldots & -x_{n_3}^{k_3-1}
\end{bmatrix}
\begin{bmatrix}
a_1\\ a_2\\ \vdots\\ a_{k_1-1}\\ b_1\\ b_2\\ \vdots\\ b_{k_2-1}\\ c_1\\ c_2\\ \vdots\\ c_{k_3-1}
\end{bmatrix}
=
\begin{bmatrix}
c_0 - a_0\\ c_0 - a_0\\ \vdots\\ c_0 - b_0
\end{bmatrix}. \tag{13}$$

There are n_3 equations and $k_1 + k_2 + k_3 - 3$ variables in the system $(k_1 + k_2 + k_3 - 3 \geq n_3)$. Each coefficient has 251 possible values. The size of the solution space is $251^{(k_1+k_2+k_3-3)-n_3}$. We pick $(k_1 + k_2 + k_3 - 3) - n_3$ coefficients at random and assign them to a random number between 0 and 250. Then the system has a unique solution, and we can use the matrix inverse method to solve for the coefficients. According to the coefficients we get, we can get the shadow image pixel value that satisfies our requirements. After the sharing of one pixel, the sharing of the whole image can be completed by traversing all the pixels of the secret image.

4.1.2. Security Analysis. When restoring the secret image within a group, less than $k_1\,(k_2)$ participants could not recover $S_1\,(S_2)$; when restoring the secret image between groups, less than k_3 participants could not recover $S_{1,2}$.

Participants without permission cannot participate in the intergroup secret recovery, and even if they do, they cannot recover the secret information. The reason is that the coefficients are calculated according to the order numbers of the legal participants, and if an unauthorized participant participates in the recovery, the Lagrange interpolation method will not be able to recover the true secret.

There is no information leakage when the shared participants recover the intergroup secret image, for all the shadow images are sent to the dealer. A shared participant cannot get access to the shadow image of the other group.

4.2. Parametric Constraint. $k_1 + k_2 + k_3 - 3 \geq n_3$. For secret sharing between groups, the number of equations that the coefficients need to satisfy is n_3. When sharing a pixel, the sharing polynomial of $S_1(S_2)$ has $k_1 - 1(k_2 - 1)$ variable coefficients; the sharing polynomial of $S_{1,2}$ has $k_3 - 1$ variable coefficients. The total number of variable coefficients is shown in the following equation:

$$(k_1 - 1 + k_2 - 1 + k_3) - 1 = (k_1 + k_2 + k_3) - 3. \quad (14)$$

In order for the solution space not to be empty, the number of variables should be greater than or equal to the number of equations (i.e., $k_1 + k_2 + k_3 - 3 \geq n_3$).

k_3 should be greater than the number of participants in each group who are permitted to join in intergroup secret sharing. This requirement is put forward from a practical point of view. Local participants in each group are able to recover their group's secret, and shared participants are able to recover the secret between groups. But participants in one group should not have permission to get the intergroup secret. k_3 is the minimum number of participants to recover the secret between the groups. As a result, k_3 should be greater than the number of participants in each group who are allowed to join in secret sharing between groups.

$n_i \geq k_i \quad (i = 1, 2, 3)$. The polynomial secret sharing scheme requires the threshold number to meet this requirement.

$n_1 + n_2 \geq n_3$. The total number of participants should be greater than or equal to the number of participants in secret sharing between groups.

5. Experiment and Comparison

In this section, we give three examples. The first example realizes the secret sharing of the intragroup $(2, 3)$ thresholds and intergroup $(3, 3)$ thresholds, the second example realizes the secret sharing of the intragroup $(2, 4)$ thresholds and intergroup $(3, 3)$ thresholds, and the third example realizes the secret sharing of the intragroup $(3, 4)$ thresholds and intergroup $(4, 4)$ thresholds. In Section 5.1, the feasibility of the scheme is verified; in Section 5.2, the experimental analysis is given; and in Section 5.3, we compare our scheme with other secret sharing schemes within one group and between groups.

5.1. Introduction of the Experiment

5.1.1. Experiment One. In the first experiment, we realized the SIS of the intragroup $(2, 3)$ thresholds and intergroup $(3, 3)$ thresholds. The experimental process is as follows. There are two groups with six participants. There are three local participants (P_1, P_2, P_3) in G_1 and three local participants (P_4, P_5, P_6) in G_2. The order numbers of $P_1, P_2, P_3, P_4, P_5, P_6$ are $1, 2, 3, 4, 5, 6$, respectively; and there are three shared participants (P_1, P_2, P_4) in intergroup secret sharing. Each participant has only one shadow image.

All participants in their own group can participate in the SIS within the group, and specific participants can participate in the SIS between the groups. In this example, P_1, P_2, P_3 can participate in recovering the secret of G_1, P_4, P_5, P_6 can participate in recovering the secret of G_2, and P_1, P_2, P_4 can participate in recovering the intergroup secret. When recovering the secret image within the group, at least two local participants are required; when recovering the secret image between groups, all three shared participants are required. The size of the intragroup and intergroup secret images is 256×256. The membership is shown in Table 2.

The sharing process is as follows. The intragroup secret image of G_1 is shared into three shadow images by our proposed screening method, and they are distributed to participants P_1, P_2, and P_3. The secret image of G_2 is also shared into three shadow images, which are distributed to participants P_4, P_5, and P_6.

Figure 3 shows the intragroup secret images of G_1, G_2, the intergroup secret image of G_1 and G_2, and the shadow images. The secret image of G_1 is given in Figure 3(a), and Figures 3(d) ~ 3(f) display the shadow images held by P_1, P_2, and P_3; the secret image of G_2 is given in Figure 3(b), and Figures 3(g) ~ 3(i) display the shadow images held by P_4, P_5, and P_6. The intergroup secret images of G_1 and G_2 are given in Figure 3(c).

When recovering the secret image within a group, at least two participants are required. By using Shamir polynomial scheme, any two of P_1, P_2, P_3 can recover the secret of G_1, and any two of P_4, P_5, P_6 can recover the secret of G_2. When recovering intergroup secret, it takes three participants to join in. The secret image can be recovered if all P_1, P_2, P_4 are involved. The recovered secret image is shown in Figure 4.

5.1.2. Experiment Two. In the second experiment, we realized the SIS of the intragroup $(2, 4)$ thresholds and intergroup $(3, 3)$ thresholds. The membership of the experiment is shown in Table 3. Each of the two groups has four participants (P_1, P_2, P_3, P_4 in G_1, P_5, P_6, P_7, P_8 in G_2). The order numbers of $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$ are $1, 2, 3, 4, 5, 6, 7, 8$, respectively; and we assigned P_1, P_4, P_7 to participate in the SIS between G_1 and G_2.

Through our proposed screening method, the secret images of G_1 and G_2 are shared into four shadow images, respectively. The intragroup secret images, the intergroup secret image, and the shadow images are shown in Figure 5.

When recovering the secret within a group, any two participants can recover the secret image; when recovering the secret between groups, three designated participants are all required to recover the secret image. Any two of SC_1, SC_2, SC_3, SC_4 can recover S_1, and any two of SC_5, SC_6, SC_7, SC_8 can recover S_2. SC_1, SC_4, SC_7 are required to recover $S_{1,2}$. The images recovered from the shadow images are shown in Figure 6.

Table 2: The membership of the experiment.

Participant	Group	Whether to participate in intergroup secret sharing
P_1	G_1	Yes
P_2	G_1	Yes
P_3	G_1	No
P_4	G_2	Yes
P_5	G_2	No
P_6	G_2	No

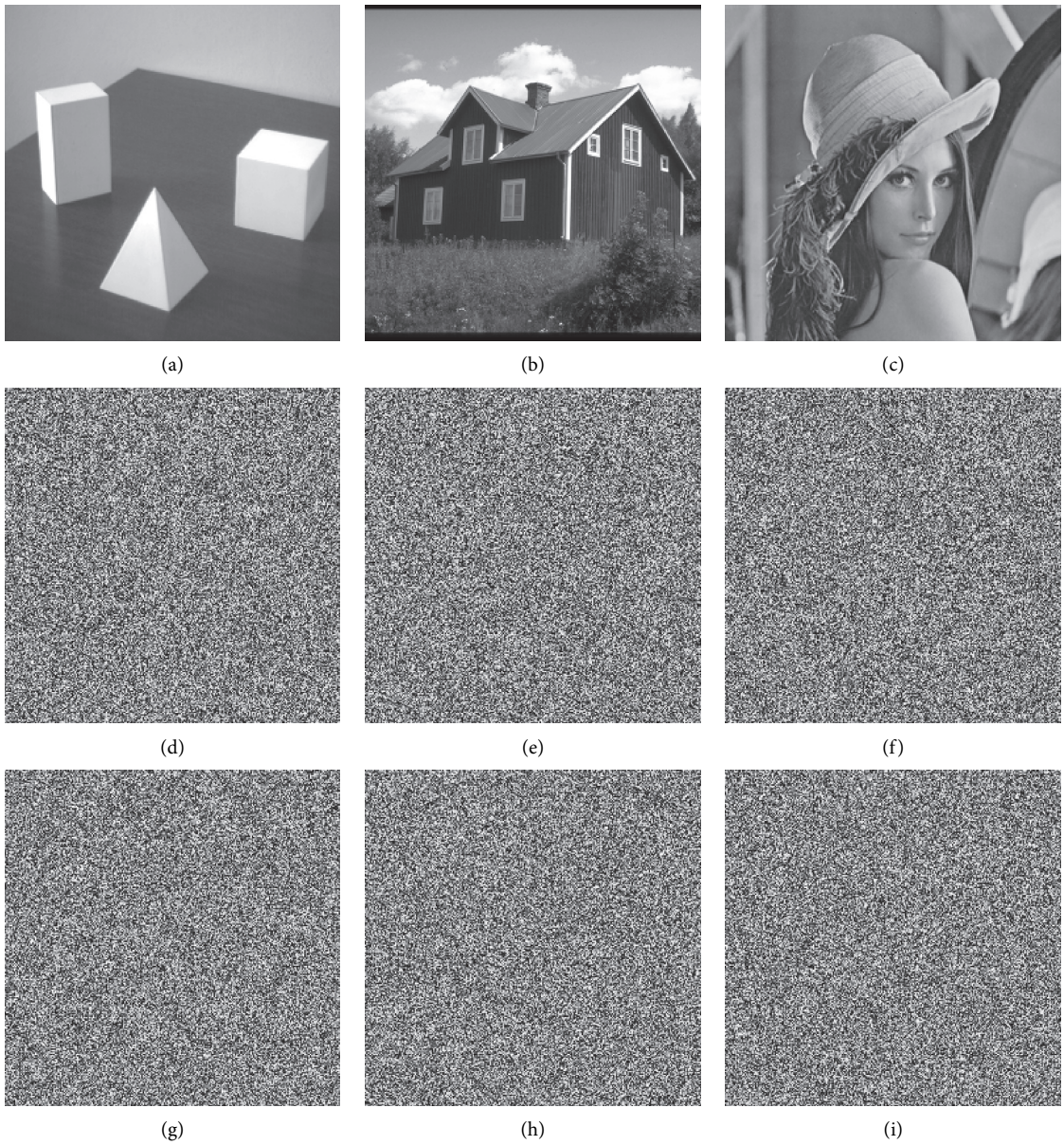

Figure 3: The intragroup and intergroup secret images and the shadow images. (a) S_1. (b) S_2. (c) $S_{1,2}$. (d) SC_1. (e) SC_2. (f) SC_3. (g) SC_4. (h) SC_5. (i) SC_6. $SC_1 \sim SC_3$ are the shadows of G_1. $SC_4 \sim SC_6$ are the shadows of G_2.

5.1.3. Experiment Three. In the third experiment, we realized the SIS of intragroup $(3, 4)$ thresholds and intergroup $(4, 4)$ thresholds. P_1, P_2, P_3, P_4 (P_5, P_6, P_7, P_8) are the local participants of G_1 (G_2); and we assigned P_1, P_2, P_5, P_6 to participate in the SIS between G_1 and G_2. The order numbers are the same as those in the second experiment. Three local participants are required to reconstruct the intragroup secret image. Four shared participants participate in intergroup secret sharing and they are all required to reconstruct the secret image.

(a) (b) (c)

Figure 4: The intragroup and intergroup secret images recovered from the shadow images. (a) S_1'. (b) S_2'. (c) $S_{1,2}'$.

Table 3: The membership of the experiment.

Participant	Group	Whether to participate in intergroup secret sharing
P_1	G_1	Yes
P_2	G_1	No
P_3	G_1	No
P_4	G_1	Yes
P_5	G_2	No
P_6	G_2	No
P_7	G_2	Yes
P_8	G_2	No

As shown in Figure 7, the secret images of G_1 and G_2 are shared into four shadow images, respectively, by our proposed random elements utilization model.

Any three of SC_1, SC_2, SC_3, SC_4 can recover S_1, and any three of SC_5, SC_6, SC_7, SC_8 can recover S_2. SC_1, SC_2, SC_5, SC_6 are required to recover $S_{1,2}$. The images recovered from the shadow images are shown in Figure 8.

5.2. Experimental Analysis. Compared with the first experiment, the intragroup threshold in the second experiment changed from $(2, 3)$ to $(3, 3)$, and the intergroup threshold remained unchanged. The number of shared participants of the two experiments and the structure of the two equation systems are the same. The difference between the two experiments is the number of shadow images in a group, and it does not affect the solution of the system.

Compared with the first two experiments, the third experiment has a greater intragroup threshold, which means that there are more variable coefficients in the system. At the same time, the intergroup threshold in the third experiment is greater than those of the first two experiments, which means that there are more restrictions. The threshold parameters in the third experiment satisfy the constraints that need to be satisfied (i.e., $k_1 = 3, k_2 = 3, k_3 = 4, n_3 = 4, k_1 + k_2 + k_3 - 3 \geq n_3$), so there exists a solution in the system.

We use the random elements utilization model to select polynomial coefficients satisfying certain conditions and realize the intragroup and intergroup SIS with each participant holding one shadow image. The experimental results show that the scheme is feasible.

5.3. Comparison. In this section, we compare the proposed scheme with other secret sharing schemes within one group and between groups. The comparisons of the main features are shown in Table 4.

The MLSS scheme proposed by Guo et al. [21] realized that each participant has different privileges to restore the secret image and can achieve lossless restoration. Pakniat et al. [22] improved the scheme and enhanced the security. Both two schemes need a dealer to divide the secret into parts with different widths and heights and give each participant a shadow of the corresponding hierarchy. Wu et al. [24] proposed a hierarchical secret sharing scheme between two groups, in which the secret image could not be restored unless participants from both groups joined in the recovery. The SIS with a hierarchical threshold access structure mentioned above all share one secret image within a group or between two groups.

The tightly coupled secret sharing scheme based on CRT proposed by Meng et al. [25] is the first time to propose secret sharing among multiple groups without any hierarchy. In this MGSS scheme, participants can go to another group to participate in the secret recovery. The secret image can be restored without loss and the computation is relatively small. However, the same secret is shared within one group and between groups in this scenario and there has to be a dealer to send an extra message to a participant who wants to participate in the secret recovery between groups. In our scheme, secrets within one group and between groups are completely different and independent, which has a different application scenery in real life.

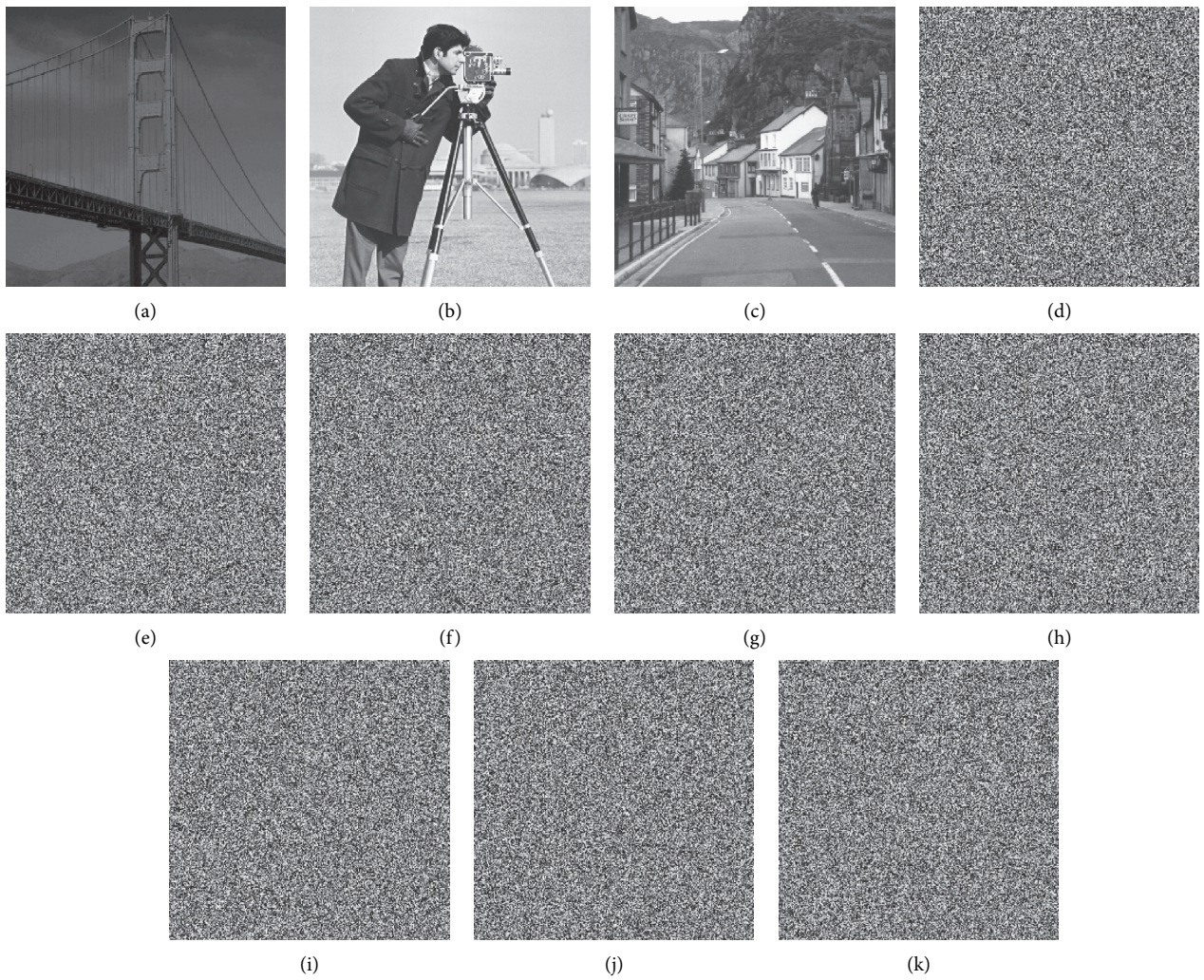

Figure 5: The intragroup and intergroup secret images and the shadow images. (a) S_1. (b) S_2. (c) $S_{1,2}$. (d) SC_1. (e) SC_2. (f) SC_3. (g) SC_4. (h) SC_5. (i) SC_6. (j) SC_7. (k) SC_8. $SC_1 \sim SC_4$ are the shadows of G_1. $SC_5 \sim SC_8$ are the shadows of G_2.

Figure 6: The intragroup and intergroup secret images recovered from the shadow images. (a) S_1'. (b) S_2'. (c) $S_{1,2}'$.

For Yang et al.'s [26] scheme, sharing and recovering multiple secrets between multiple groups is proposed for the first time. In the scheme, $2^m - 1$ secret images are shared among m groups, and the recovery is lossless. However, in this scheme, multiple shadow images are held by a participant who participates in both intragroup and intergroup secret sharing. In our scheme, every participant holds only one shadow image, which is easier to manipulate and more secure in practical applications. Besides, Yang et al.'s scheme is proposed on the basis of GF(2^8) domain and needs to calculate the basis matrix, so it requires a large amount of calculation, while our scheme requires a smaller amount of calculation.

To sum up, the advantages of our scheme are as follows: compared with the existing MLSS and MGSS schemes, we

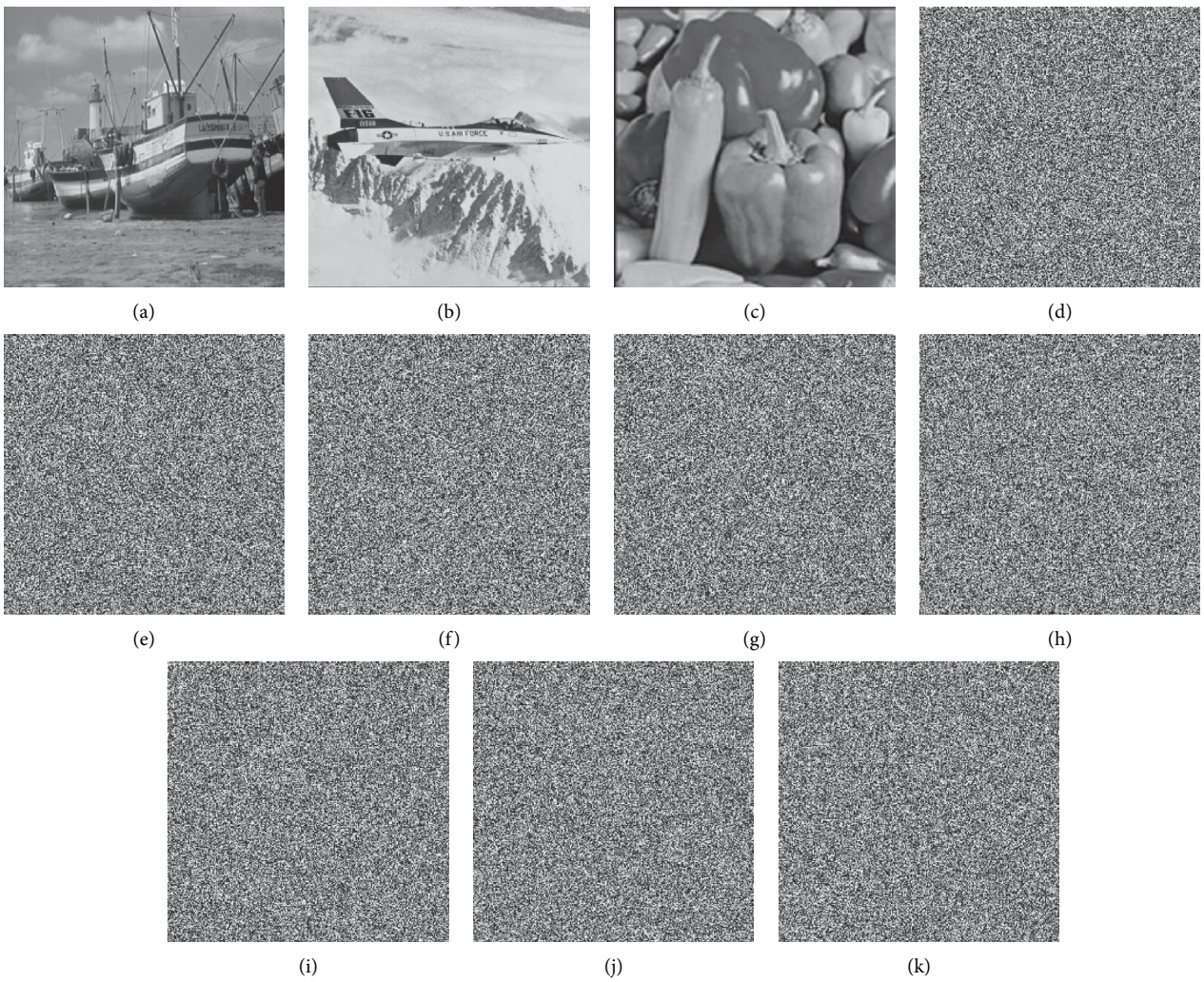

Figure 7: The intragroup and intergroup secret images and the shadow images. (a) S_1. (b) S_2. (c) $S_{1,2}$. (d) SC_1. (e) SC_2. (f) SC_3. (g) SC_4. (h) SC_5. (i) SC_6. (j) SC_7. (k) SC_8. $SC_1 \sim SC_4$ are the shadows of G_1. $SC_5 \sim SC_8$ are the shadows of G_2.

Figure 8: The intragroup and intergroup secret images recovered from the shadow images. (a) S_1'. (b) S_2'. (c) $S_{1,2}'$.

can share multiple secret images within one group and between groups; compared with Yang et al.'s [26] scheme, each participant only needs to hold one shadow image in the proposed scheme based on the random elements utilization model and there is no information leakage in the process of inter-roup SIS.

Table 4: Comparisons of the main features.

	Guo et al. [21]	Pakniat et al. [22]	Wu et al. [24]	Meng et al. [25]	Yang et al. [26]	Proposed scheme
Based method	Polynomial	$GF(2^8)$	Polynomial	CRT	$GF(2^8)$	Polynomial
Number of groups	1	1	2	m	m	2
Number of secrets	1	1	1	1	$2^m - 1$	3
The number of shadows held by a participant	One	One	One	One	Multiple	One
Computational complexity	Easy	Easy	Easy	Easy	Complicated	Easy
Is there a dealer?	Yes	Yes	No	Yes	No	Yes

6. Conclusion

In this paper, we proposed an intragroup and intergroup secret sharing scheme, in which each participant holds one shadow image. There is no need for additional information to participate in secret recovery between groups. Participants who are able to join in the intergroup secret recovery are assigned in advance and when the number of legal participants reaches the threshold, they can recover the intergroup secret. Participants without permission can only participate in the secret recovery within the group but cannot participate in the secret recovery between groups. Even if they participate, they cannot recover the true secret. The secrets within one group and between groups are completely different and the scheme is simple to implement; thus it has a good application prospect in real life. In future work, we will further extend our scheme to SIS between more than two groups.

Data Availability

Some or all data, models, or codes generated or used during the study are available from the corresponding author upon request (publictiger@126.com).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (no. 61602491).

References

[1] S. Adi, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of the Afips National Computer Conference*, vol. 48, p. 313, 1979.

[3] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, no. 9, pp. 1–12, 1994.

[4] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," *Multimedia Tools and Applications*, vol. 74, no. 9, pp. 3231–3252, 2015.

[5] A. A. Abd El-Latif, X. Yan, L. Li, N. Wang, J.-L. Peng, and X. Niu, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics & Laser Technology*, vol. 54, pp. 389–400, 2013.

[6] T. Katoh and H. Imai, "An extended construction method for visual secret sharing schemes," *Electronics and Communications in Japan*, vol. 81, no. 7, pp. 55–63, 2010.

[7] Z. Zhi Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441–2453, 2006.

[8] X. Yan, X. Liu, and C. N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, vol. 14, 2018.

[9] S. Wang, X. Yan, J. Sang, and X. Niu, "Meaningful visual secret sharing based on error diffusion and random grids," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3353–3373, 2016.

[10] X. Yan, Y. Lu, C.-N. Yang, X. Zhang, and S. Wang, "A common method of share authentication in image secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology Early Access*, vol. 31, no. 7, pp. 2896–2908, 2021.

[11] X. Yan, S. Wang, L. Li, A. El-Latif, Z. Wei, and X. Niu, "A new assessment measure of shadow image quality based on error diffusion techniques," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 118–126, 2013.

[12] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[13] P. Li, C. N. Yang, and Z. Zhou, "Essential secret image sharing scheme with the same size of shadows," *Digital Signal Processing*, vol. 50, p. 12, 2015.

[14] A. Kanso and M. Ghebleh, "An efficient (t, n)-threshold secret image sharing scheme," *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 1–20, 2016.

[15] Y. Liu and C. Yang, "Scalable secret image sharing scheme with essential shadows," *Signal Processing Image Communication*, vol. 58, 2017.

[16] P. Li, C.-N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 41–50, 2018.

[17] Y.-X. Hu and Y.-N. Liu, "A progressively essential secret image sharing scheme using hierarchy shadow," *Journal of Information Security and Applications*, vol. 47, pp. 371–376, 2019.

[18] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology*, vol. 20, no. 2, pp. 237–264, 2007.

[19] E. Brickell, "Some ideal secret sharing schemes," *Lecture Notes in Computer Science*, vol. 434, no. 4, pp. 468–475, 1989.

[20] L. Harn and M. Fuyou, "Multilevel threshold secret sharing based on the Chinese remainder theorem," *Information Processing Letters*, vol. 114, no. 9, pp. 504–509, 2014.

[21] C. Guo, C.-C. Chang, and C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, vol. 33, no. 1, pp. 83–91, 2012.

[22] N. Pakniat, M. Noroozi, and Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," *Journal*

of Visual Communication and Image Representation, vol. 25, no. 5, pp. 1093–1101, 2014.

[23] H. X. Li, L. J. Pang, and W. D. Cai, "An efficient threshold multi-group-secret sharing scheme," in *Proceedings of the International Conference on Fuzzy Information and Engineering*, Guangzhou, China, May 2007.

[24] Z. Wu, Y. Liu, and X. Jia, "A novel hierarchical secret image sharing scheme with multi-group joint management," *Mathematics*, vol. 8, 2020.

[25] K. Meng, F. Miao, W. Huang, and Y. Xiong, "Tightly coupled multi-group threshold secret sharing based on Chinese remainder theorem," *Discrete Applied Mathematics*, vol. 268, pp. 152–163, 2019.

[26] C. N. Yang, X. Wu, H. Y. Lin, and H. Y. Lin, "Intragroup and intergroup secret image sharing based on homomorphic Lagrange interpolation," *Journal of Information Security and Applications*, vol. 61, 2021.