Hindawi
Security and Communication Networks
Volume 2021, Article ID 5597592, 11 pages
https://doi.org/10.1155/2021/5597592

Research Article

Weighted Polynomial-Based Secret Image Sharing Scheme with Lossless Recovery

Yongjie Wang, Jia Chen, Qinghong Gong, Xuehu Yan, and Yuyuan Sun

National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Jia Chen; chenjia9624@nudt.edu.cn and Xuehu Yan; publictiger@126.com

Received 3 March 2021; Revised 14 April 2021; Accepted 16 May 2021; Published 25 May 2021

Academic Editor: Jialiang Peng

In some particular scenes, the shadows need to be given different weights to represent the participants' status or importance. And during the reconstruction, participants with different weights obtain various quality reconstructed images. However, the existing schemes based on visual secret sharing (VSS) and the Chinese remainder theorem (CRT) have some disadvantages. In this paper, we propose a weighted polynomial-based SIS scheme in the field of GF (257). We use (k, k) threshold polynomial-based secret image sharing (SIS) to generate k shares and assign them corresponding weights. Then, the remaining $n - k$ shares are randomly filled with invalid value 0 or 255. When the threshold is satisfied, the number and weight of share can affect the reconstructed image's quality. Our proposed scheme has the property of lossless recovery. And the average light transmission of shares in our scheme is identical. Experiments and theoretical analysis show that the proposed scheme is practical and feasible. Besides, the quality of the reconstructed image is consistent with the theoretical derivation.

1. Introduction

With the development of Internet technology and digital multimedia technology, digital images are more and more widely used. Meanwhile, security is also threatened. In particular, personal privacy images, confidential commercial images, medical images, and military drawings are easy to be intercepted, tampered, and destroyed in the process of storage and transmission. Cryptography [1, 2] and steganography [3, 4] are commonly used to protect images. A normal image is converted into a noise-like image through encryption technology. We cannot understand the secret image, but we can tamper with or destroy it, because it is clear that the image has been encrypted. Steganography improves the security of images, making it difficult for attackers to detect the existence of secret information. But steganography is the single-channel transmission, and if part of the area of data hiding is lost in transmission, the secret message could not be recovered.

Secret sharing (SS) is another technology to protect data with the features of multichannel transmission and loss tolerance. In 1979, Shamir [5] and Blakley [6] independently proposed the (k, n)-threshold SS scheme. The extension of SS to images is called secret image sharing (SIS). The secret image can be distributed among n participants by dividing it into n shadow images (also called shares or shadows). The secret can be reconstructed from any k or more authorized shadow images, while any $k - 1$ or fewer shadow images could not recover the secret. At present, in the SIS research field, visual cryptography schemes (VCS), also called visual secret sharing (VSS), schemes based on the CRT, and polynomial-based SIS schemes are the primary branches.

In 1995, Noar and Shamir [7] first proposed the (k, n)-threshold VCS. In general VCS, a binary image is encrypted to n shadow images on transparencies. The secret image can be obtained by superposing any k or more shadow images. The recovery process relies on the human visual system (HVS) and does not require cryptographic computation or device [8, 9]. According to the implementation principle, the VCS can be divided into schemes based on the basis matrix [7] and the random grid [10]. In the VCS field, current researches focus on these areas, including improving the visual quality of reconstructed images [11, 12],

implementing general access structures [13, 14], share authentication [15], and meaningful shadow images [16–18].

Mignotte [19] first proposed the (k, n)-threshold SS scheme based on the CRT in 1982. Then, Asmuth and Bloom [20] proposed a threshold SS scheme based on the CRT with random factors A. In their scheme, a set of integers $\{p, m_1 < m_2 < \cdots < m_n\}$ is chosen subject to certain conditions. Then, $A \in [\lfloor N/p \rfloor, \lceil (M/p) - 1 \rceil]$, where p is a prime number, $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$. Yan et al. [21] first applied the CRT to SIS. But the scheme has slight information leakage, and the recovery is lossy. Yan et al. [22] proposed a (k, n)-threshold SIS based on CRT for grayscale images. The scheme is lossless recovery and without auxiliary encryption. After that, most of the SIS schemes [23, 24] based on the CRT were studied based on Asmuth and Mignotte's scheme.

Thien and Lin [25] applied SS proposed by Shamir to SIS and first proposed a (k, n)-threshold SIS scheme. For the polynomial-based SIS, the sharing and recovery processes are simple, efficient, and easy to implement and have fewer public parameters. Therefore, polynomial-based SIS schemes are widely used [26–28]. However, most polynomial-based SIS schemes are slightly lossy. To achieve lossless recovery, many polynomial-based SIS schemes have been studied. We can segment pixel values greater than 250, operate in the field of GF(2^8), or choose a prime number greater than 255. In this paper, we choose the prime number 257 and use the screening operation to achieve lossless recovery.

In the above SIS schemes, the participants have the same weight and importance. However, in some scenarios, to indicate the status or importance of the participants, the shadow images need to be given different weights. Hou et al. [29] proposed a privilege-based VSS model. The model implemented a $(2, n)$-threshold VSS without pixel expansion. The participants of their scheme have the same size and different privileges. In the recovery phase, the greater the shadows' weight, the better the quality of the reconstructed image. But the average light transmissions of shares are not equal. Yang et al. [30] extended Hou et al.'s scheme with a correct privilege level, achieving the consistency of the average light transmission and the sum of privilege levels. Both Hou and Yang's schemes require a codebook and are lossy in recovery. Liu et al. [31] proposed a weighted (k, n)-threshold random grid VSS(RG-VSS) with lossless recovery. Each share has a weight in their scheme, and the secret image can be recovered by OR and XOR operations. Especially, the recovered image is lossless when using XOR operations. The secret image format of the weighted VSS schemes is only binary image. Tan et al. [23] proposed a weighted (k, n)-threshold SIS scheme based on the CRT for sharing grayscale images. Tan et al.'s scheme requires a weight generation modulus. And the average light transmissions of shares of their scheme are also unequal. To sum up, the weighted schemes based on VSS are lossy and can only share the binary images, not grayscale images. For the weighted schemes based on the CRT, we need to set parameters according to requirements in advance, and the number of participants is limited. Compared with VSS and CRT, polynomial-based SIS has some advantages. Therefore, we consider combining polynomial-based SIS with different weights to overcome the above disadvantages.

In this paper, we propose a weighted polynomial-based SIS scheme with lossless recovery. Each share is assigned to a weight. We improve Thien and Lin's scheme, choosing the prime number 257 and using the screening operation to achieve lossless recovery. A polynomial generates the n share pixel values, and then k of them are selected according to their weights. The remaining $n - k$ shadows are randomly filled with invalid value 0 or 255. In the recovery phase, when the threshold is satisfied, the greater the weight of one of the shadows or the number of shadows, the better the quality of the recovery secret image.

The contributions of our work are summarized as follows:

(1) We propose a weighted polynomial-based SIS scheme in the field of GF(257).

(2) When the threshold is satisfied, the number and weight of share can affect the quality of the reconstructed image. And the reconstructed image is lossless when all shares are selected.

(3) The scheme overcomes the problem that the average light transmissions of shares are not identical.

The rest of this paper is organized as follows. In Section 2, we review Shamir's scheme and Thien and Lin's scheme and then introduce the definition of the correct recovery probability (CRP). The proposed scheme and the theoretical analyses are described in Section 3. Section 4 gives experimental results and comparisons. Finally, conclusions are drawn in Section 5.

2. Preliminaries

In this section, we review the polynomial-based SIS schemes proposed by Shamir and Thien and Lin. Then, the evaluation parameter CRP of the reconstructed secret images of our scheme is given.

2.1. Review of Shamir's Scheme. In 1997, Shamir [5] proposed the (k, n)-threshold SS scheme based on polynomial properties. If a plane has k points, there exists a unique $k - 1$ degree polynomial. Shamir shared a secret S into n different shares $S_1, S_2, \ldots, S_n$ based on this property. Then, n shares were distributed to n participants $P_1, P_2, \ldots, P_n$. The secret S was chosen from the field of GF(p), where p is a prime greater than S and n. The polynomial of Shamir's scheme was defined as shown in

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \pmod{p}, \quad (1)$$

where the coefficient a_0 was the secret S, and the other $k - 1$ coefficients are chosen from the field of GF(p). In the sharing phase, we set $x = x_i$ and then obtain $f(x_i)$, where $i = 1, 2, \ldots, n$. The n pair of points $(x_i, f(x_i))$ were generated according to the above polynomial.

After obtaining n pair of points, any k or more of which can recover the secret S, while any $k-1$ or fewer pairs cannot recover the secret. The secret S can be reconstructed by using Lagrange's interpolation as shown in equation (2). When $x=0$, the secret was reconstructed by calculating $\psi(x)$, i. e., $S=\psi(0)$.

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

where $x_i \neq x_j$, and $i, j = 1, 2, \ldots, n$.

2.2. Review of Thien and Lin's Scheme. Thien and Lin [25] first applied the SS scheme to share a secret grayscale image in 2002. In their scheme, a secret image S was shared to n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$, and any k or more of which can recover the secret image. In Thien and Lin's scheme, all the coefficients were used to share the secret image's pixels. Then, the successive k pixels of the secret image were shared through a polynomial presents two problems. The first is that each shadow image size is $(1/k)$ of the original secret image. Second, there may be information leakage because of the correlation among pixels. Therefore, the secret image pixels should be encoded before the sharing phase to increase security. In Thien and Lin's scheme, the value of prime p was taken as 251. However, the range of the 8-bit grayscale image pixel value was $[0, 255]$. The pixels between 251 and 255 were truncated to 250, resulting in the fact that all the pixels were within $[0, 250]$. Therefore, the reconstructed secret images were lossy. At the same time, the method of lossless recovery was provided in their scheme. The secret pixel values of more than 250 required additional operations, and that led to the expansion of shadow images.

There are 256 pixels of the 8-bit grayscale image between 0 and 255. To achieve lossless recovery, all need to be included in the sharing phase. A prime number greater than 256 is 257, $[0, 255] \subset \mathrm{GF}(257)$. But 256 also belongs to $\mathrm{GF}(257)$, and the sharing process needs to be redone if a pixel value is shared to 256. Random numbers are generated to update the other $k-1$ coefficients in the polynomial except a_0 until all the share pixel values are within $[0, 255]$. Thus, the probability P of an invalid value occurring when sharing a pixel is $P = (257 - 256/257) \times 100\% \approx 0.389\%$. At the same time, in the weighted SIS scheme, we filled in 0 and 255 as invalid values. That is to say, there may be three invalid values, i.e., 0, 255, and 256, during the sharing of a pixel value. The probability P_w of an invalid value occurring per share operation is $P_w = (3/257) \times 100\% \approx 1.167\%$. This can achieve lossless recovery, and the efficiency of sharing is not greatly affected, which is within the acceptable range. Therefore, in our scheme, we choose the prime number 257 and use the screening operation.

2.3. Correct Recovery Probability (CRP). For the quality evaluation of the reconstructed image in the general SIS schemes, the most commonly used is mean squared error (MSE) and peak sign-to-noise value relation (PSNR). MSE is used to assess the distinction between the recovered image and the secret image. The lower MSE value indicates that the reconstructed image is close to the original image. PSNR represents the reconstructed image's quality. The higher the PSNR value is, the closer the reconstructed image is to the original image.

In our weighted SIS scheme, we adopt the correct recovery probability (CRP) [32] to evaluate the reconstructed image's quality. CRP is the ratio of the number of identical pixels in the same locations between the reconstructed image and the secret image to the image's total pixels. The higher the CRP value is, the more the number of pixel values is recovered correctly, that is, the closer the reconstructed image is to the secret image. The reconstructed image is lossless when $\mathrm{CRP} = 1$.

For a secret image S with the size of $A \times B$, the CRP of its reconstructed image S' is calculated by

$$\mathrm{CRP} = \frac{T}{A \times B}, \tag{3}$$

where T is the number of identical pixels in the same locations in both two images.

3. The Proposed Scheme

In this section, we propose a weighted polynomial-based SIS scheme based on Shamir's scheme. To achieve lossless recovery, we choose the prime number 257 and use the screening operation. Each participating shadow image is assigned a weight, and the sum of these weights is equal to 1. Each pixel of the secret image generates k share pixel values by a polynomial, and we assign them weights. The remaining $n-k$ shares are randomly filled with invalid value 0 or 255.

When recovering the secret image, we adopt Lagrangian interpolation to obtain the secret pixel values. The secret image cannot be recovered from less than k shares. When more than k shares are collected, the higher the weights of the shares are, the better the recovered secret image's quality is. At the same time, our scheme can achieve lossless recovery when all the shadow images are used to participate in the recovery. The design idea of the sharing phase of our scheme is shown in Figure 1.

3.1. The Sharing Phase. In the sharing phase of our scheme, for each pixel of the original secret image, k share pixels are generated by the polynomial-based SIS scheme with a (k, k)-threshold ($\mathrm{PSIS}(k, k)$). Then, k shares are distributed to k participants through a certain probability determined by the weights of the participants, and the shares of the other $n-k$ participants are filled with invalid values. The detailed steps are described in Algorithm 1.

In the sharing phase, each shadow image is assigned a certain weight. Suppose that the weights of shares are $w_1, w_2, \ldots, w_n$, where $w_1 + w_2 + \cdots + w_n = 1$. Then, we set corresponding weight interval for each shadow image in the interval of $[0, 1]$ as shown in Figure 2. The proportion of the $t-$th interval in the whole interval is w_t. We randomly generate any real numbers x in the interval of $[0, 1]$. If $x \in [w_1 + w_2 + \cdots + w_{t-1}, w_1 + w_2 + \cdots + w_{t-1} + w_t]$,

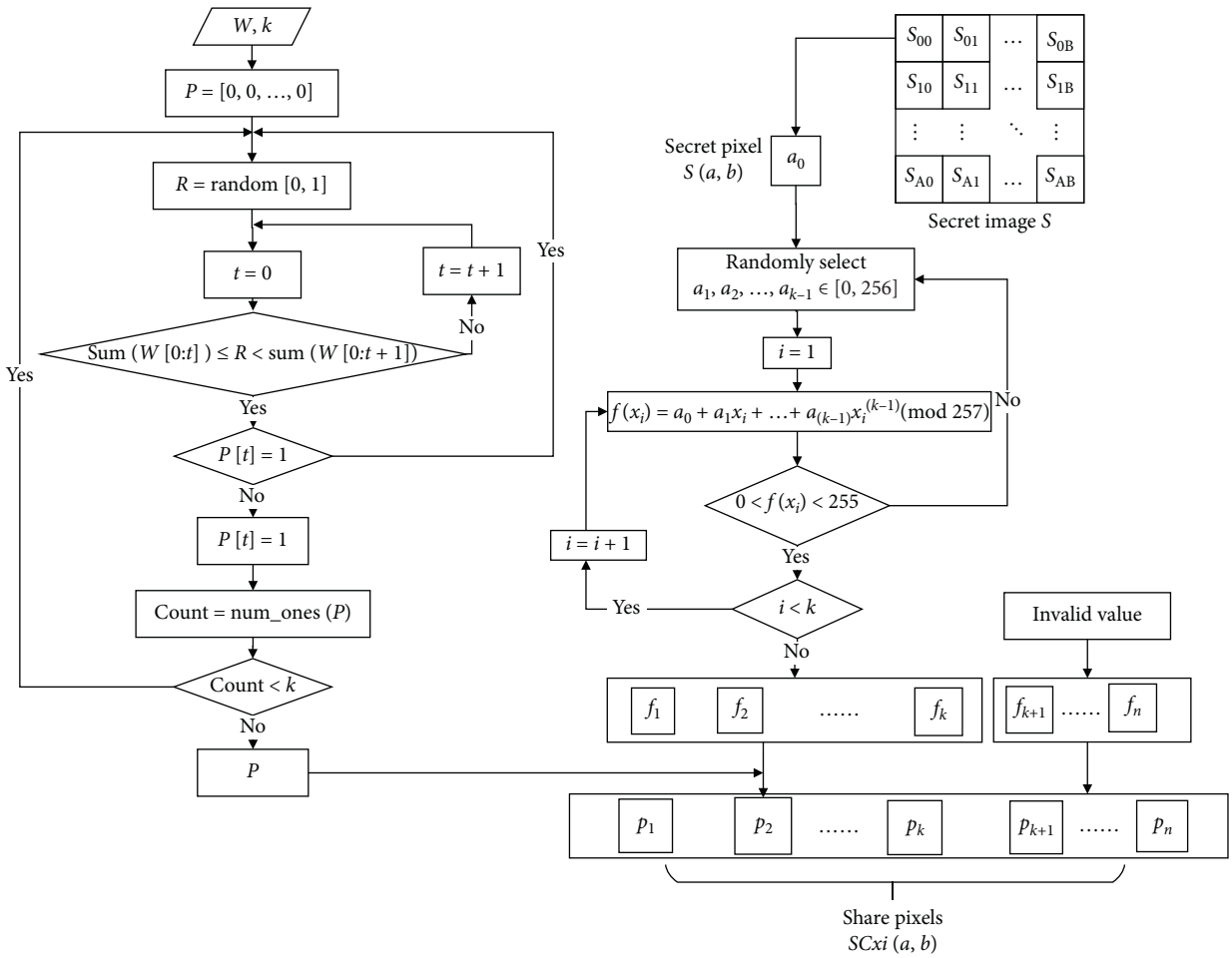

Figure 1: The flowchart for generating shares with different weights.

(1) Input: a secret image S with the size of $A \times B$; the threshold parameters (k, n); n participant serial numbers $x_1, x_2, \ldots, x_n$; the weights $W = [w_1, w_2, \ldots, w_n]$; initial share allocation list P.
(2) Output: n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$.
(3) Step 1. Repeat Steps 2–7 for each pixel of the secret image, where the pixel position is $(a, b) \in \{(a, b) | 1 \le a \le A, 1 \le b \le B\}$.
(4) Step 2. Randomly generate any real number R in the interval of [0, 1]. When $\mathrm{sum}(W[0: t]) < R < \mathrm{sum}(W[0: t + 1])$, let $P[t] = 1$. If $P[t]$ has been set to 1, a random number will be generated again until the number of "1" in the share allocation list P is k.
(5) Step 3. Set polynomial coefficient, where $a_0 = s$, and $a_1, \ldots, a_{k-1}$ are assigned to a random value within the field of GF(257).
(6) Step 4. Repeat Steps 5–6 until k share values are calculated for each participant $P(x_i)(i \in [1, k])$.
(7) Step 5. Calculate the shared value $f(x_i)$ by the formula $f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \bmod 257$.
(8) Step 6. If $0 < f(x_i) < 255$, continue or return to Step 3 and redo Steps 3–6.
(9) Step 7. Scan the share allocation list P; if $P[t] = 1$, valid values $f(x_i)$, $(i \in [1, k])$ are assigned to $\mathrm{SC}_t(a, b)$; if $P[t] = 0$, randomly fill in the invalid value.
(10) Step 8. Output n shadow images $\mathrm{SC}_1, \mathrm{SC}_2, \ldots, \mathrm{SC}_n$.

Algorithm 1: The sharing process of the weighted polynomial-based SIS scheme.

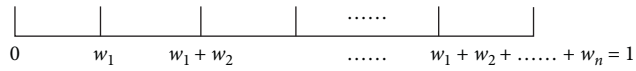

Figure 2: The weights interval partition.

participant P_t is selected, i.e., $P[t] = 1$. If the interval has been selected before that, i.e., $P[t]$ has been set to 1, then random real number will be generated to perform the above operation. This process is repeated until k different participants are selected. By performing this operation, k shares have been distributed to k of the n participants according to a certain probability, while the remaining $n - k$ participants have been distributed to invalid values.

3.2. The Recovery Phase. Our scheme is based on the polynomial-based SIS scheme and can be recovered by Lagrangian interpolation. The secret image cannot be recovered from less than k shares. When more than k shares are collected, the higher the weights of the shares are, the better the recovered secret image's quality is. If all the shares participate in the restoration of the secret image, the reconstructed image is lossless. The specific recovery steps are shown in Algorithm 2.

3.3. Theoretical Analyses. In this subsection, some theoretical analyses of our scheme are presented. First, our weighted polynomial-based SIS scheme is based on Shamir's scheme. The constant coefficient of the polynomial is replaced with the pixel value of the secret image. And all the operations are performed in the field of GF(257). There are 256 pixels of grayscale image, and $[0, 255] \subset \mathrm{GF}(257)$. Therefore, our scheme can be applied to grayscale images. According to the principle of polynomial and Lagrange interpolation algorithm, any less than k equations cannot obtain the polynomial coefficients. Thus, $k - 1$ or fewer shares could not recover the pixel value of the secret image. Because we fill in invalid values to represent different weights of shares, when k shares are involved in reconstruction, some pixel values cannot be correctly recovered. When all shares are involved in reconstruction, we can exclude all invalid values and then use the remaining k valid values to recover the secret image's corresponding pixel value. Therefore, our scheme can achieve lossless recovery.

Then, we theoretically analyze the quality and the effect factors of the reconstructed secret image. Each share is assigned a weight w_i in the proposed scheme, and $\sum_{i=1}^{n} w_i = 1$. The reconstructed secret image's quality is related to the weights of the shares involved in the reconstruction. To evaluate the quality of the reconstructed secret image, we compared the pixels in the corresponding positions of the two images, counted the number of identical pixels in the same positions, and combined them with the weights. Then, we calculated the CRP of the reconstructed secret image in our scheme with (k, n)-threshold theoretically as $\mathrm{CRP}_t(S)$ according to

$$\mathrm{CRP}_t(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{4}$$

where k, n are threshold parameters, and t denotes the number of shares involved in the reconstruction. i_j is the j th share in the i th combination, w_{i_j} denotes the weight of share i_j, and $\sum_{j=1}^{t} w_{i_j} = 1$. The number of combinations of arbitrary k of t shares is denoted by C_t^k $(k \le t \le n)$. $\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}$ denotes the probability sum that arbitrary k of t shares are selected. The probability sum that arbitrary k of t shares are selected is denoted by $\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}$.

Intuitively, we can guess that the number and weight of shadows can affect the reconstructed secret image's quality. Theoretically, if the threshold is satisfied, and the number of shadows is increased, the recovery quality of the secret image will be better. When all shadows participate in reconstruction, the secret image can be recovered in a lossless way. That is to say, our scheme is progressive in reconstruction. Second, if the threshold is satisfied, and the weight of one of the shadows in the set increases, the recovery quality of the secret image will be better.

Assuming that there are t shadows in the set, the secret image could be recovered when these shadows participate in the recovery. The CRP of the reconstructed image is shown in equation (4). If another shadow l is added in the set to participate in the recovery, and the weight of shadow l is w_l, then the CRP of the reconstructed image of $t+1$ shadows recovery as $\mathrm{CRP}_t(S)$ is calculated by

$$\mathrm{CRP}'_t(S) = \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}. \tag{5}$$

When comparing the two reconstructed images' quality, it can be determined by subtracting $\mathrm{CRP}_t(S)$ and $\mathrm{CRP}'_t(S)$. The result is shown in

$$\mathrm{CRP}'_t(S) - \mathrm{CRP}_t(S) = \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} - \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}. \tag{6}$$

According to the properties of combinatorial numbers, equation (7) holds.

$$\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} = \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right), \tag{7}$$

where $i'_j \neq l$.

Therefore, equation (6) can be rewritten as

$$\begin{aligned} \mathrm{CRP}'_t(S) - \mathrm{CRP}_t(S) &= \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &\quad - \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &= \frac{w_l \left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j} \right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k}} > 0, \end{aligned} \tag{8}$$

where $i'_j \neq l$.

(1) Input: k shadow images $SC_{i_1}, SC_{i_2}, \ldots, SC_{i_k}$ and the corresponding participant serial number x_{i_j}, $(i_1, i_2, \ldots, i_k) \subseteq \{1, 2, \ldots, n\}$
(2) Output: the original secret image S
(3) Step 1. Repeat Steps 2–4 for each pixel $SC_{i_j}(a, b)$ of the shadow image, where $(a, b) \in \{(a, b) | 1 \le a \le A, 1 \le b \le B\}$.
(4) Step 2. Judge whether the share pixel value is invalid value 0 or 255. Only if it is valid, it will participate in the recovery.
(5) Step 3. Calculate Lagrange interpolation $f(x)$ in the field of GF(257) by the formula $\psi(x) = \sum_{j=1}^{k} f(i_j) \prod_{\substack{l=1 \\ l \neq j}}^{k} ((x - i_l)/(i_j - i_l))$. Then, set $x = 0$ to obtain $f(0)$.
(6) Step 4. $S(a, b) = f(0)$.
(7) Step 5. Output the recovered image S.

Algorithm 2: The recover procedure of the weighted polynomial-based SIS scheme.

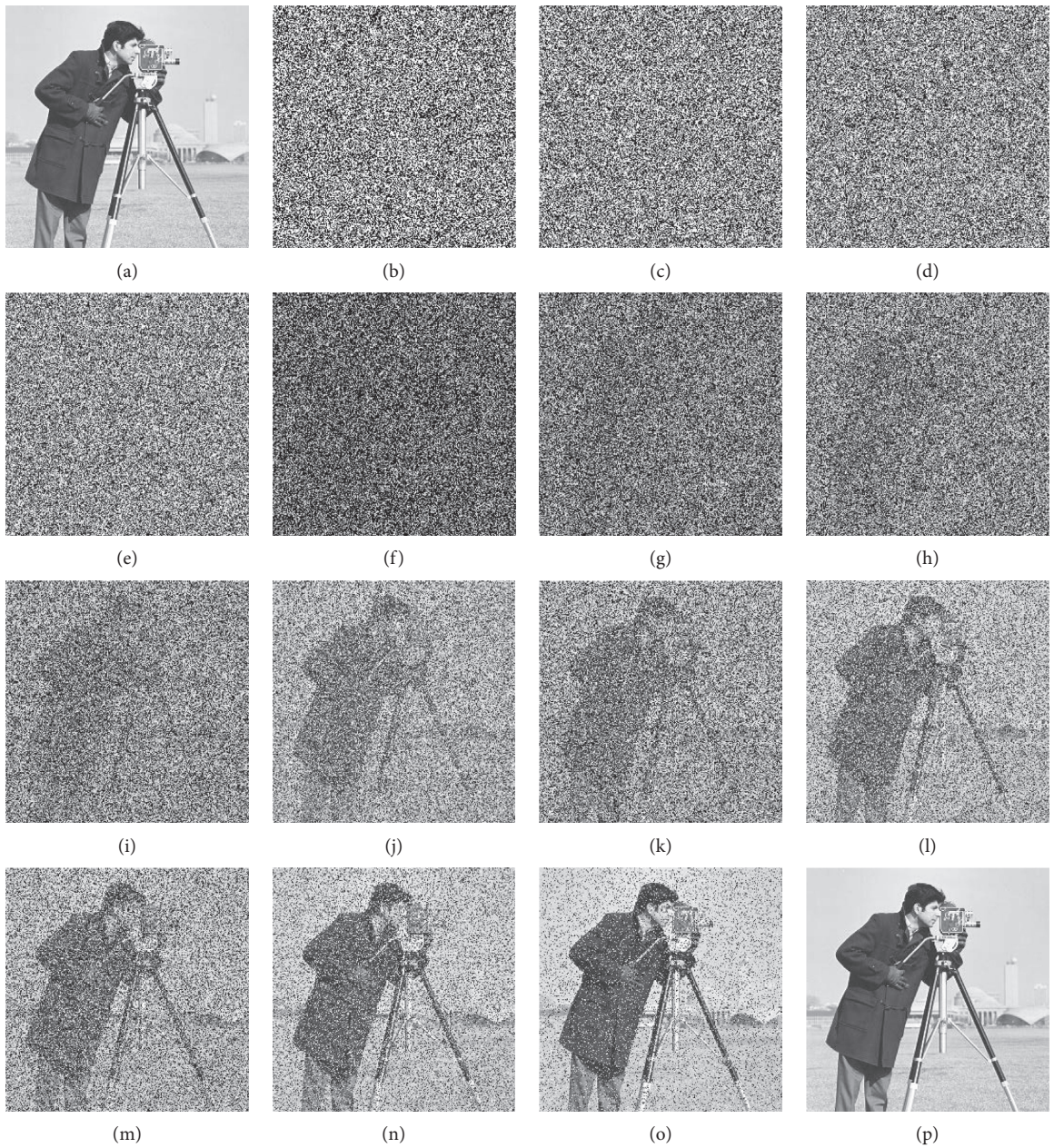

Figure 3: Our $(2, 4)$-threshold weighted SIS scheme. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) $SC_{1,2}$. (g) $SC_{1,3}$. (h) $SC_{1,4}$. (i) $SC_{2,3}$. (j) $SC_{1,2,3}$. (k) $SC_{2,4}$. (l) $SC_{1,2,4}$. (m) $SC_{3,4}$. (n) $SC_{1,3,4}$. (o) $SC_{2,3,4}$. (p) All. In $f - p$, the subscript indicates the number of shares involved in the reconstruction.

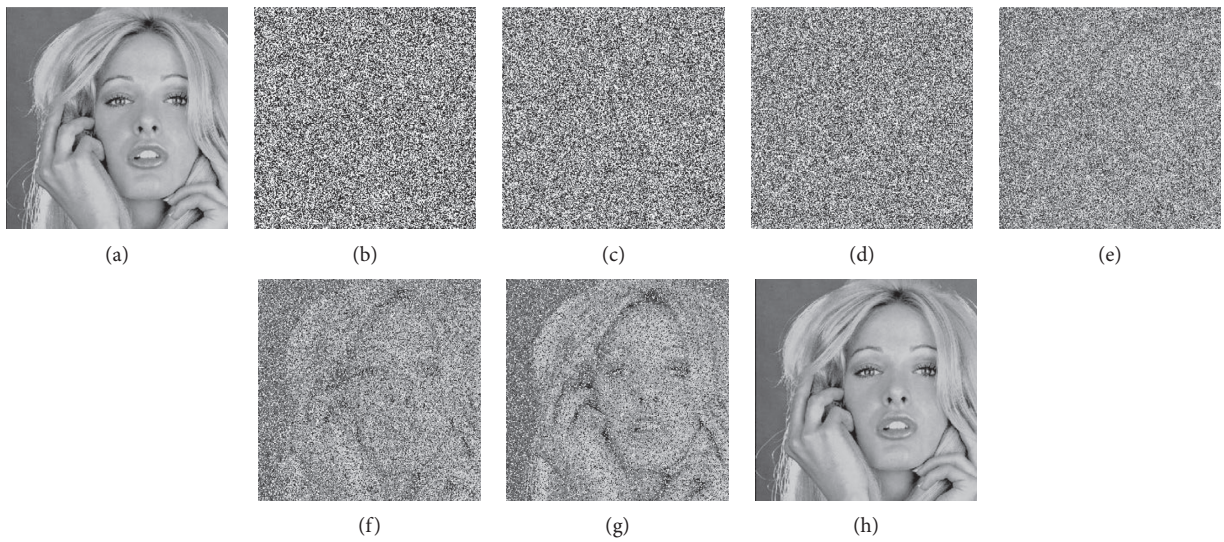

Figure 4: Our $(2,3)$-threshold weighted SIS scheme. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) $SC_{1,2}$. (f) $SC_{1,3}$. (g) $SC_{2,3}$. (h) $SC_{1,2,3}$. In $e-h$, the subscript indicates the number of shares involved in the reconstruction.

Table 1: Evaluating the quality of reconstructed images for $(2,4)$-threshold scheme.

Participants	Weights	Weights sum	Identical pixels in Tan's	Identical pixels in our	$CRP_{Our}(S)$	$CRP_{Tan}(S)$	$CRP_t(S)$
[1, 2]	[0.1, 0.2]	0.3	3258	3393	0.0497	0.0518	0.0571
[1, 3]	[0.1, 0.3]	0.4	5190	5119	0.0792	0.0781	0.0857
[1, 4]	[0.1, 0.4]	0.5	7475	7340	0.1141	0.1120	0.1143
[2, 3]	[0.2, 0.3]	0.5	10548	10703	0.1609	0.1633	0.1714
[2, 4]	[0.2, 0.4]	0.6	15392	15353	0.2349	0.2343	0.2286
[3, 4]	[0.3, 0.4]	0.7	24649	24439	0.3761	0.3729	0.3428
[1, 2, 3]	[0.1, 0.2, 0.3]	0.6	18684	18760	0.2851	0.2863	0.3143
[1, 2, 4]	[0.1, 0.2, 0.4]	0.7	25672	25781	0.3916	0.3917	0.4000
[1, 3, 4]	[0.1, 0.3, 0.4]	0.8	36937	36560	0.5636	0.5579	0.5429
[2, 3, 4]	[0.2, 0.3, 0.4]	0.9	50158	50240	0.7654	0.7666	0.7429
[1, 2, 3, 4]	[0.1, 0.2, 0.3, 0.4]	1.0	65536	65536	1.0	1.0	1.0

Table 2: Evaluating the quality of reconstructed images for $(2,3)$-threshold scheme.

Participants	Weights	Weights sum	Identical pixels	$CRP_{Our}(S)$	$CRP_t(S)$
[1, 2]	[0.2, 0.3]	0.5	10721	0.1636	0.1935
[1, 3]	[0.2, 0.5]	0.7	21326	0.3254	0.3226
[2, 3]	[0.3, 0.5]	0.8	34005	0.5189	0.4839
[1, 2, 3]	[0.2, 0.3, 0.5]	1.0	65536	1.0	1.0

In equation (8), $CRP'_t(S)$ is greater than $CRP_t(S)$. That is to say, the quality of the reconstructed secret image from $t+1$ shadows is better than that of t shadows. Therefore, if the threshold is satisfied, the reconstructed image's quality will improve with the increase in the number of shadows involved in the recovery.

Assuming that there are t shadows in the set, the secret image could be recovered when these shadows participate in the recovery. The shadow v is replaced by the more heavily weighted shadow u, where $w_v > w_u$. According to equations (8) and (7), we can get equations (9) and (10).

$$CRP_t^v(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_v\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{9}$$

where $i'_j \neq v$;

$$CRP_t^u(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_u\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i'_j}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}}, \tag{10}$$

where $i'_j \neq u$.

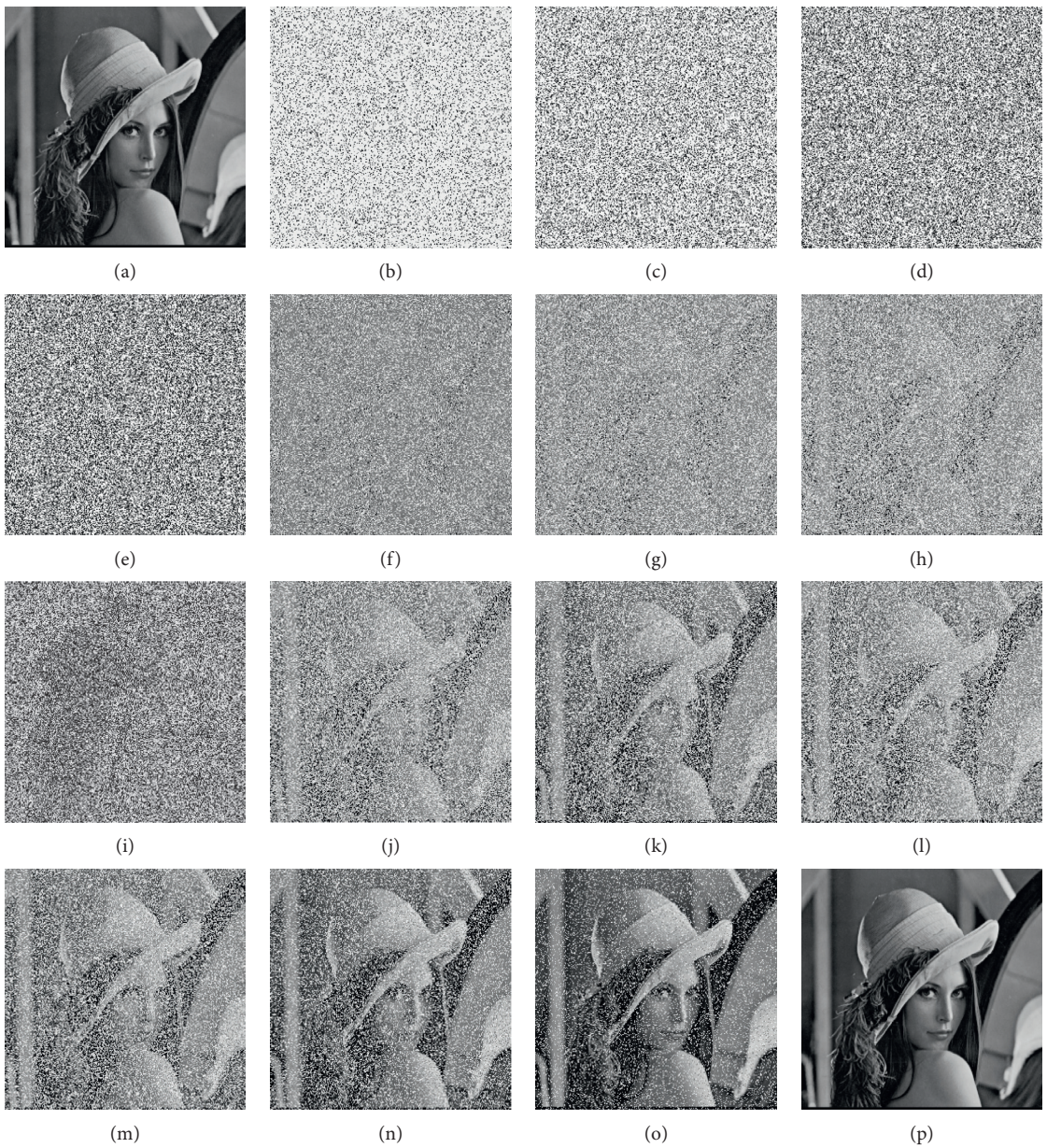

FIGURE 5: Tan's $(2, 4)$-threshold weighted SIS scheme based on CRT. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) $SC_{1,2}$. (g) $SC_{1,3}$. (h) $SC_{1,4}$. (i) $SC_{2,3}$. (j) $SC_{2,4}$. (k) $SC_{3,4}$. (l) $SC_{1,2,3}$. (m) $SC_{1,2,4}$. (n) $SC_{1,3,4}$. (o) $SC_{2,3,4}$. (p) All. In $f - p$, the subscript indicates the number of shares involved in the reconstruction.

Then, the result of subtracting equations (9) from (10) is shown in

$$\mathrm{CRP}_t^u(S) - \mathrm{CRP}_t^v(S) = \frac{(w_u - w_v)\left(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i_j'}\right)}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j} > 0.} \quad (11)$$

As shown in equation (11), $\mathrm{CRP}_t^u(S)$ is greater than $\mathrm{CRP}_t^v(S)$. Therefore, if the threshold is satisfied, the reconstructed image's quality will improve with increasing the weight of one of the shadows.

4. Experiment and Evaluation

In this section, we give two examples to verify the feasibility of the scheme in the Subsection 4.1 and evaluate the reconstructed image's quality in the Subsection 4.2. Then, we compare other weighted SIS schemes in the Subsection 4.3.

4.1. Image Illustration. To verify the feasibility of our scheme, two examples with $(2, 4)$ and $(2, 3)$ thresholds are given using Python in a PC with Windows 10. Figure 3

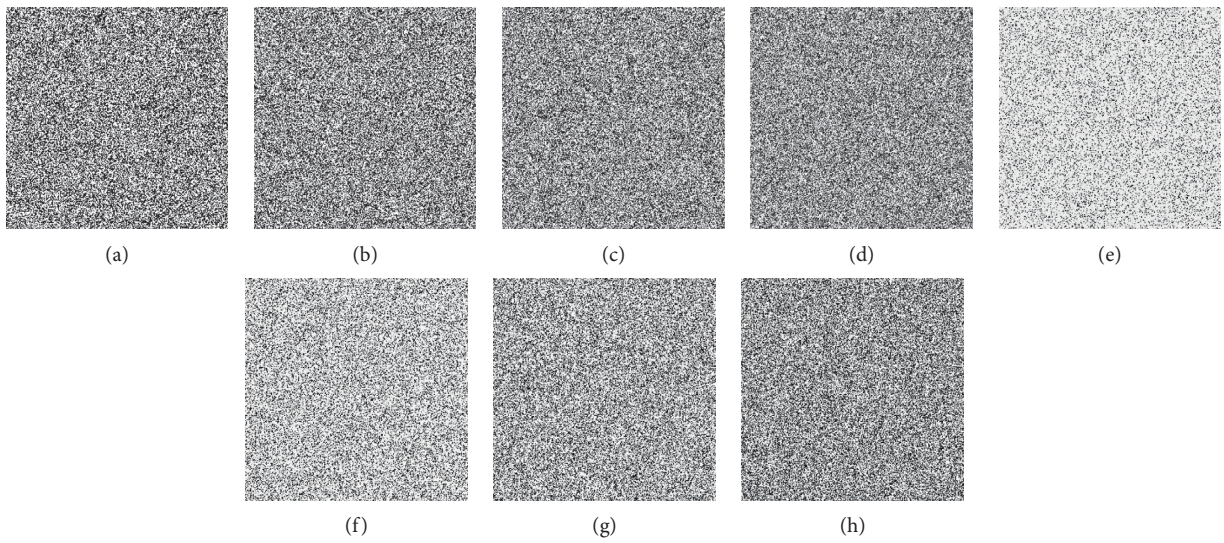

Figure 6: The average light transmission of shares in two schemes. ($a \sim d$) are our scheme. ($e \sim j$) are Tan's scheme.

Table 3: Comparisons with the characteristics of weighted schemes.

	Threshold	Image format	Based methods	Is lossless?	Identical average light transmission?	Additional information
Hou et al. [29]	$(2, n)$	Binary image	VSS	No	Yes	Codebook
Yang et al. [30]	$(2, n)$	Binary image	VSS	No	Yes	Codebook
Liu et al. [31]	(k, n)	Binary image	VSS	Yes	Yes	Weight generation and RG
Tan et al. [23]	(k, n)	Grayscale image	CRT	Yes	No	Weight generation and modulus
Our	(k, n)	Grayscale image	Polynomial	Yes	Yes	Weight generation

illustrates our $(2, 4)$-threshold SIS scheme. A Cameraman image with the size of 256×256 is tested as the secret image as shown in Figure 3(a). The weights of the shares are $W = [0.1, 0.2, 0.3, 0.4]$. Figures 3(b) ~ 3(e) show four shares generated by a polynomial. When two shares are collected, the secret image could be recovered. Figures 3(f) ~ 3(p) show the results of different weights of shares participating in recovery, and the sum of weights goes from low to high. When all shares participate in reconstruction, the secret image can be recovered in a lossless way as shown in Figure 3(p). The subscript of the name indicates the number of shadows involved in the reconstruction.

Figure 4 shows our $(2, 3)$-threshold SIS scheme. The secret image is the blonde woman image with the size of 256×256 as shown in Figure 4(a). The weights of the shares are $W = [0.2, 0.3, 0.5]$. The three shares are shown in Figures 4(b) ~ 4(d). Figures 4(e) ~ 4(g) display the reconstructed images recovered from two shares. Figure 4(h) presents the reconstructed lossless image recovered from all shares. The subscript of the name indicates the number of shadows involved in the reconstruction.

4.2. Quality of the Reconstructed Images. In our scheme, each share is assigned a weight in the sharing phase, and the recovery phase is progressive. Both the weight and the number of shadows affect the quality of the reconstructed image. The CRP is used to evaluate the quality of the reconstructed images. The greater the CRP value, the better the quality of the reconstructed image, and the more effective our scheme. Equations (4) and (5) are used to compute $\mathrm{CRP}(S)$ and $\mathrm{CRP}_t(S)$. $\mathrm{CRP}_{\mathrm{Our}}(S)$ represents the actual value of the experiment for our proposed scheme. $\mathrm{CRP}_t(S)$ denotes the theoretical value. The results of our $(2, 4)$ and $(2, 3)$ threshold weighted schemes are shown in Tables 1 and 2.

From Figure 3 and Table 1, we can draw the following conclusions:

(1) Our weighted polynomial-based SIS scheme is effective, and the shadows have weights that can affect the quality of the recovered secret image.

(2) The quality of the reconstructed image is consistent with theoretical estimates.

(3) When the numbers of shares involved in reconstruction are the same, the greater the sum of the weights is, the better the reconstructed image's quality is. When the sums of the weights of the shares are the same, the more shares involved in the reconstruction are, the better the quality of the

reconstructed image is. When the number and weights sum of shares involved in the reconstruction are the same, the reconstructed image's quality is judged according to the identical pixels in two images.

4.3. Comparison with Other Weighted SIS Schemes. In this subsection, we compare our scheme with other weighted SIS schemes from several relevant features. Figure 5 shows Tan's $(2, 4)$-threshold scheme based on the CRT with $(p, m_1, m_2, m_3, m_4) = (131, 247, 249, 251, 253)$. The weights of shares are also $W = [0.1, 0.2, 0.3, 0.4]$. Figure 5(a) shows the secret image Lena with the size of 256×256. Figures 5(b) ~ 5(e) are four shares. Figures 5(f) ~ 5(p) are reconstructed secret images by collecting different shares, in which Figure 5(p) is lossless by collecting all shares. Each share has a weight in both our scheme and Tan's scheme, and the reconstructed secret image can be recovered in a lossless way.

From Table 1, we can find that the theoretical values are the same between our scheme and Tan's scheme. And our experimental values are similar to those of Tan's scheme, which are consistent with the theoretical values. This is because the same method is used to give weight to each share in our scheme and Tan's scheme. The obvious difference between the two schemes is the average light transmission of shares as shown in Figure 6. There is no obvious difference for the average light transmission of four shares in our scheme. For the remaining $n - k$ shares, we fill with invalid value 0 or 255 randomly. However, the average light transmissions of four shares in Tan's scheme are different. In their scheme, the remaining $n - k$ shares are filled with the corresponding privacy modulus. As the weight increases, the shadow image gets darker. Obviously, this phenomenon will leak out the importance of shadow images and reduce the security of the weighted scheme to some extent.

In general, SIS schemes have many features. Table 3 shows the main characteristics and comparisons of our scheme with related weighted schemes. All schemes listed are weighted schemes. Liu et al.'s, Tan et al.'s, and our schemes with (k, n)-threshold are more flexible than $(2, n)$-threshold of Hou et al. and Yang et al. Image format, lossless recovery, and additional information are related to the sharing method. Compared to the methods based on VSS and the CRT, our polynomial-based scheme has many advantages, such as less computation, less additional information, and lossless recovery. Meanwhile, compared with Tan's scheme, we overcome the problem that the average light transmissions of shares are not identical.

5. Conclusion

In this paper, a weighted SIS scheme with lossless recovery is proposed. Each share has a weight. The larger the weight is, the greater the influence on the reconstructed image's quality is, when it participates in the recovery. When the threshold of secret image recovery is satisfied, the number and weight of share can affect the reconstructed image's quality. When all shares are involved in the reconstruction, the reconstructed image can be lossless. And we overcome the problem that the average light transmissions of shares are not identical. Theoretical analysis and experimental results show the effectiveness of the scheme. In future work, we will extend our weighted SIS scheme for color images and study the polynomial-based SIS scheme in the field of $GF(2^8)$.

Data Availability

Some or all data, models, or code generated or used during the study are available from the corresponding (chenjia9624@nudt.edu.cn) author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (number: 61602491). The authors are thankful to the reviewers for their valuable comments and suggestions to improve the manuscript.

References

[1] L. Li, A. A. A. El-Latif, Z. Shi, and X. Niu, "A new loss-tolerant image encryption scheme based on secret sharing and two chaotic systems," *Research Journal of Applied Ences, Engineering and Technology*, vol. 4, no. 8, pp. 877–883, 2012.

[2] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on ISB matching revisited," *IEEE Trans Inform Forensics Secure*, vol. 5, no. 2, pp. 201–214, 2010.

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

[6] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference*, vol. 48, June 1979.

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

[8] X. Yan, S. Wang, and X. Niu, "Threshold construction from specific cases in visual cryptography without the pixel expansion," *Signal Processing*, vol. 105, pp. 389–398, 2014.

[9] X. Yan, S. Wang, A. A. A. El-Latif, X. Niu, and Z. Wei, "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.

[10] 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, no. 1, pp. 61–73, 2018.

[11] X. Wu, T. Liu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing via error diffusion,"

Journal of Visual Communication and Image Representation, vol. 24, no. 5, pp. 552–566, 2013.

[12] X. Yan, S. Wang, A. A. A. El-Latif, X. Niu, and Z. Wei, "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.

[13] S. Shyu Jian, "Visual cryptograms of random grids for general access structures," *Theoretical Computer Science*, vol. 565, pp. 30–49, 2015.

[14] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 1–20, 2017.

[15] 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. 193, p. 1, 2020.

[16] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 307–322, 2011.

[17] X. Wu and W. Sun, "Extended capabilities for XOR-based visual cryptography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1592–1605, 2017.

[18] A. A. A. El-Latif, X. Yan, L. Li, N. Wang, J. 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.

[19] M. Mignotte, "How to share a secret," *Eurocrypt*, vol. 149, no. 4, pp. 371–375, 1982.

[20] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[21] W. Yan and Q. Dongxu, "Image sharing based on Chinese remainder theorem," *Journal of North China University of Technology*, vol. 12, no. 1, pp. 6–9, 2000.

[22] X. Yan, Y. Lu, L. Liu, S. Wan, and H. Liu, "Chinese remainder theorem-based secret image sharing for (k, n) threshold," in *Proceedings of the International Conference on Cloud Computing and Security*, November 2017.

[23] L. Tan, Y. Lu, X. Yan, L. Liu, and L. Li, "Weighted secret image sharing for a (k, n) threshold based on the Chinese remainder theorem," *IEEE Access*, no. 99, p. 1, 2019.

[24] L. Li, Y. Lu, X. Yan, L. Liu, and L. Tan, "Lossless (k, n)-threshold image secret sharing based on the Chinese remainder theorem without auxiliary encryption," *IEEE Access*, vol. 7, pp. 75113–75121, 2019.

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

[26] 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.

[27] P. Li, Z. Liu, and C. N. Yang, "A construction method of (t, k, n) -essential secret image sharing scheme," *Signal Processing Image Communication*, vol. 65, pp. 210–220, 2018.

[28] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3848–3858, 2020.

[29] Y. C. Hou, Z. Y. Quan, and C. F. Tsai, *A Privilege-Based Visual Secret Sharing Model*, Academic Press, Inc., Cambridge, USA, 2015.

[30] C.-N. Yang, J.-K. Liao, and D.-S. Wang, "New privilege-based visual cryptography with arbitrary privilege levels," *Journal of Visual Communication and Image Representation*, vol. 42, pp. 121–131, 2017.

[31] F. Liu, X. Yan, X. Yan, L. Liu, Y. Lu, and L. Tan, "Weighted visual secret sharing with multiple decryptions and lossless recovery," *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 5750–5764, 2019.

[32] L. Liu, Y. Lu, X. Yan, and H. Wang, "Greyscale-images-oriented progressive secret sharing based on the linear congruence equation," *Multimedia Tools and Applications*, vol. 77, 2017.