mathematics

Article

Practical Secret Image Sharing Based on the Chinese Remainder Theorem

Longlong Li [1,2], Yuliang Lu [1,2,*], Lintao Liu [1,2], Yuyuan Sun [1,2] and Jiayu Wang [1,2]

[1] College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China; lilongs@nudt.edu.cn (L.L.); lintao89@nudt.edu.cn (L.L.); sun_yuyuan@nudt.edu.cn (Y.S.); wangjiayu@nudt.edu.cn (J.W.)
[2] Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China
* Correspondence: luyuliang@nudt.edu.cn

Abstract: Compared with Shamir's original secret image sharing (SIS), the Chinese-remainder-theorem-based SIS (CRTSIS) generally has the advantages of a lower computation complexity, lossless recovery and no auxiliary encryption. However, general CRTSIS is neither perfect nor ideal, resulting in a narrower range of share pixels than that of secret pixels. In this paper, we propose a practical and lossless CRTSIS based on Asmuth and Bloom's threshold algorithm. To adapt the original scheme for grayscale images, our scheme shares the high seven bits of each pixel and utilizes the least significant bit (LSB) matching technique to embed the LSBs into the random integer that is generated in the sharing phase. The chosen moduli are all greater than 255 and the share pixels are in the range of [0, 255] by a screening operation. The generated share pixel values are evenly distributed in the range of [0, 255] and the selection of (k, n) threshold is much more flexible, which significantly improves the practicality of CRTSIS. Since color images in RGB mode are made up of three channels, it is easy to extend the scheme to color images. Theoretical analysis and experiments are given to validate the effectiveness of the proposed scheme.

Keywords: secret image sharing; Chinese remainder theorem; (k, n) threshold; practical; lossless

MSC: 94A64

Citation: Li, L.; Lu, Y.; Liu, L.; Sun, Y.; Wang, J. Practical Secret Image Sharing Based on the Chinese Remainder Theorem. *Mathematics* **2022**, *10*, 1959. https://doi.org/10.3390/math10121959

Academic Editor: Antanas Cenys

Received: 5 May 2022
Accepted: 5 June 2022
Published: 7 June 2022

1. Introduction

The transmission of sensitive images such as military images, confidential images, private photos, etc., over insecure communication channels causes a challenging issue. Transmitting a single image may suffer from a single point of failure (SPOF) if the communication channel is blocked; transmitting multiple copies increases the danger of secret leakage. Secret image sharing (SIS) can be a solution. A (k, n) threshold secret image sharing (SIS) scheme was proposed to divide a secret image into n shares, known as shadow images or shadows. Fewer than k shares reveal no clue about the secret image; having at least k shares makes it easy to compute the secret image. Therefore, even with at most $n - k$ shares lost, the secret image can still be recovered; this is the so-called loss-tolerant property. SIS has widely been applied to many fields, such as key distribution [1], access control [2], identity authentication [3,4], watermarking [5], blockchain [6], cloud distributive storage [7,8] and others [9]. The basic SIS schemes chiefly includes visual cryptography (VC) [10,11], polynomial-based SIS [12] and the Chinese-remainder-theorem-based SIS [13,14].

VC, also called visual secret sharing (VSS), requires low computation in the recovery phase. In (k, n)-threshold VC [15,16], a binary secret is divided into n binary shares. If the generated shares are printed on transparent materials, the secret image can be recovered by superposing any k or more shares. Therefore, the computational equipment's absence fixes the problem of transmitting top secrets that cannot be stored digitally. However, the random interference introduced in the sharing phase makes it impossible to recover the

secret without loss by superposing. The increase of participants also significantly reduces the quality of the recovered secret image, which limits the threshold k and participants n. According to the different basic mechanisms, existing schemes may have the flaws of pixel expansion, auxiliary codebook and low image quality, which have been studied in some works [17–22].

A polynomial-based secret-sharing algorithm was first propose by Shamir in 1979 [12]. The scheme constructs a $k-1$ degree polynomial with $k-1$ random coefficients and one constant as the secret to generate n shares. Gathering any k or more shares makes it possible to reconstruct the polynomial by Lagrange interpolation. Thien and Lin [23] applied the polynomial-based secret-sharing algorithm to images. They used every coefficient to embed the secret image pixel so that the size of shares decreases to $1/k$ of the secret image. However, auxiliary encryption was required in their scheme to prevent secret leakage. Then, some works were proposed to extend the field in the following aspects: multiple decoding options, lossless recovery, weighted shares and so on [24–27]. Nevertheless, some challenges in the polynomial-based SIS still exist, including auxiliary encryption, lossy recovery and high computation complexity. Auxiliary encryption is used to eliminate the correlation of image pixels, which leads to the leakage of secrets. Since the prime number chosen to form the field is 251 and grayscale image pixels range from 0 to 255, five pixel values are unable to be calculated. Thus, in general, there is a little loss. Moreover, the computation complexity is proven to be $O(k \log^2 k)$ [13], which is a high cost to SIS.

The Chinese-remainder-theorem-based secret sharing (CRTSS) was proposed in 1983 by Asmuth and Bloom [13] and Mignotte [14], respectively. Compared with Mignotte's algorithm, Asmuth and Bloom's algorithm utilized a large random integer to confuse the secret, bringing more security against attacks. The computation complexity of the scheme was only $O(k)$. Yan et al. [28] firstly introduced the CRT into SIS in 2000, but with some information leakage and a lossy recovery. Shyu et al. [29] proposed a CRTSIS based on Mignotte's scheme and used a pseudorandom noise generation (PRNG) algorithm to scramble the correlation of the pixels. In the work of Ulutas et al. [30], Asmuth and Bloom's algorithm was the base and the distinctive modification was dividing the pixels into two intervals. Since they did not give precise parameters in their work, there may be some problems in some conditions. For example, the (k, n) threshold cannot be achieved if the random number is too small. Hu et al. [31] used the chaotic map in the CRTSIS, which means auxiliary encryption was involved. Chuang et al. [32] proposed a CRTSIS to share the most significant seven bits to satisfy the restrictions of Asmuth and Bloom's algorithm. They stored and transmitted the least significant bit (LSB) independently or just threw it away. Therefore, their scheme has the drawback of extra transmission cost or lossy recovery. Yan et al. [33,34] divided the grayscale pixels into two intervals, which corresponded to different ranges of the random integer. Li et al. [35] shared the high seven bits of the grayscale image pixels and embedded the LSB into the random integer. Both Yan et al.'s scheme and Li et al.'s scheme achieved the (k, n) threshold with lossless recovery and provided applicable explicit parameters for the implementation. However, when n in their schemes is big, it is difficult to find the coprime integers as the moduli, and the pixel values have a bad distribution. As a result, they suggested n be no more than six.

In general, the CRTSIS based on Asmuth and Bloom's algorithm is neither perfect nor ideal, which has been proven in some works [36,37]. The size of the share space is smaller than that of the secret space. In Asmuth and Bloom's algorithm, the share ranges from 0 to $m_i - 1$, where m_i is the corresponding modulus. Furthermore, the secret ranges from 0 to $p - 1$, where p is an integer with $(p, m_i) = 1$ for all i. The limitation of the share pixel range creates obstacles to the application of CRTSIS. On the one hand, the (k, n) threshold determines the number of participants, so CRTSIS is not applicable in scenarios that require many participants. On the other hand, since the pixels ranging in $[m_i, 255]$ cannot be generated, achieving some functions based on the CRTSIS such as meaningful shares, multisecret and share authentication may suffer from a smaller screening space than PSIS. Therefore, it is of great importance to improve CRTSIS to fit more application scenarios.

This paper aims to solve the problem of loss recovery and limited threshold when Asmuth and Bloom's algorithm is applied to image sharing and provide a more practical scheme for secret image sharing based on the Chinese remainder theorem. Considering the features of grayscale images, we take the high seven bits as the shared secret and embed the LSB into the random integer that is generated in the sharing phase of Asmuth and Bloom's algorithm by LSB matching [38]. In order to eliminate the restriction of shared pixel values, moduli are creatively chosen slightly bigger than 255, and a filter is used to avoid the abnormal share pixels. The advantage is that number of participants can be larger than that in the schemes of Yan et al. [33] and Li et al. [35]. For color images, the RGB channels can be split and shared, respectively. Then, we can merge the corresponding RGB shares into color shares.

The contributions are summarized as follows.

(1) A (k, n)-threshold CRTSIS scheme with lossless recovery and no auxiliary encryption is proposed, which generates shares with the same pixel space ranging from 0 to 255, so that the limitation of the threshold can be released.
(2) Concrete parameters are provided in the paper. We traverse all the integers that meet the conditions and screen out the optimal ones, with which users can achieve a sharing process among as many as 10 participants.
(3) To evaluate the effectiveness of the proposed scheme, both theoretical analysis and experiments are carried out. Furthermore, comparisons with other remarkable works are given to indicate our advantages.

The paper hypothesizes that the proposed scheme is a valid lossless secret image sharing scheme with good practicability.

The rest of the paper is organized as follows. Section 2 gives some basic knowledge, presents the detailed scheme and a security analysis. Section 3 shows the experimental results of the proposed scheme and discussion. In Section 4, we conclude the paper.

2. Materials and Methods

This section provides some important ground knowledge and the detailed scheme.

2.1. Preliminaries

Some basic knowledge for our work is given in this section, including the Chinese remainder theorem and Asmuth and Bloom's Algorithm.

For (k, n)-threshold SIS, the secret image S is divided into n shares $SC_1, SC_2, \cdots, SC_n$, which are distributed to n participants. When t ($k \leq t \leq n, t \in Z^+$) shares are gathered, the secret image S' can be recovered.

2.1.1. Chinese Remainder Theorem (CRT)

The CRT is used to solve a set of linear congruence equations. The number can be determined with a set of coprime integers $m_i (i = 1, 2, \cdots, k)$ and their corresponding remainders, shown as below.

$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) (\text{mod } M), y \in [0, M-1]$ subject to

$$\begin{aligned} y &\equiv a_1 (\text{mod } m_1) \\ y &\equiv a_2 (\text{mod } m_2) \\ &\cdots \\ y &\equiv a_{k-1} (\text{mod } m_{k-1}) \\ y &\equiv a_k (\text{mod } m_k) \end{aligned} \tag{1}$$

where $\gcd(m_i, m_j) = 1, i \neq j$, $M = \prod_{i=1}^{k} m_i$, $M_i = {}^{M}/_{m_i}$ and $M_i M_i^{-1} \equiv 1 (\text{mod } m_i)$.

It is worth noting that there is one and only one solution in $[0, M-1]$ with all the k linear congruence equations, which is the inherent characteristic of the CRT. Assuming

only $k-1$ equations are available and a_j is missing, y_0 is calculated as the only solution in $[0, \prod_{i=1,i\neq j}^{k} m_i - 1]$. However, for $b = 1, 2, \cdots, m_j - 1$, $y_0 + b\prod_{i=1,i\neq j}^{k} m_i$ are also the solutions in $[0, M-1]$, which correspond to every possible a_k in $[0, m_j - 1]$. Therefore, even with $k-1$ equations, we still get nothing about the exact solution y for all the k equations, which achieves the secure condition for a (k, n) threshold in the proposed scheme.

2.1.2. Asmuth and Bloom's Algorithm

In 1983, Asmuth and Bloom proposed a secret sharing algorithm based on the CRT, shown in Algorithm 1, achieving a (k, n) threshold and $O(k)$ operations for recovery.

Algorithm 1: Asmuth and Bloom's CRT-based secret sharing algorithm.

Input: A nonnegative integer s as the secret and (k, n) as the threshold.
Output: n shares $sc_1, sc_2, \cdots sc_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$.
Step 1: A set of integers $\{s < p < m_1 < m_2 \cdots < m_n\}$ is selected to satisfy the following:

1. $\gcd(m_i, m_j) = 1, i \neq j$.
2. $\gcd(m_i, p) = 1$ for $i = 1, 2, \cdots, n$.
3. $M > pN$

where $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$ and p will be informed to all the participants.
Step 2: Randomly generate an integer A in $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ by a PRNG and let $y = s + Ap$.
Step 3: Calculate $a_i \equiv y (\mathrm{mod}\ m_i)$ and let $sc_i = a_i$ for $i = 1, 2, \cdots, n$.
Step 4: Output n shares $sc_1, sc_2, \cdots sc_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots m_n$.

We note that Asmuth and Bloom's algorithm maps the secret number s into a much big number y, and at the same time, introduces randomness to enhance the security. The obstacle to applying the scheme to images is the inconsistency between the space of secret and shares. Pixel values are in $[0, 255]$ for grayscale images, which means $0 \leq a_i \leq 255$ and $0 \leq s \leq 255$. According to the statement in Step 1, we get $\{s < p < m_1 < m_2 \cdots < m_n \leq 255\}$. Therefore, secret pixels cannot be entirely shared, leading to lossy recovery. Furthermore, the loss becomes more severe with the increase of n.

2.2. The Proposed CRTSIS Scheme

In this section, we present the basic design of our scheme, which is based on Asmuth and Bloom's algorithm. Creative modifications are applied to solve the problem of loss recovery as well as the inconsistency between the space of secret and shares.

The scenario is described as follows. A dealer firstly divides the original grayscale secret image S into n shares, namely $SC_1, SC_2, \cdots SC_n$. Then, the shares and their corresponding private modulus $m_1, m_2, \cdots m_n$ are sent to n different participants. When at least k shares are gathered, the secret image S' is able to be recovered. The order of the shares in the recovery phase is arbitrary as long as it corresponds to the order of the moduli.

To maintain lossless recovery, we take out the high 7 bits of the grayscale pixels as the secret ($[0, 127]$) and embed the LSB into the random integer A. It is important to note that the moduli in our scheme are greater than 255. The screening operation is applied to eliminate invalid shared values. So the size of the secret image space and the shares are the same. First, we list the variables in Table 1. The design concept is shown in Figure 1. The generation steps and the recovery steps are described in Algorithms 2 and 3.

Table 1. Variables used in Algorithms 2 and 3.

Variable	Meaning
$H \times W$	Size of a image
k	Threshold for recovering the secret image
n	Number of the participants/number of all shares
SC_i	ith generated shares
m_i	Modulus corresponding to i-th share
p	Integer defined in Asmuth and Bloom's Algorithm
A	Random integer selected to confuse the secret
M	$\prod_{i=1}^{k} m_i$
N	$\prod_{i=1}^{k-1} m_{n-i+1}$
r	Number of gathered shares
$S(h,w)$	Secret pixel at the position of (h,w)

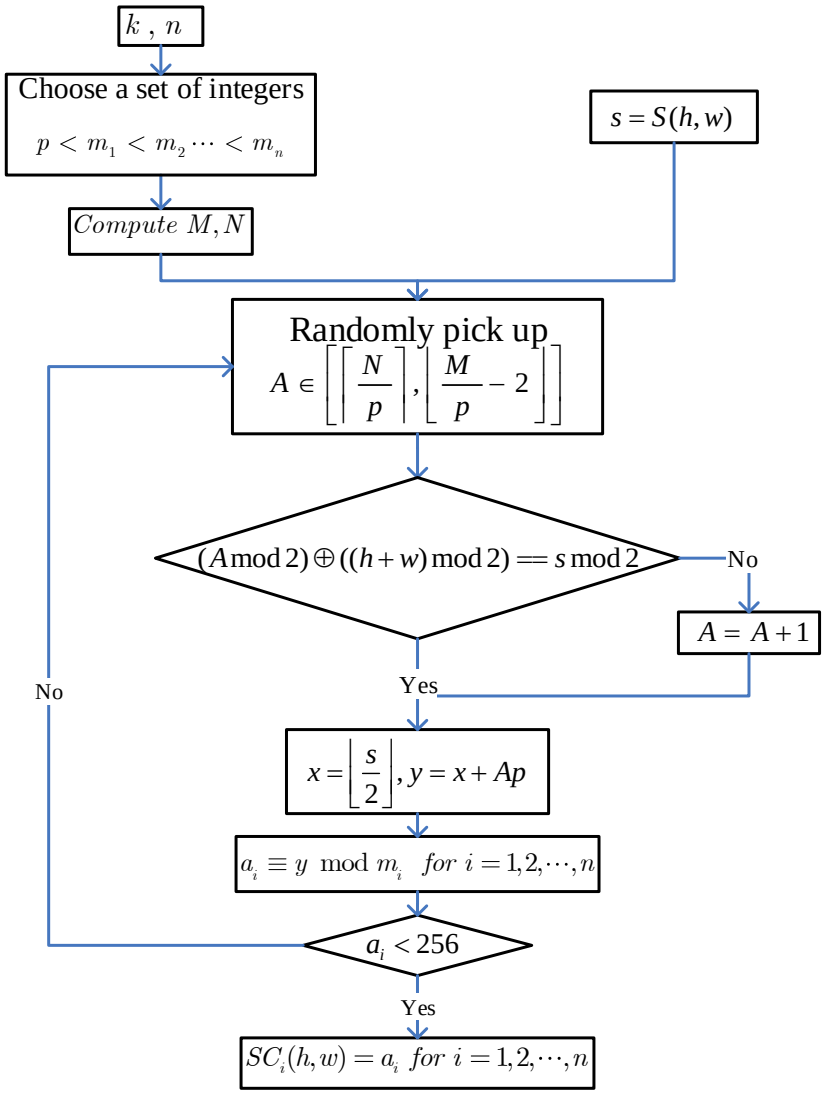


Figure 1. Design concept for the proposed scheme.

Algorithm 2: The sharing phase of the proposed scheme.

Input: An $H \times W$ secret image S and threshold parameters (k, n)
Output: n shares $SC_1, SC_2, \cdots SC_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$.
Step 1: A set of integers $\{128 \leq p < 256 \leq m_1 < m_2 \cdots < m_n\}$ is selected to satisfy the following:
1. $\gcd(m_i, m_j) = 1, i \neq j$.
2. $\gcd(m_i, p) = 1$ for $i = 1, 2, \cdots, n$.
3. $M > pN$

where $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$ and p will be informed to all the participants.
For every pixel position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, let $s = S(h, w)$. Repeat Steps 2–4.
Step 2: Randomly generate an integer A in $\left[\left\lceil \frac{N}{p} + 1 \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$.
If $(A \bmod 2) \oplus ((h + w) \bmod 2) == s \bmod 2$, keep A unchanged; otherwise A randomly adds or subtracts 1.
Step 3: Calculate $x = \lfloor s/2 \rfloor$, which means taking out the high 7 bits of the pixel. Let $y = x + Ap$.
Step 4: Calculate $a_i \equiv y (\bmod\ m_i)$. If $a_i < 256$, it is valid and assign it to $SC_i(h, w)$ for $i = 1, 2, \cdots, n$; otherwise throw it away and go back to Step 2, randomly generating another integer A for s.
Step 5: After all secret pixels have been traversed, output n shared images $SC_1, SC_2, \cdots SC_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots m_n$.

Algorithm 3: The recovery phase of the proposed scheme.

Input: Gathered r shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_r} (k \leq r \leq n)$ with the same size of $H \times W$, their corresponding privacy modular integers $m_{i_1}, m_{i_2}, \cdots m_{i_r}$ and p.
Output: A recovered secret image S'.
Step 1: For every position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2–3.
Step 2: Let $a_{i_j} = SC_{i_j}(h, w)$ for $j = 1, 2, \cdots, r$ and get the following linear equations.

$$\begin{aligned} y &\equiv a_{i_1} (\bmod\ m_{i_1}) \\ y &\equiv a_{i_2} (\bmod\ m_{i_2}) \\ &\cdots \\ y &\equiv a_{i_{r-1}} (\bmod\ m_{i_{r-1}}) \\ y &\equiv a_{i_r} (\bmod\ m_{i_r}) \end{aligned} \tag{2}$$

Step 3: Calculate $A = \left\lfloor \frac{y}{p} \right\rfloor$. Let $x = y \bmod p$.
$s' = x \times 2 + (A \bmod 2) \oplus ((h + w) \bmod 2)$. Assign s' to $S'(h, w)$.
Step 4: After all positions have been traversed, output the recovered secret image S'.

For Algorithm 2, we give the following notes.

1. In Step 1, the constraint $\{128 \leq p < 256 \leq m_1 < m_2 \cdots < m_n\}$ is obtained through the pixel range in grayscale images and $M > pN$. Since the shared value x is in $[0, 127]$, 128 exactly covers the secret value and 131 is the smallest prime that meets the conditions, we suggest p as 128 or 131.
2. In Step 2, the random A is chosen in $\left[\left\lceil \frac{N}{p} + 1 \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$ so as to achieve the (k, n) threshold, which is going to be proven later. The lower bound and upper bound are slightly modified to ensure the security in case of the adjustment of A at bound.
3. In Step 2, we associate a pixel's position with the modification of A, so that every s can be shared using a full range of A, instead of odd s always corresponding to odd A and even s corresponding to even A. The modification of A applies LSB matching, which has better performance than the basic LSB information hiding method. LSB matching is a simple improvement on LSB substitution. If the embedded bit is the same as the lowest bit of the carrier, it is not modified, and if it is different, it randomly increases or decreases by 1.

4. In Step 3, A is randomly generated by a PRNG for every x and multiplied by p plus the secret x to form a big integer y. Therefore, the secret space is greatly enlarged to scramble the pixel values, and the correlations between adjacent pixels are broken without auxiliary encryption due to the introduction of the nonlinear operation, namely the PRNG.
5. In Step 3, we take out the high 7 bits of the grayscale pixels as the secret ($[0, 127]$) and embed the LSB into the random integer A. As a result, lossless recovery is achieved.
6. In Step 4, the screening operation is applied. The rate of valid shared pixel values is $\frac{256}{m_1} \times \frac{256}{m_2} \times \cdots \times \frac{256}{m_n}$, which is equal to $\frac{256^n}{M}$. Therefore, we suggest m_i be as small as possible to reduce the generated invalid pixel values.

For Algorithm 3, we also give some notes.

1. To recover the secret image, a dealer or a participant group must gather at least k shares and their corresponding privacy modular integers, while p is public for all the participants.
2. In Step 2, the order of shares is arbitrary as long as every share matches the right modulus. Moreover, there can be more than k congruence equations to work out the right y.
3. The recovery process is based on CRT and the computation complexity is still $O(n)$.

2.3. Security Analyses

This subsection theoretically analyses the security of the proposed scheme.

Lemma 1. *Nothing about the secret image can be obtained from a single share generated by our scheme.*

Proof. The sufficient and necessary condition is that $SC_i(h, w) = a_i$ is random in $[0, m_i - 1]$ for every possible secret pixel, which can be proven from $y = x + Ap$ and $y \equiv a_i (\mathrm{mod}\ m_i)$.

For a fixed secret pixel s, we share its high 7 bits, namely x in $[0, 127]$. Since $\gcd(m_i, p) = 1$ and every x needs two values of A to embed the LSB, $Ap (\mathrm{mod}\ m_i)$ can generate all the integers in $[0, m_i - 1]$ as long as there exist a continuous interval of A with the least size $2m_i$. As we all know, A ranges in $\left[\left\lceil \frac{N}{p} + 1 \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$, so the continuous interval space of A, denoted as $|A|$, is

$$|A| = \left| \frac{M}{p} - 2 \right| - \left\lceil \frac{N}{p} + 1 \right\rceil > \frac{M - N}{p} - 5 \tag{3}$$

When $k \geq 3$, considering $M > pN$, we get $|A| \geq \frac{p-1}{p} N - 5$, which has a minimum at $k = 3$. Thus, $|A| \geq \frac{p-1}{p} m_{n-1} m_n - 5$. Because of the constraint $\{128 \leq p < 256 \leq m_1 < m_2 \cdots < m_n\}$, it is obvious that $|A|$ is much greater than $2m_i$. Therefore, $Ap (\mathrm{mod}\ m_i)$ can generate all the integers in $[0, m_i - 1]$ for $k \geq 3$. Furthermore, with the increase of A, $x + Ap$ obviously has the same characteristic. Therefore, we come to the conclusion that a_i is random in $[0, m_i - 1]$ for the randomness of A.

When $k = 2$, we find $|A| \approx \frac{m_1 m_2 - m_n}{p} - 5 \approx \frac{m_1 m_2}{p} - 7$. In practice, we suggest p as 128 or 131 and m_i as close to 256 as possible, so $|A|$ is close to but slightly smaller than $2m_i$, which means some values in $[0, m_i - 1]$ may not be reached while other values still have the randomness to be generated.

In general, when $k = 2$, although the generated share pixels cannot cover all the values in $[0, 255]$, the secret image still cannot be revealed from a single share. When $k \geq 3$, the shared pixels are evenly distributed in $[0, 255]$, so no clue about the secret image can be obtained. □

Lemma 2. *Any $k - 1$ shares reveal nothing about the secret image.*

Proof. Supposing $k-1$ share pixels $a_{i_1}, a_{i_2}, \cdots a_{i_{k-1}}$ are given, according to the CRT, we get the solution y_1 mod N_1, where $N_1 = \prod_{j=1}^{k-1} m_{i_j}$. So $y_1 \in [0, N_1 - 1]$. Since $0 \leq < N_1 < y < M$, $M/N_1 > p$ and $\gcd(N_1, p) = 1$, we can construct other different solutions $y_1 + bN_1$ for $b = 1, 2, \cdots, m_{i_k} - 1$ in $[N_1, M-1]$, which indicates there are other $m_{i_k} - 1$ solutions in $[N_1, M-1]$ to the congruence equations of $k-1$ share pixels. Therefore, $k-1$ or less shares reveal nothing about the secret image. □

Lemma 3. *Any k or more shares are sufficient to recover the secret image losslessly.*

Proof. First, we prove that the shared x, the high 7 bits of a secret pixel, can be recovered without loss with any k or more shares. When $a_{i_1}, a_{i_2}, \cdots a_{i_r} (k \leq r \leq n)$ are given, according to the CRT, there exists only one solution y_2 in $[0, N_2]$, where $N_2 = \prod_{j=1}^{r} m_{i_j}$. Since $N_2 \geq M$, the exact solution y_0 is also in $[0, N_2]$, indicating y_1 and y_0 are the same, because if y_1 and y_0 are different, there are two solutions to the r congruence equations, which is inconsistent with the CRT. Therefore, with any k or more shares, the unique x can be determined by y modulo p. Then the secret pixel s' can be losslessly recovered with $s' = x \times 2 + (A \bmod 2) \oplus ((h + w) \bmod 2)$. □

According to the above lemmas, we have proved that our scheme is a valid (k, n)-threshold SIS.

3. Results and Discussion

In this section, we provide available parameters that allow as many as 10 participants to join in the sharing process and present the experiments and discussion to evaluate the proposed scheme.

3.1. Available Parameters

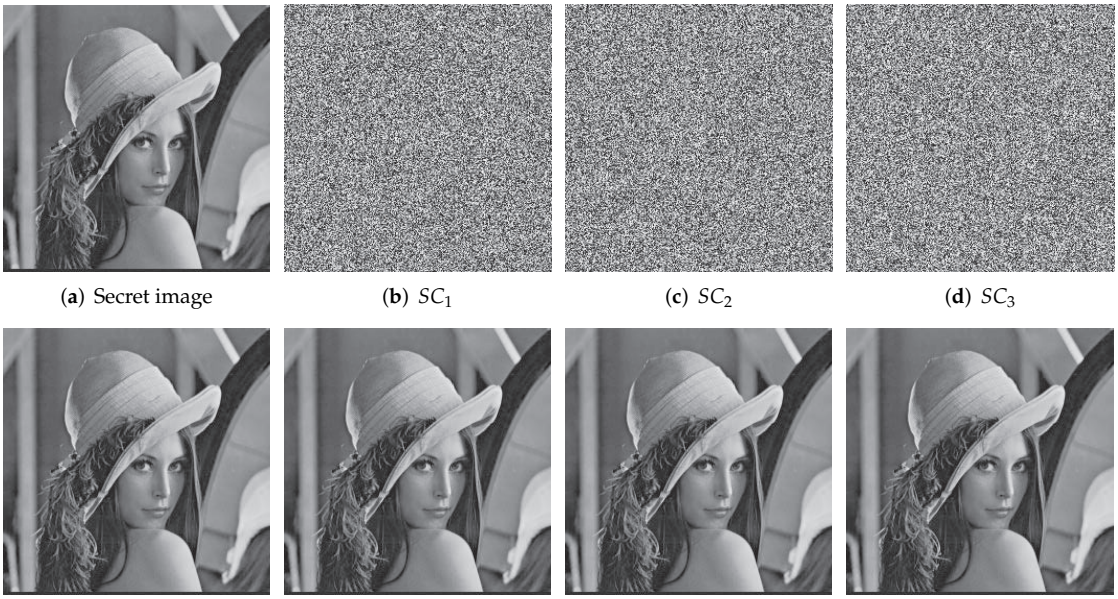
According to the suggestion given in Section 2.2, we traversed the integers in $[256, 512]$ and screened out the optimal parameters, shown in Table 2, which were used in the following experiments. Users can also search other parameters according to specific thresholds. For convenience, all the moduli can be chosen from prime numbers, while the screening cost in Step 4 of Algorithm 2 will increase dramatically.

Table 2. Available parameters of $m_1, m_2 \cdots, m_n$.

n	p	$m_1, m_2 \cdots, m_n$
2	128	257, 259
2	131	256, 257
3	128	257, 259, 261
3	131	256, 257, 259
4	128	257, 259, 261, 263
4	131	256, 257, 259, 261
5	128	257, 259, 261, 263, 265
5	131	256, 257, 259, 261, 263
6	128	257, 259, 261, 263, 265, 269
6	131	256, 257, 259, 261, 263, 265
7	128	257, 259, 261, 263, 265, 269, 271
7	131	256, 257, 259, 261, 263, 265, 269
8	128	257, 259, 261, 263, 265, 269, 271, 277
8	131	256, 257, 259, 261, 263, 265, 269, 271
9	128	257, 259, 261, 263, 265, 269, 271, 277, 281
9	131	256, 257, 259, 261, 263, 265, 269, 271, 277
10	128	257, 259, 261, 263, 265, 269, 271, 277, 281, 283
10	131	256, 257, 259, 261, 263, 265, 269, 271, 277, 281

3.2. Image Illustration

First, in Figure 2 we give the experimental results for the $(2,3)$ threshold, which is frequently used to test an SIS. The secret image is Lena, one of the most commonly used standard images, with a size of 512×512. p was chosen to show that it was applicable though p was not a prime. Figure 2b–d are the generated shares SC_1, SC_2 and SC_3, from which we cannot distinguish anything about the secret image. We used every combination of two or three shares to reconstruct the secret image shown in Figure 2e–h, where $CRT(SC_{1,2})$ denotes the recovery by shares SC_1 and SC_2. In addition, we have $\sum_{h=1}^{H}\sum_{w=1}^{W}|S(h,w) - S'(h,w)| = 0$, therefore the secret image can be losslessly recovered by CRT with sufficient shares.

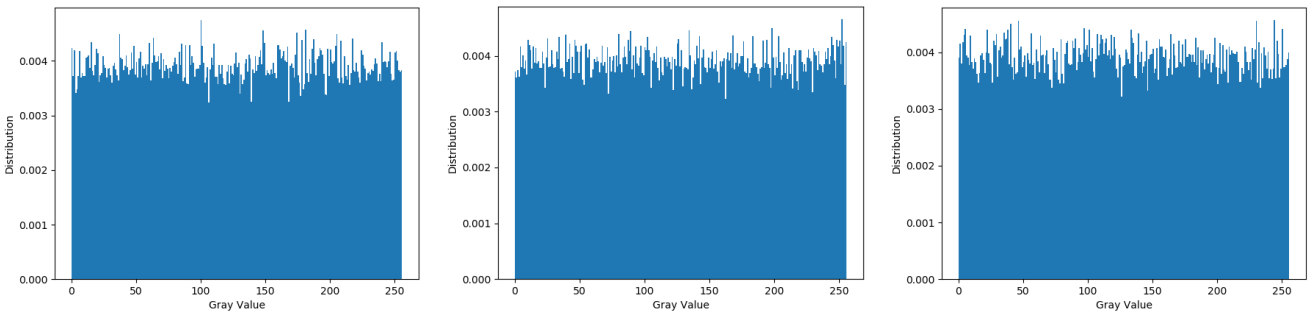


(**a**) Secret image (**b**) SC_1 (**c**) SC_2 (**d**) SC_3

(**e**) $CRT(SC_{1,2})$ (**f**) $CRT(SC_{1,3})$ (**g**) $CRT(SC_{2,3})$ (**h**) $CRT(SC_{1,2,3})$

Figure 2. Experimental results of the introduced scheme for the $(2,3)$ threshold. (**a**) Secret image; (**b**–**d**) three generated shares SC_1, SC_2 and SC_3; (**e**–**g**) recovered images with two shares; (**h**) recovered image with three shares.

Histograms of the shares in Figure 2 are shown in Figure 3. The pixel values in every shares are approximately evenly distributed in $[0, 255]$, which indicates that each share reveals nothing about the secret image.



(**a**) Hist of SC_1 (**b**) Hist of SC_2 (**c**) Hist of SC_3

Figure 3. Histograms of the shares in Figure 2.

Next, to prove the security with $k-1$ shares, we performed an experiment with a $(3,5)$ threshold, sharing the grayscale secret image shown in Figure 4, which has very distinguish-

able shapes and obvious edges and simple textures. Thus, a leakage of the secret image can be easily observed. Other parameters were chosen from Table 2, where $p = 128$ and the moduli were 257, 259, 261, 263 and 265. Five shares and recovered images with two or three shares are displayed in Figure 5, while their corresponding histograms are shown in Figure 6.

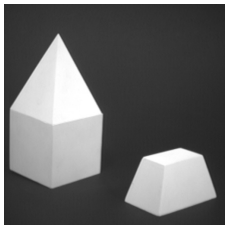
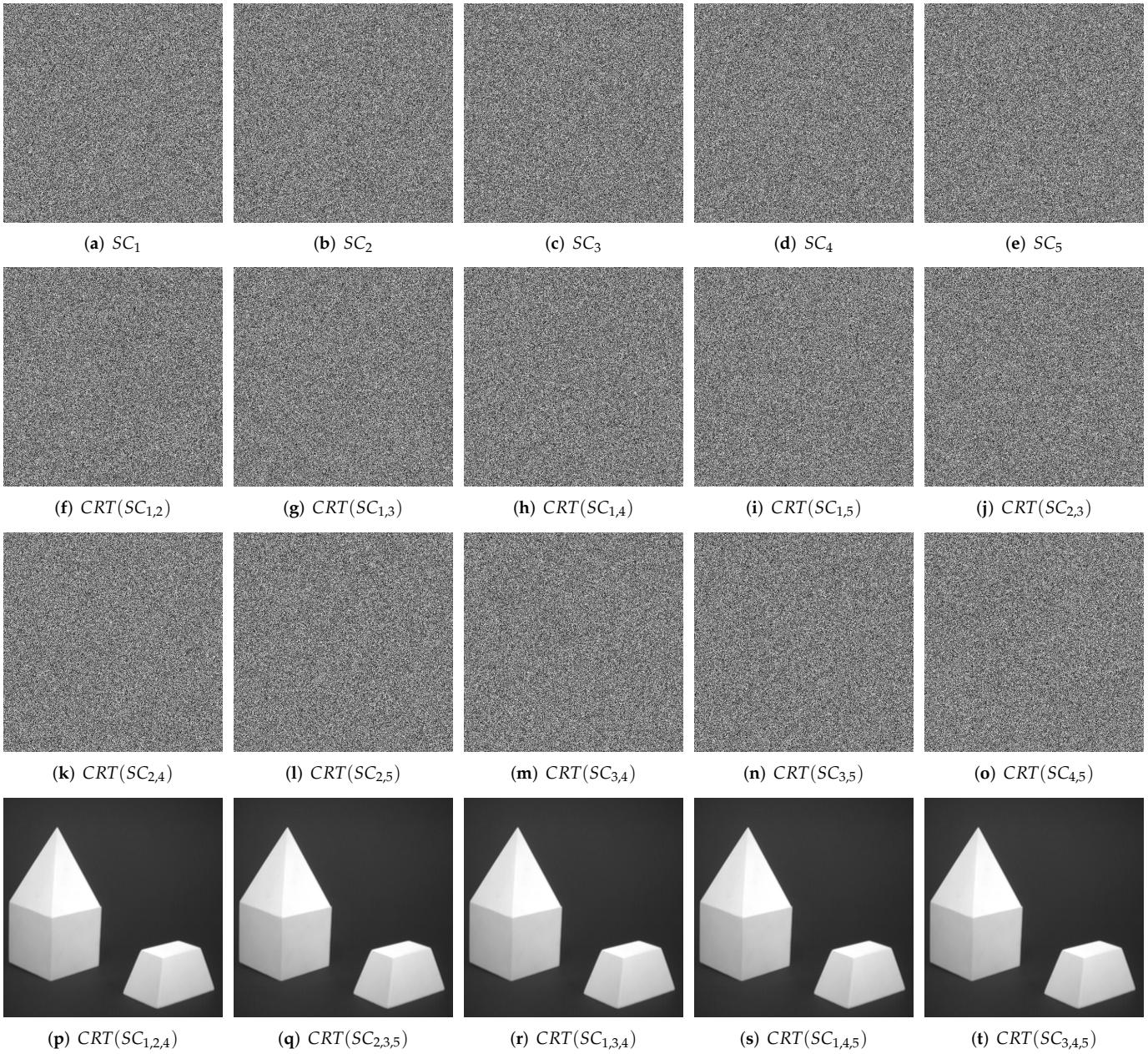


Figure 4. Grayscale secret image with a size of 512×512.



(**a**) SC_1 (**b**) SC_2 (**c**) SC_3 (**d**) SC_4 (**e**) SC_5

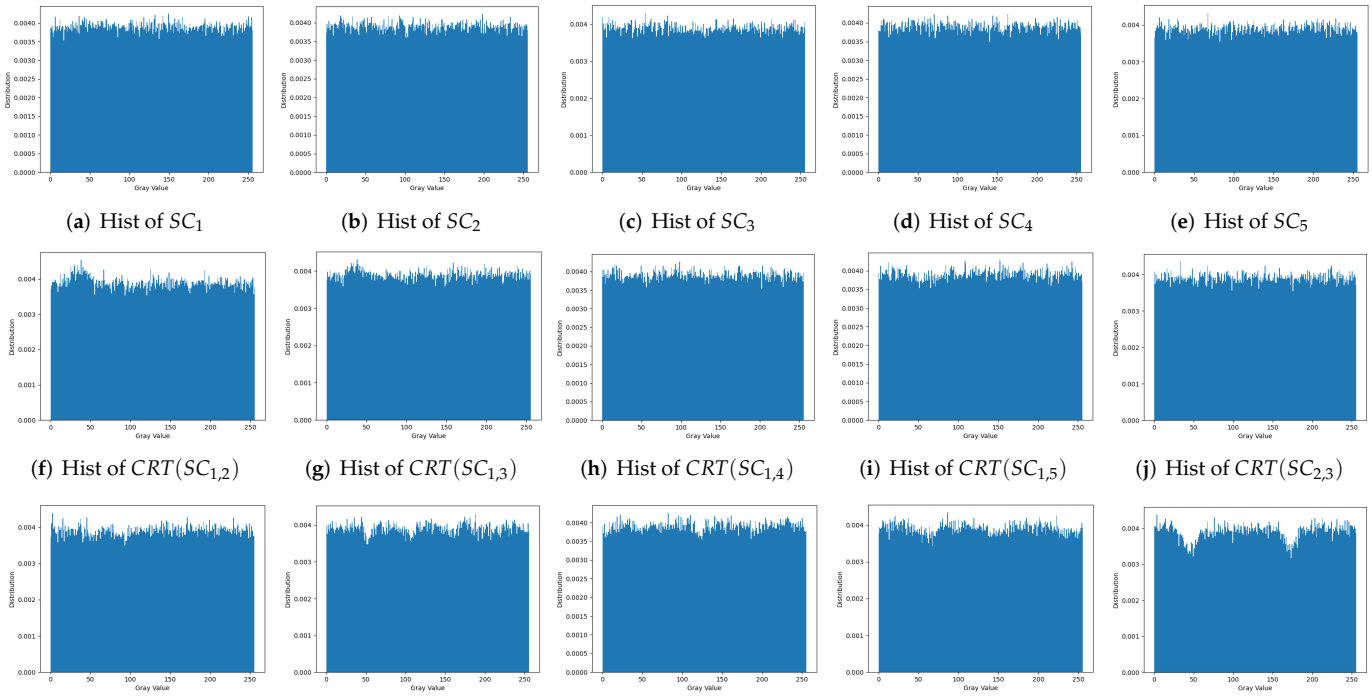
(**f**) $CRT(SC_{1,2})$ (**g**) $CRT(SC_{1,3})$ (**h**) $CRT(SC_{1,4})$ (**i**) $CRT(SC_{1,5})$ (**j**) $CRT(SC_{2,3})$

(**k**) $CRT(SC_{2,4})$ (**l**) $CRT(SC_{2,5})$ (**m**) $CRT(SC_{3,4})$ (**n**) $CRT(SC_{3,5})$ (**o**) $CRT(SC_{4,5})$

(**p**) $CRT(SC_{1,2,4})$ (**q**) $CRT(SC_{2,3,5})$ (**r**) $CRT(SC_{1,3,4})$ (**s**) $CRT(SC_{1,4,5})$ (**t**) $CRT(SC_{3,4,5})$

Figure 5. Experimental results of the introduced scheme for the $(3, 5)$ threshold. (**a**–**e**) Five generated shares SC_1, SC_2, SC_3, SC_4 and SC_5; (**f**–**o**) recovered images with two shares; (**p**–**t**) recovered images with three shares.

From the noise-like shares of Figure 5a–e, we cannot visually recognize anything about the secret image, and the corresponding histograms also show that pixels are evenly distributed in $[0, 255]$, which proves not a clue is leaked from the shares. When using two shares to recover the secret image by the CRT, we only get meaningless images, namely Figure 5f–o, whose histograms fully cover the range of $[0, 255]$, demonstrating the security of the proposed scheme with $k - 1$ shares. Figure 5p–t display the successfully recovered secret images that are exactly the same as the original image, Figure 4. Although we only show five of the ten recovered images for reason of space, it is sufficient to prove that the secret image can be losslessly recovered with any k shares.



(**a**) Hist of SC_1 (**b**) Hist of SC_2 (**c**) Hist of SC_3 (**d**) Hist of SC_4 (**e**) Hist of SC_5

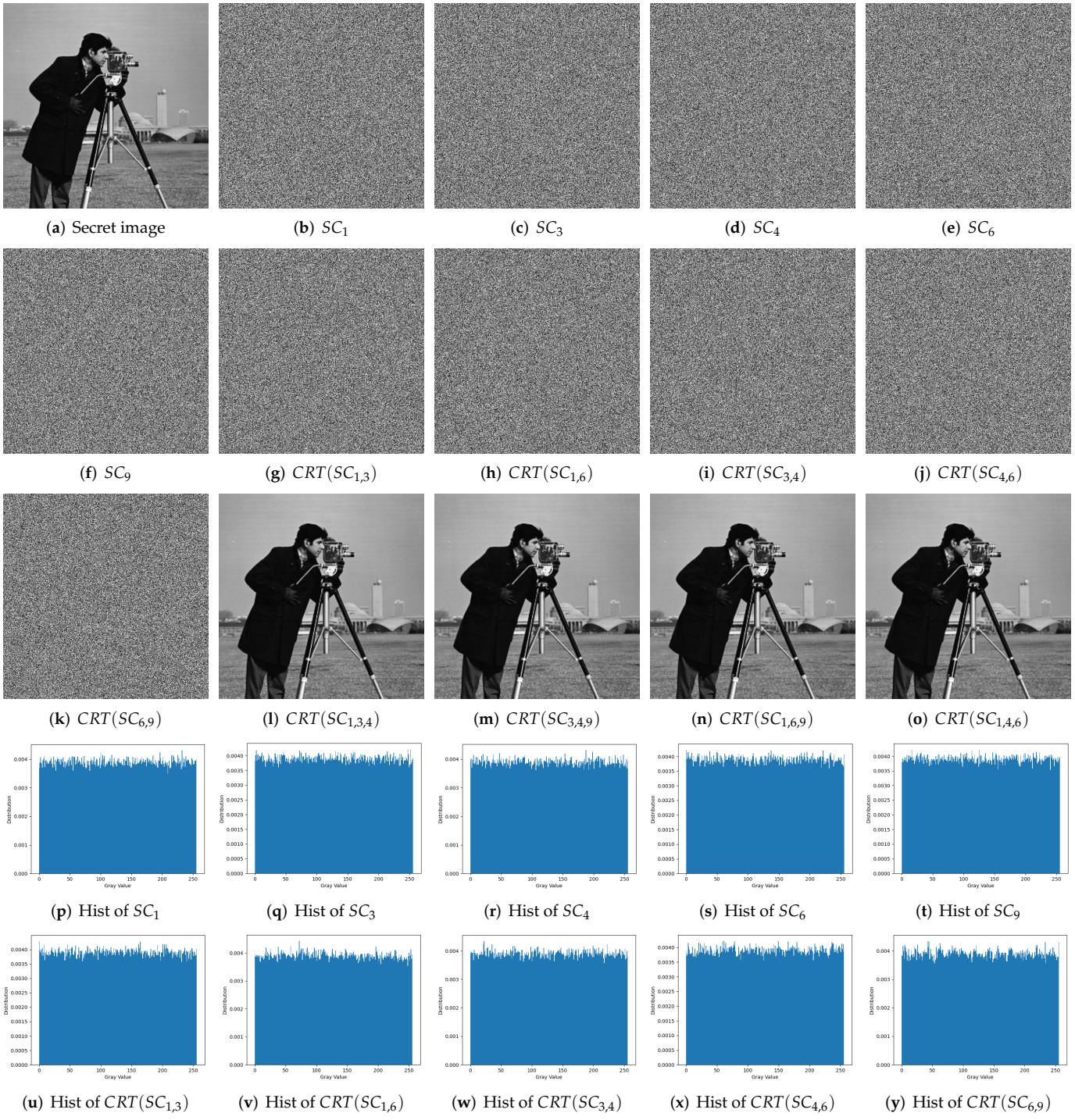
(**f**) Hist of $CRT(SC_{1,2})$ (**g**) Hist of $CRT(SC_{1,3})$ (**h**) Hist of $CRT(SC_{1,4})$ (**i**) Hist of $CRT(SC_{1,5})$ (**j**) Hist of $CRT(SC_{2,3})$

(**k**) Hist of $CRT(SC_{2,4})$ (**l**) Hist of $CRT(SC_{2,5})$ (**m**) Hist of $CRT(SC_{3,4})$ (**n**) Hist of $CRT(SC_{3,5})$ (**o**) Hist of $CRT(SC_{4,5})$

Figure 6. Histograms of the shares and recovered images with two shares in Figure 5.

Our scheme also has good performance when n is much bigger than k. We performed an experiment where $k = 3, n = 10$ and $p = 128$, and m_i was selected from the parameter table given in Table 2. We chose five shares to show the effectiveness, including SC_1, SC_3, SC_4, SC_6 and SC_9, shown in Figure 7b–f. With two shares, we only got noise-like images as in Figure 7g–k and with at least three shares, the secret image could be losslessly recovered (Figure 7l–o). Figure 7p–y shows the histograms of the displayed shares and the recovered images with two shares. All of them are approximately evenly distributed in $[0, 255]$. Therefore, the effectiveness of our scheme for $(3, 10)$ threshold is illustrated.

The proposed scheme is also applicable to color images by sharing the split RGB channels. Figure 8 shows the results of sharing a color secret image with size of $512 \times 512 \times 3$ by the proposed CRTSIS, where $k = 4$, $n = 6$, $p = 131$ and $m_i = [256, 257, 259, 261, 263, 265]$. Figure 8b–g are six noise-like color shares, SC_1, SC_2, SC_3, SC_4, SC_5 and SC_6, which tell nothing about the secret image. We also cannot distinguish anything from $k - 1$ shares, as shown in Figure 8h–o. Then, with sufficient shares, the secret image is able to be losslessly recovered. Therefore, it is demonstrated that the proposed scheme is applicable to color images.



(**a**) Secret image (**b**) SC_1 (**c**) SC_3 (**d**) SC_4 (**e**) SC_6

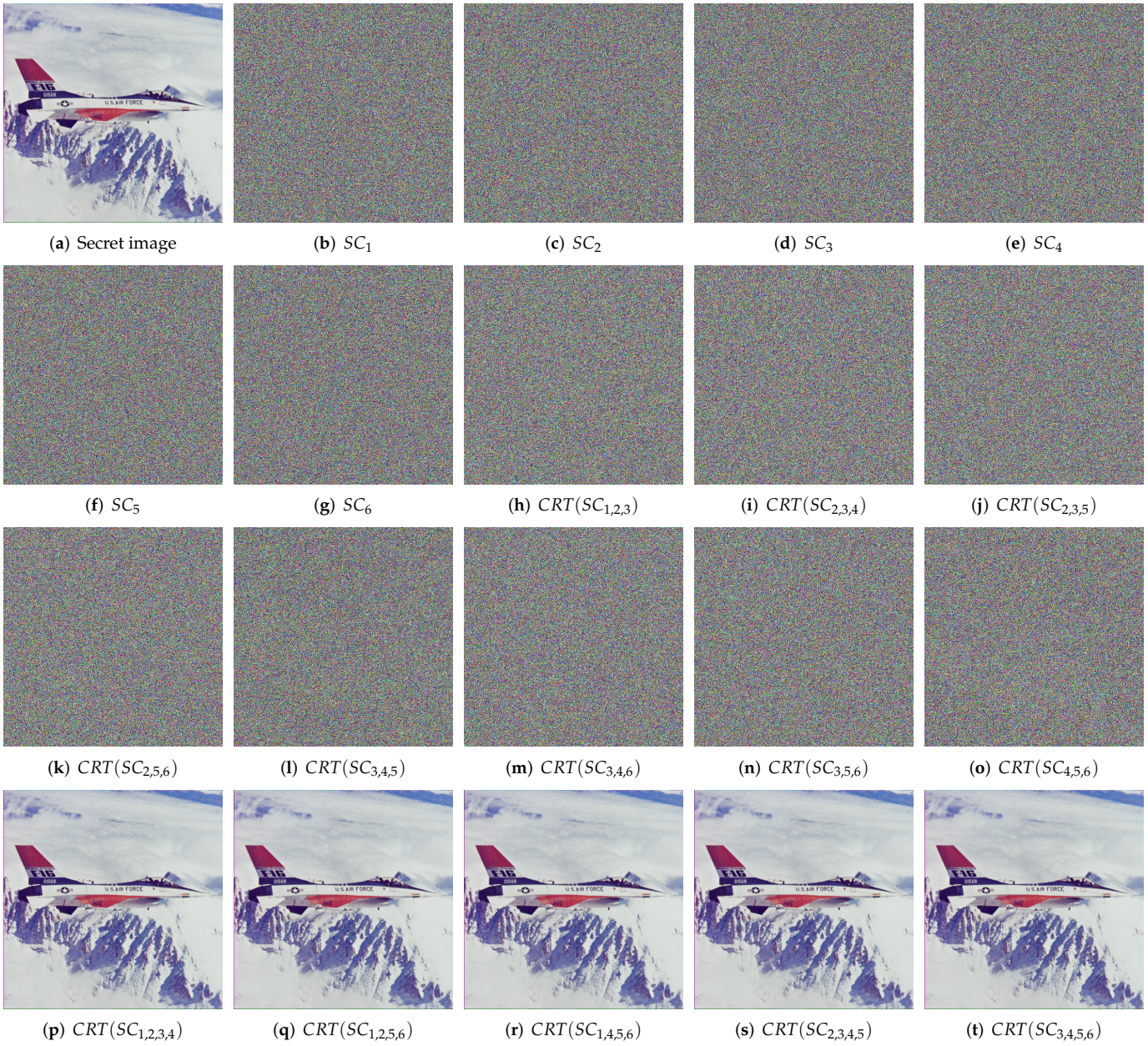
(**f**) SC_9 (**g**) $CRT(SC_{1,3})$ (**h**) $CRT(SC_{1,6})$ (**i**) $CRT(SC_{3,4})$ (**j**) $CRT(SC_{4,6})$

(**k**) $CRT(SC_{6,9})$ (**l**) $CRT(SC_{1,3,4})$ (**m**) $CRT(SC_{3,4,9})$ (**n**) $CRT(SC_{1,6,9})$ (**o**) $CRT(SC_{1,4,6})$

(**p**) Hist of SC_1 (**q**) Hist of SC_3 (**r**) Hist of SC_4 (**s**) Hist of SC_6 (**t**) Hist of SC_9

(**u**) Hist of $CRT(SC_{1,3})$ (**v**) Hist of $CRT(SC_{1,6})$ (**w**) Hist of $CRT(SC_{3,4})$ (**x**) Hist of $CRT(SC_{4,6})$ (**y**) Hist of $CRT(SC_{6,9})$

Figure 7. Experimental results of the introduced scheme for the $(3, 10)$ threshold. (**a**) Secret image; (**b**–**f**) five of the generated shares SC_1, SC_3, SC_4, SC_6 and SC_9; (**g**–**k**) five recovered images with two shares; (**l**–**o**) five recovered images with three shares. (**p**–**y**) ten corresponding histograms.



(**a**) Secret image (**b**) SC_1 (**c**) SC_2 (**d**) SC_3 (**e**) SC_4

(**f**) SC_5 (**g**) SC_6 (**h**) $CRT(SC_{1,2,3})$ (**i**) $CRT(SC_{2,3,4})$ (**j**) $CRT(SC_{2,3,5})$

(**k**) $CRT(SC_{2,5,6})$ (**l**) $CRT(SC_{3,4,5})$ (**m**) $CRT(SC_{3,4,6})$ (**n**) $CRT(SC_{3,5,6})$ (**o**) $CRT(SC_{4,5,6})$

(**p**) $CRT(SC_{1,2,3,4})$ (**q**) $CRT(SC_{1,2,5,6})$ (**r**) $CRT(SC_{1,4,5,6})$ (**s**) $CRT(SC_{2,3,4,5})$ (**t**) $CRT(SC_{3,4,5,6})$

Figure 8. Experimental results of the introduced scheme for the $(4, 6)$ threshold. (**a**) Secret image; (**b**–**g**) six generated shares SC_1, SC_2, SC_3, SC_4, SC_5 and SC_6; (**h**–**o**) eight recovered images with three shares; (**p**–**t**) five recovered images with four shares.

In short, we can conclude from the above illustrations as follows.

(1) Any single share is noise-like, revealing nothing about the secret image.
(2) With fewer than k shares, the recovered images are still meaningless, proving our scheme's security.
(3) The secret image can be losslessly recovered with any k shares, indicating the effectiveness of the proposed scheme.
(4) The proposed scheme has flexible thresholds and is also applicable to color images, thus possessing a strong practicability.

3.3. Discussion

To ensure the generated share pixels were valid, we added the screening operation in the sharing phase to eliminate values over 255, which costed extra computation time. We

give the generation rate of valid shares, denoted as R_vg in (4), to evaluate the cost for the (k, n) threshold.

$$R_vg = \frac{256^n}{m_1 m_2 \cdots m_n} \tag{4}$$

The valid generation rate becomes lower with the increase of participants, which means invalid share values appear more often and more computation time is needed. Figure 9 shows the valid generation rate R_vg obtained with the increase of participants n and the parameters given in Section 3.1. For $n = 10$ and $p = 128$, the valid generation rate is 0.6218, so the extra time for regeneration is acceptable.

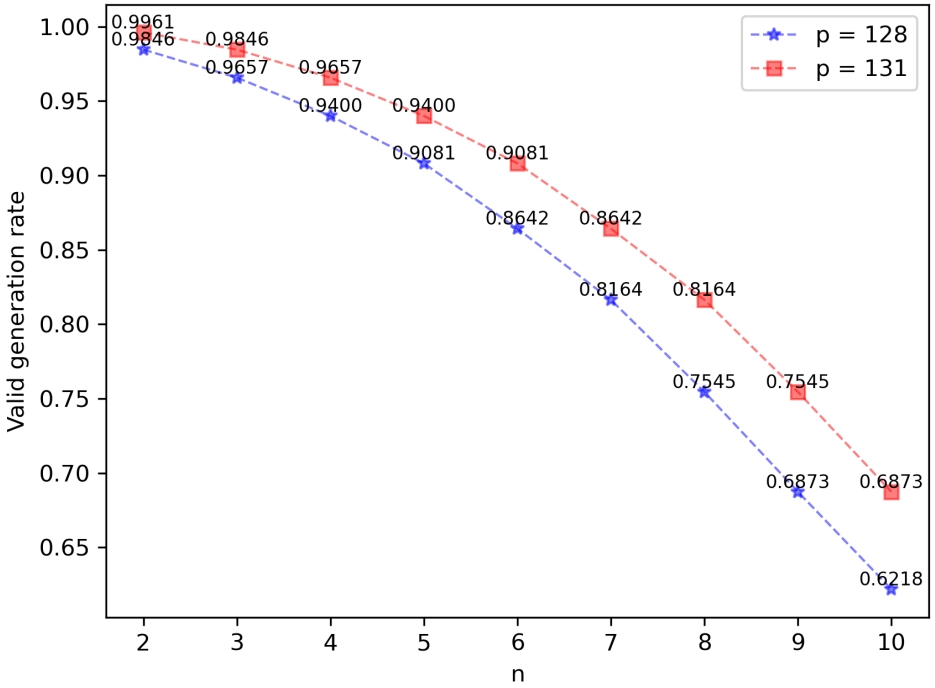


Figure 9. The valid generation rate with the increase of n.

The proposed scheme limits the range of the random integer A to $\left[\left\lceil \frac{N}{p} + 1 \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$, so as to obtain the (k, n) threshold. However, the size of interval $\left[1, \left\lceil \frac{N}{p} \right\rceil\right]$ is rather small compared with the size of interval $\left[1, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$. In practice, we can weaken the security constraint and pick up A starting from 1. Although some secret pixels may be correctly recovered with $k - 1$ shares in a small probability, less than $\frac{1}{p}$, it is scarcely possible to reveal the secret image because of the large number of pixels. Figure 10 shows the result of sharing the secret image, Figure 4, with the same parameters as Figure 5, where the only difference is the range of A, in $\left[1, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$. Apparently, the shares and recovered images with two shares are still noise-like, leaking nothing about the secret image. Their histograms are also similar to the corresponding ones in Figure 5. Therefore, the sacrifice of security is quite little and can be ignored in the application of CRTSIS.

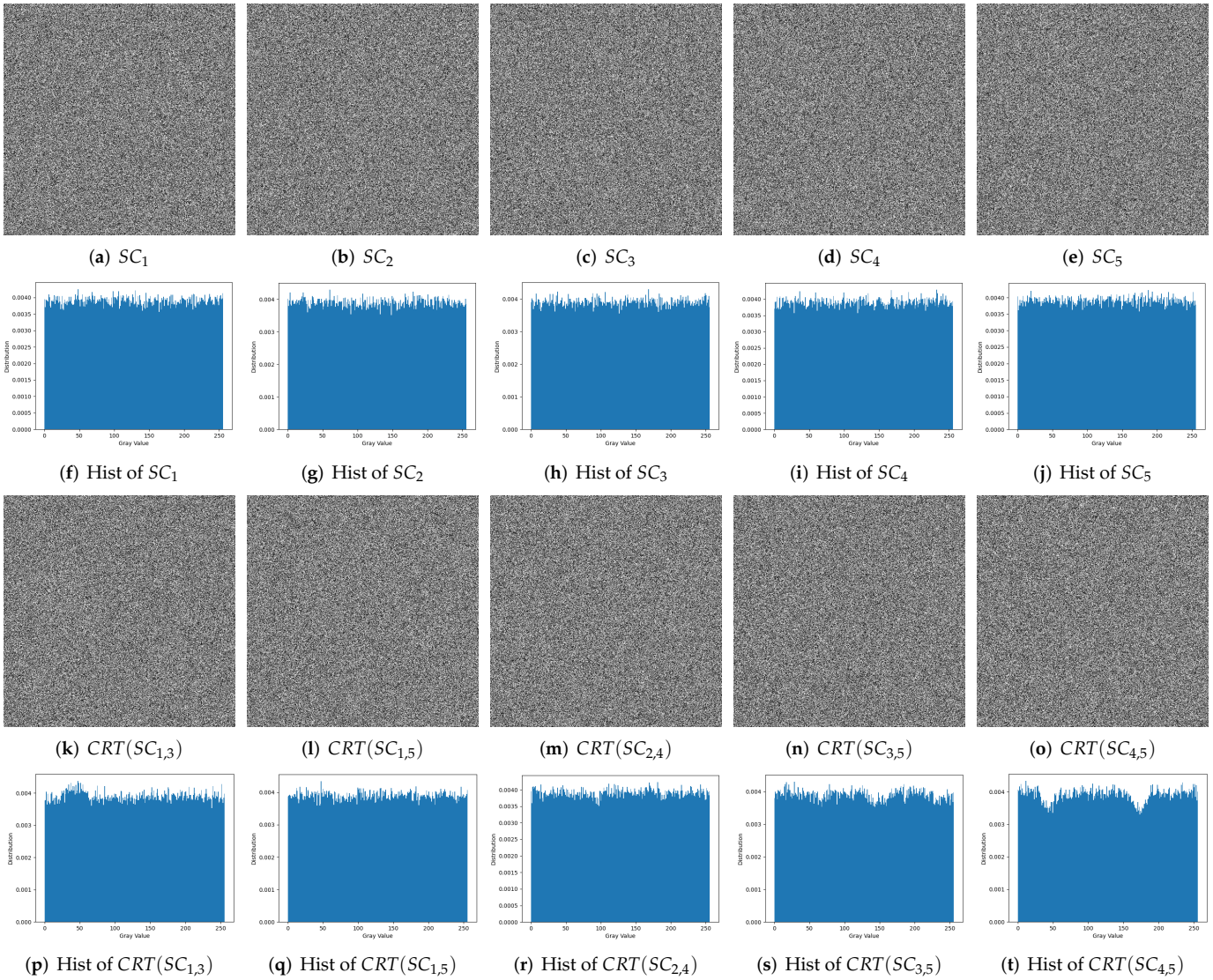


Figure 10. Experimental results of the introduced scheme for the $(3,5)$ threshold and A in $\left[1, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$. (**a**–**e**) Five generated shares SC_1, SC_2, SC_3, SC_4 and SC_5; (**f**–**j**) histograms of the shares; (**k**–**o**) five recovered images with two shares; (**p**–**t**) histograms of the recovered images.

3.4. Comparisons with Related Works

In this part, we compare our scheme with some typical CRTSIS schemes [30,32,33,35], focusing on applicable parameters, lossless recovery, extra transmission and flexible participants.

Ulutas et al.'s scheme [30] introduced the idea of dividing the secret pixels into two intervals and sharing, respectively, based on Asmuth and Bloom's algorithm. However, they did not provide explicit parameters, which creates some confusion in practice, resulting in lossy recovery and security problems in some conditions. Similarly, Yan et al. [33] proposed a CRTSIS scheme based on Asmuth and Bloom's algorithm, dividing the secret pixels into two intervals, corresponding to two equally divided intervals of the random integer A. They also provided restrictions on the range of A and explicit parameters of m_i and p, ensuring the realization of the (k,n) threshold and lossless recovery. However, they had to transmit the parameter T to recover the secret image, bringing extra transmission costs and potential security risks. Our scheme requires no extra parameters except p, shares and corresponding privacy moduli.

Chuang et al. [32] shared the high seven bits of pixels to adapt Asmuth and Bloom's algorithm for images. However, the LSBs of the secret image had to be stored and transmitted

to realize lossless recovery, or they were simply thrown away with a bit of quality loss. Inspired by the technique of LSB matching in information hiding, we embedded the LSBs into A, achieving lossless recovery without extra data transmission. Moreover, they also did not give specific parameters, leaving barriers to users.

Li et al. [35] also shared the high seven bits of the secret pixels and embedded the LSBs into A. However, they chose the moduli smaller than 256, the same as in Chuang et al.'s scheme and Yan et al.'s scheme. Therefore, with the increase of n, the range of shared pixels in their scheme became narrower, leading to potential security problems. As a result, they suggested n be no more than six, which is inapplicable to situations with many participants. However, our scheme remained applicable to many more participants. Furthermore, they applied the basic LSB embedding technique, which is easily analyzed and weakens the security, while we introduced an LSB matching technique as an improvement.

We summarize the comparisons in Table 3, and the overall advantages of our scheme are as follows:

(1) It is a practical and lossless (k, n)-threshold CRTSIS with high security.
(2) No extra transmission cost is introduced to achieve lossless recovery.
(3) The share pixels are evenly distributed in $[0, 255]$, relaxing the limitation of the number participants.
(4) Specific parameters are provided for the convenience of users, supporting the occasions with as many as 10 participants.

Table 3. Comparisons with typical CRTSIS schemes.

Schemes	Applicable Parameters	Lossless Recovery	Extra Transmission	Flexible Participants
Ulutas et al. [30]	No	Yes (Conditional)	Yes	No
Chuang et al. [32]	No	No	Yes (for LSBs of pixels)	No
Yan et al. [33]	Yes	Yes	Yes	No
Li et al. [35]	Yes	Yes	No	No
The proposed scheme	Yes	Yes	No	Yes

4. Conclusions

This paper proposed a practical and lossless Chinese-remainder-theorem-based secret image sharing (CRTSIS) with a (k, n) threshold. Our scheme was based on Asmuth and Bloom's algorithm and overcame the challenges of applying it to images. We took the high seven bits of grayscale pixels as the secret and utilized the LSB matching technique to embed LSBs into the random integer according to the secret pixel's positions. The innovation of the proposed scheme is using the moduli greater than 255 and applying the screening operation to eliminate invalid generated pixels. Therefore, the size of the secret space is the same as that of the shares. We achieved the properties of a (k, n) threshold, lossless recovery and no auxiliary encryption. Furthermore, the much more flexible constraint of a (k, n) threshold significantly improved the practicability of CRTSIS. Theoretical analyses proved the security of the proposed scheme and typical experiments illustrated the effectiveness. Comparison with representative works showed the better performance of our scheme. Therefore, we proved that the proposed scheme is a valid lossless secret image sharing scheme with good practicability. Future work may focus on two aspects. First, design schemes based on the proposed CRTSIS to achieve some practical characteristics, such as meaningful shares, multisecret, etc. Second, since modification of the random integer weakens the scheme's security, it is of great significance to propose quantitative criteria.

Author Contributions: Data curation, L.L. (Lintao Liu); Investigation, Y.L. Methodology, L.L. (Longlong Li); Validation, Y.S.; Writing—original draft, L.L. (Longlong Li); Writing—review & editing, J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (grant number: 61602491).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Cheng, Y.; Fu, Z.; Yu, B. Improved Visual Secret Sharing Scheme for QR Code Applications. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2393–2403. [CrossRef]
2. Yan, X.; Lu, Y.; Liu, L.; Wan, S.; Ding, W.; Liu, H. Exploiting the Homomorphic Property of Visual Cryptography. *Int. J. Digit. Crime Forensics* **2017**, *9*, 45–56. [CrossRef]
3. Li, Y.; Guo, L. Robust Image Fingerprinting via Distortion-Resistant Sparse Coding. *IEEE Signal Process. Lett.* **2018**, *25*, 140–144. [CrossRef]
4. Chavan, P.V.; Atique, M.; Malik, L. Signature based authentication using contrast enhanced hierarchical visual cryptography. In Proceedings of the 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 1–2 March 2014; pp. 1–5. [CrossRef]
5. Abd El-Latif, A.A.; Abd-El-Atty, B.; Hossain, M.S.; Rahman, M.A.; Alamri, A.; Gupta, B.B. Efficient Quantum Information Hiding for Remote Medical Image Sharing. *IEEE Access* **2018**, *6*, 21075–21083. [CrossRef]
6. Fukumitsu, M.; Hasegawa, S.; Iwazaki, J.y.; Sakai, M.; Takahashi, D. A Proposal of a Secure P2P-Type Storage Scheme by Using the Secret Sharing and the Blockchain. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 803–810. [CrossRef]
7. Zou, S.; Liang, Y.; Lai, L.; Shamai, S. An Information Theoretic Approach to Secret Sharing. *IEEE Trans. Inf. Theory* **2015**, *61*, 3121–3136. [CrossRef]
8. Soleymani, M.; Mahdavifar, H.; Avestimehr, A.S. Analog Secret Sharing With Applications to Private Distributed Learning. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1893–1904. [CrossRef]
9. Beugnon, S.; Puech, W.; Pedeboy, J.P. Format-Compliant Selective Secret 3-D Object Sharing Scheme. *IEEE Trans. Multimed.* **2019**, *21*, 2171–2183. [CrossRef]
10. Naor, M.; Shamir, A. Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994*; Springer: Berlin/Heidelberg, Germany, 1995; pp. 1–12.
11. Wang, G.; Liu, F.; Yan, W.Q. Basic Visual Cryptography Using Braille. *Int. J. Digit. Crime Forensics* **2016**, *8*, 85–93. [CrossRef]
12. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
13. Asmuth, C.A.; Bloom, J. A Modular Approach to Key Safeguarding. *Inf. Theory IEEE Trans.* **1983**, *29*, 208–210. [CrossRef]
14. Mignotte, M. How to Share a Secret. In *Cryptography: Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, 29 March–2 April 1982*; Springer: Berlin/Heidelberg, Germany, 1983; pp. 371–375.
15. Weir, J.; Yan, W.Q. *A Comprehensive Study of Visual Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 70–105.
16. Wang, Z.; Arce, G.R.; Di Crescenzo, G. Halftone visual cryptography via error diffusion. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 383–396. [CrossRef]
17. Wang, S.; Yan, X.; Sang, J.; Niu, X. Meaningful visual secret sharing based on error diffusion and random grids. *Multimed. Tools Appl.* **2016**, *75*, 3353–3373. [CrossRef]
18. Fu, Z.x.; Yu, B. Visual Cryptography and Random Grids Schemes. In *Digital-Forensics and Watermarking*; Springer: Auckland, New Zealand, 2014; pp. 109–122.
19. Guo, T.; Liu, F.; Wu, C. Threshold visual secret sharing by random grids with improved contrast. *J. Syst. Softw.* **2013**, *86*, 2094–2109. [CrossRef]
20. Meghrajani, Y.K.; Mazumdar, H.S. Enhanced Contrast of Reconstructed Image for Image Secret Sharing Scheme Using Mathematical Morphology. *J. Inf. Secur.* **2015**, *6*, 273–279. [CrossRef]
21. Yan, X.; Lu, Y. Progressive visual secret sharing for general access structure with multiple decryptions. *Multimed. Tools Appl.* **2018**, *77*, 2653–2672. [CrossRef]
22. Prasetyo, H.; Hsia, C.H.; Prayuda, A.W.H. Progressive Secret Sharing with Adaptive Priority and Perfect Reconstruction. *J. Imaging* **2021**, *7*, 70. [CrossRef] [PubMed]
23. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
24. Yang, C.N.; Ciou, C.B. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image Vis. Comput.* **2010**, *28*, 1600–1610. [CrossRef]
25. Li, P.; Yang, C.N.; Wu, C.C.; Kong, Q.; Ma, Y. Essential secret image sharing scheme with different importance of shadows. *J. Vis. Commun. Image Represent.* **2013**, *24*, 1106–1114. [CrossRef]
26. Li, P.; Yang, C.N.; Kong, Q. A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. *J. Real-Time Image Process.* **2018**, *14*, 41–50. [CrossRef]
27. Liu, Y.X.; Yang, C.N.; Wu, C.M.; Sun, Q.D.; Bi, W. Threshold changeable secret image sharing scheme based on interpolation polynomial. *Multimed. Tools Appl.* **2019**, *78*, 18653–18667. [CrossRef]
28. Yan, W.; Ding, W.; Dongxu, Q. Image Sharing Based on Chinese Remainder Theorem. *J. North China Univ. Technol.* **2000**, *12*, 6–9.

29. Shyu, S.J.; Chen, Y.R. Threshold Secret Image Sharing by Chinese Remainder Theorem. In Proceedings of the IEEE Asia-Pacific Services Computing Conference, Washington, DC, USA, 9–12 December 2008; pp. 1332–1337.
30. Ulutas, M.; Nabiyev, V.V.; Ulutas, G. A new secret image sharing technique based on Asmuth Bloom's scheme. In Proceedings of the 2009 International Conference on Application of Information and Communication Technologies, Baku, Azerbaijan, 14–16 October 2009; pp. 1–5.
31. Chunqiang, H.; Xiaofeng, L.; Di, X. Secret image sharing based on chaotic map and Chinese remainder theorem. *Int. J. Wavelets Multiresolut. Inf. Process.* **2012**, *10*, 1250023.
32. Chuang, T.W.; Chen, C.C.; Chien, B. Image Sharing and Recovering Based on Chinese Remainder Theorem. In Proceedings of the 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi'an, China, 4–6 July 2016; pp. 817–820.
33. Yan, X.; Lu, Y.; Liu, L.; Liu, J.; Yang, G. Chinese remainder theorem-based two-in-one image secret sharing with three decoding options. *Digit. Signal Process.* **2018**, *82*, 80–90. [CrossRef]
34. Yan, X.; Lu, Y.; Liu, L.; Wan, S.; Ding, W.; Liu, H. Chinese Remainder Theorem-Based Secret Image Sharing for (k, n) Threshold. In *Cloud Computing and Security*; Sun, X., Chao, H.C., You, X., Bertino, E., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 433–440.
35. Li, L.; Lu, Y.; Yan, X.; Liu, L.; Tan, L. Lossless (k, n)-Threshold Image Secret Sharing Based on the Chinese Remainder Theorem without Auxiliary Encryption. *IEEE Access* **2019**, *7*, 75113–75121. [CrossRef]
36. Quisquater, M.; Preneel, B.; Vandewalle, J. On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In *Public Key Cryptography*; Naccache, D., Paillier, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; pp. 199–210.
37. Drăgan, C.C.; Tiplea, F.L. On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme. *Inf. Sci.* **2018**, *463–464*, 75–85. [CrossRef]
38. Ker, A.D. Improved Detection of LSB Steganography in Grayscale Images. In *Information Hiding*; Fridrich, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 97–115.