Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 18(3): 2473–2495.
DOI: 10.3934/mbe.2021126
Received: 10 January 2021
Accepted: 05 March 2021
Published: 12 March 2021

Research article

Fake and dishonest participant location scheme in secret image sharing

Jingju Liu, Lei Sun*, Jinrui Liu and Xuehu Yan

National University of Defense Technology, Hefei 230037, China

* **Correspondence:** Email: sun0119@nudt.edu.cn.

Abstract: A (k, n) threshold secret image sharing (SIS) scheme divides a secret image into n shadows. One can reconstruct the secret image only when holding k or more than k shadows but cannot know any information on the secret from fewer than k shadows. Based on this characteristic, SIS has been widely used in access control, information hiding, distributed storage and other areas. Verifiable SIS aims to prevent malicious behaviour by attackers through verifying the authenticity of shadows and previous works did not solve this problem well. Our contribution is that we proposed a verifiable SIS scheme which combined CRT-based SIS and $(2, n + 1)$ threshold visual secret sharing(VSS). Our scheme is applicable no matter whether there exists a third party dealer. And it is worth mentioning that when the dealer is involved, our scheme can not only detect fake participants, but also locate dishonest participants. In general, loose screening criterion and efficient encoding and decoding rate of CRT-based SIS guarantee high-efficiency shadows generation and low recovery computation complexity. The uncertainty of the bits used for screening prevents malicious behavior by dishonest participants. In addition, our scheme has the advantages of lossless recovery, no pixel expansion and precise detection.

Keywords: secret image sharing; visual secret sharing; Chinese remainder theorem; shadow authentication; high-efficiency shadows generation

1. Introduction

With the rapid development of computer technology, the importance of information security becomes more and more prominent. As an important carrier of information transmission, image protection has been paid more and more attention by the society. And image encryption technology has developed rapidly in recent years. For different image protection needs, various image encryption technology was proposed, including modern cryptographic mechanism [1, 2] (such as DES, RSA, secret image sharing), digital watermarking technology [3–5], compressive sensing technology [6–8], etc. Among them, secret image sharing technology divides the secret into n shadows and only k or more than k shadows can reconstruct the secret. Due to this characteristic, it is widely used in access

control, information hiding, key management and so on.

Blakley [9] and Shamir [10] firstly proposed the concept of secret sharing independently in 1979. Then more and more secret sharing schemes have been proposed. For example, Gutub et al. proposed a novel counting-based secret sharing scheme [11] by replacement operations in 2017. Al-Ghamdi et al. [12] enhanced the security of Gutub's scheme in 2018. [13] improved the security and efficiency of counting-based secret sharing scheme and [14] pursued higher security and lower computation complexity.

In 1995, Naor and Shamir [15] introduced the threshold control into image field and proposed visual cryptography: visual secret sharing(VSS). The secret image is shared into n transparencies. Any k of them can reveal the secret by stacking k transparencies, but any $k-1$ of them cannot get any information on secret. The essence of VSS is stacking recovery or XOR recovery, which requires little or no cryptographic computations. However, VSS has disadvantages such as pixel expansion and low image quality which needs more research on it.

Based on the Shamir' polynomial-based method, Thien and Lin [16] expanded the secret sharing into image encryption, also known as secret image sharing (SIS). SIS scheme for (k, n) threshold divides a secret image into n noise-like shadows. One can reconstruct the secret by k or more than k shadows while gain nothing from fewer than k shadows.

In order to divide the secret a_0 into n shadows, polynomial-based SIS constructs a $(k-1)$ degree polynomial with the secret a_0 and other $(k-1)$ randomly selecting numbers $a_1, a_2, \cdots, a_{k-1}$ to form the coefficients of the polynomial. n shares $(f(i), i = 1, 2, \cdots, n)$ are generated by using different variables. And the secret a_0 can be rebuilt by using Lagrange interpolation. The polynomial is defined as

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \mod P \tag{1.1}$$

where P is a prime number, a_0 represents the secret information and $a_1, a_2, \cdots, a_{k-1}$ are selected randomly.

However, Shamir's original polynomial-based SIS is generally lossy recovery with higher computation and auxiliary encryption. Since the modulus P is chosen as 251 instead of 256, the recovery image will be lossy when the pixel value of the secret image exceeds 251. In the secret recovery phase, the computational complexity of Lagrange interpolation is as high as $O(klog^2k)$. And some auxiliary encryption may be applied before sharing.

In comparison with Shamir's original polynomial-based SIS, Chinese remainder theorem-based SIS has advantages of lossless recovery, low recovery computation(the modular only $O(k)$ operations) and no auxiliary encryption. Yan et al. [17] proposed a (k, n) threshold secret image sharing scheme based on Chinese remainder theorem(CRTSIS) which is the basic algorithm in [18]. Through dividing the grayscale pixel values into two intervals corresponding to two available mapping intervals, the proposed method realizes (k, n) threshold and lossless recovery for grayscale image without auxiliary encryption. We adopt CRTSIS as our sharing algorithm and the specific algorithm implementation is described in section 4 .

However, traditional SIS scheme ignores the authenticity of shadows which is fatal in many scenarios such as e-voting, e-auctions and so on. The fake shadow may be forged by a fake participant to defraud the real shadow and then obtain the secret, or be generated by a dishonest participant. As an example, if a dishonest participant wants to monopolize the secret, he\she only needs to forge a fake shadow in exchange for another $k-1$ real shadows. If there is no shadow authentication, only the

dishonest participant can recover the secret and other $k-1$ participants cannot get any information on the secret. It is possible to find the dishonest participant with the help of other $n-k$ participants, but the execution complexity is high. Therefore, it is necessary to verify the authenticity of the shadows to locate the attacker.

The rest of the paper is organized as follows. Section 2 introduces related work. Section 3 demonstrates the application scenarios. Section 4 introduces some basic requirements for the proposed scheme. The proposed scheme is presented in detail in section 5. Section 6 shows the experimental results and analysis and section 7 concludes this paper.

2. Related work

Chor et al. [19] firstly proposed "verifiable secret sharing" and achieved verifying through simultaneous broadcast network. Due to the widespread use of SIS, more and more attention is paid to verifiable SIS scheme.

Traditional SIS with shadow authentication capacity usually rely on hash function [20, 21] and information hiding method such as fragile watermark [22–26]. Li et al. [20] enhanced (k, n) threshold SIS scheme with authentication. The size of stego image is reduced to $3.5/k$ times while it is 4 times in previous scheme. And the authentication capability is guaranteed by hash function. Lin et al. [22] proposed a (k, n) threshold SIS scheme with additional capabilities of steganography and authentication. A secret image is firstly shared into n shares and then they are hidden into n meaningful camouflage images to improve security. Furthermore, fragile watermark is embedded into camouflage images for authenticating the fidelity of each processed camouflage image. In general, most SIS schemes with authentication capability embed shares into cover images which leads to high generation and recovery complexity and pixel expansion.

Different from traditional methods, Yan et al. [27] proposed a (k, n) threshold SIS scheme with a separate shadow authentication capacity. Yan et al. [27] combined polynomial-based SIS and VSS. A binary authentication image is split into two shadows by using the $(2, 2)$ threshold RG-VSS. One is distributed to dealer to verify the identities of participants, another is used to guide the generation of secret shadow images. Their scheme has the advantages of lossless recovery, no pixel expansion and precise detection. However, their scheme is only applicable to dealer-participatory. Another flaw is that their scheme can not resist the malicious behaviour of dishonest participants since they can easily forge a fake shadow passing verifying from the real shadow they hold.

Yang et al. [28] proposed a novel compressed SIS with shadow verification capability based on polynomial-based SIS and $(2, 2)$ threshold VSS. By utilizing the randomness of the sharing phase of polynomial-based SIS, one share generated from $(2, 2)$ threshold random-grid VSS is embedded into all shares of polynomial-based SIS as the verification information and another share is distributed to dealer for verification. In order to balance efficiency and safety, Yang et at. [28], unlike Thien and Lin [16], uses coefficients a_0 and a_{k-1} in Eq 1.1 to store secret information. However, the sharing process may fail when k is less than 4 due to small random range. Just like Yan et al. [27], their scheme is only applicable to dealer-participatory and is invalid for dishonest participants.

Jiang et al. [29] proposed a SIS method for a (k, n) threshold with dealer-participatory and non-dealer-participatory mutual shadow authentication capabilities. They combined polynomial-based SIS and $(2, n+1)$ threshold VSS utilized the result of the VSS to screen out the

eligible secret shadow images. Due to the rigorous screening criterion and the Lagrange interpolation method, the computation complexity of generation and recovery phase is relatively high. In order to obtain a lossless reconstructed image, the prime P in Eq 1.1 is set as 257. When the value of 256 appears, the screening operation is re-performed, which further increases the complexity of shadow generation. Similarly, Jiang's scheme can not detect the dishonest participants. In fact, we can find a more general approach in [30].

Traditional verifiable SIS schemes have disadvantages of pixel expansion, requiring extra information and high computation complexity. Yan et al. [27], Yang et al. [28] and Jiang et al. [29] have low efficiency in shadow generation process, relatively high computation complexity in secret recovery phase and no ability to detect dishonest participants. In addition, Yan et al. [27] and Yang et al. [28] are only applicable to dealer involved.

In this paper, we propose a verifiable SIS scheme combining CRT-based SIS and $(2, n+1)$ threshold VSS. A binary authentication image with the same size as the secret image is divided into $n+1(n)$ binary shadows with dealer involved(uninvolved). N binary shadows are used to screen out the secret shadows meeting the criterion. When there exists a dealer, we utilize the uncertainty of the bits used for screening to detect the dishonest participants. When there is no dealer involved, participants verify the authenticity of shadows mutually. In addition, loose screening criterion and efficient encoding and decoding rate of CRT-based SIS guarantee high-efficiency shadows generation and low recovery computation complexity.

3. Application scenarios

Here, we only consider three kinds of roles, participants, dealer and attacker. Dealer divides secret into shadows and distributes them to participants, participants hold their own shadow. As to attackers, we divide them into dishonest participants and fake participants, and the difference between them is whether they hold real shadows. More precisely, dishonest participants tend to monopolize secrets, while fake participants want to steal them. The proposed scheme is applicable to both dealer involved and dealer uninvolved. When there exists a dealer, he\she is trusted by everyone. Dealer calculates and distributes shadows to participants. In the recovery phase, the dealer collects shadows to reconstruct the secret. If the recovery fails, the authenticity of shadows should be verified. The forged shadows may come from dishonest participants or fake participants. Dealer can accurately locate the attacker by the binary authentication shadow S_1C_{n+1}. Because of the uncertainty of bits used for screening, even the dishonest participant can not forge a fake shadow passing verification. When there is no dealer involved, all the participants trust each other, which implies that there is no dishonest participant. In this case, bits used for screening are fixed, and each participant can calculate the binary authentication shadow from the secret shadow they hold. Before the recovery phase, to prevent fake participants from impersonating participants, k (or more) participants exchange binary authentication shadows. Only when the verification is successful can they exchange shadows to reconstruct the secret. Both these scenarios are common and meaningful in real life.

Herein, symbol S and S_1 respectively represent grayscale secret image and binary authentication image and the notations used in this paper is introduced in Table 1. For the (k, n) threshold, mark n grayscale secret shadows as $SC_1, SC_2, \cdots, SC_n$ held by participants, use S_1C_{n+1} to represent the binary authentication shadow belonging to dealer. $S_2C_1, S_2C_2, \cdots, S_2C_k$ respresent binary authentication

shadows calculated from the secret shadows.

Table 1. The notations used in the paper.

Notations	Decriptions
k	The minimum number of shadows in recovery phase.
n	The number of participants.
S	The grayscale secret image.
S_1	The binary authentication image.
SC_i	The secret shadows obtained from CRT-based SIS.
S_1C_i	The binary authentication shadows obtained from VSS.
S_2C_i	The binary shadows extracted from SC_i for authentication.
ETO	The function converting the grayscale pixel into the eight-bit binary form.
COL	The function counting the amount of 1 in binary sequence.

When there exists a dealer, as shown in Figure 1, Participant II is the attacker(dishonest participant or fake participant). Dealer collects k shadows and try to reconstruct secret. Since shadow SC_2 is fake, recovery phase fails. Dealer then extracts k binary authentication shadows $S_2C_1, S_2C_2, \cdots, S_2C_k$ from $SC_1, SC_2, \cdots, SC_k$ according to the bits used for screening. And dealer verifies the authenticity of shadows by doing XOR operation between S_1C_{n+1} and $S_2C_i (i = 1, 2, \cdots, k)$. Finally, S_2C_2 fails the verification and Participant II is identified as the attacker.

When there is no dealer, k participants verify the identities of others mutually. For each one of the k participants, the identities of the remaining $k-1$ participants need to be verified, and on the other hand, each participant receives $k-1$ authentication results. Take $(3, 3)$ threshold as an example, as shown in Figure 2, Participant I, Participant II and Participant III hold secret shadows SC_1, SC_2, SC_3 respectively. They obtain their own binary authentication shadows S_2C_1, S_2C_2, S_2C_3 respectively calculated from the secret shadows they hold. In the verification phase, Participant I sends S_2C_1 to Participant II and Participant III and receives S_2C_2 and S_2C_3 from them. Participant I verifies the identities of Participant II and Participant III by doing XOR operation and receives two results from them. It is the same for Participant II and Participant III.

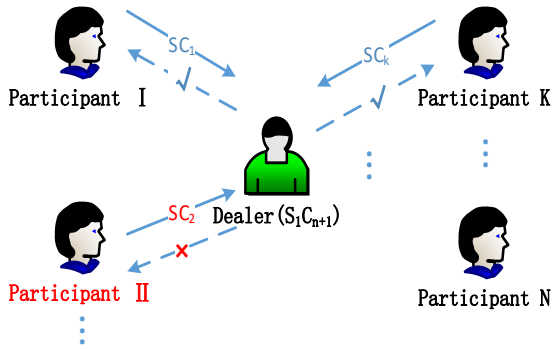


Figure 1. (k, n) threshold with dealer.

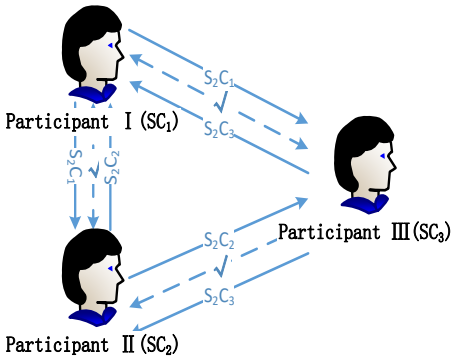


Figure 2. $(3, 3)$ threshold without dealer.

4. Preliminaries

In this section, we introduce some preliminaries for the designed scheme. Herein, symbol $\oplus$ indicates the Boolean XOR. A grayscale secret image S (a binary authentication image S_1) with the size of $H \times W$ is divided into n $(n + 1)$ shadows denoted as $SC_1, SC_2, \cdots, SC_n$ $(S_1C_1, S_1C_2, \cdots, S_1C_{n+1})$. The first n binary authentication shadows are used to guide the generation of secret shadows. The $(n + 1)$-th binary authentication shadow is distributed to the dealer to verify the authenticity of shadows.

4.1. (2-n)-VSS

Algorithm 1 : $(2, n)$ **VSS.**
Input: A binary secret image S_1 with size of $H \times W$ **Output**: n binary shadow images $S_1C_1, S_1C_2, \cdots, S_1C_n$
Step 1: For each position $(h, w) \in \{(h, w)\|1 \le h \le H, 1 \le w \le W\}$, repeat Steps 2–5. Use b_x denotes the temporary pixels, $x = 1, 2, \cdots, H \times W$. **Step 2:** Generate b_{x_1}, b_{x_2} randomly where b_{x_i} is equal to 0 or 1, $i = 1, 2$. **Step 3:** Check whether $b_{x_1} \oplus b_{x_2}$ is equal to b_x, if so, skip to Step5, otherwise go to Step4. **Step 4:** Pick the inverse of either b_{x_1} or b_{x_2} at random so that $b_{x_1} \oplus b_{x_2}$ is equal to b_x. **Step 5:** Set $b_{x_3} = b_{x_1}, b_{x_4} = b_{x_2}, b_{x_5} = b_{x_1}, b_{x_6} = b_{x_2} \cdots$ if $n \pmod 2 = 0, b_{x_n} = b_{x_2}$, else $b_{x_n} = b_{x_1}$ **Step 6:** Output n binary shadow images $S_1C_1, S_1C_2, \cdots, S_1C_n$.

Algorithm 1 describes the sharing phase for $(2, n)$ VSS. It is remarkable that Step 2 and Step 3 ensure that $b_{x_1} \oplus b_{x_2} = b_x$. Step 5 extends the threshold from $(2, 2)$ to $(2, n)$. In our proposal, it should be noted that when the threshold of SIS is (k, n), the threshold of VSS is $(2, n + 1)$ for dealer involved and $(2, n)$ for dealer uninvolved.

Recover: Choose any two shadows from the n participants, do XOR operation between the corresponding pixel values and obtain the reconstructed binary image.

4.2. SIS Based on CRT

4.2.1. CRT

Chinese remainder theorem is an important theorem in number theory and has been widely used in various fields of information security such as RSA algorithm [31, 32], secret sharing [17] and so on. And a lot of work [33, 34] has been done to analyze the performance characteristics and security characteristics of the CRT-based cryptosystems. CRT aims to solve a set of linear congruence equations. A set of integers $m_i (i = 1, 2, \cdots, n)$ are chosen to subject to $gcd(m_i, m_j) = 1$ for $i \neq j$. Let $M = \prod_{i=1}^{k} m_i, M_i = \frac{M}{m_i}$ and $M_i M_i^{-1} \equiv 1 \pmod{m_i}$. Then there exists only one solution $y \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}) \pmod{M}$ in $[0, M - 1]$ for the following linear congruence equations

$$y \equiv a_1 \pmod{m_1}$$

$$y \equiv a_2 \pmod{m_2}$$

...

$$y \equiv a_k \pmod{m_k} \tag{4.1}$$

4.2.2. (k, n) SIS based on CRT

A (k, n) threshold secret image sharing scheme based on Chinese remainder theorem(CRTSIS) was proposed in [17]. The original secret image S is divided into n shadow images $SC_1, SC_2, \cdots, SC_n$ with corresponding privacy modular integers $m_1, m_2, \cdots, m_n$. The generation steps are described in Algorithm 2 and the recovery steps are presented in Algorithm 3.

Algorithm 2 : CRTSIS method for (k, n) threshold.

Input: The original secret image S with size of $H \times W$ and threshold parameters (k, n).
Output: n shadows $SC_1, SC_2, \cdots, SC_n$ and corresponding privacy modular integers $m_1, m_2, \cdots, m_n$.

Step 1: Choose a set of integers $128 \leq p < m_1 < m_2 \cdots < m_n \leq 256$ subject to

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 is public among all the participants.

Step 2: Compute $T = \left\lfloor \frac{\left\lfloor \frac{M}{p} - 1 \right\rfloor - \left\lceil \frac{N}{p} \right\rceil}{2} + \left\lceil \frac{N}{p} \right\rceil \right\rfloor$ and T is public among all the participants as well. For each position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 3–4.
Step 3: Let $x = S(h, w)$.
If $0 \leq x < p$, pick up a random integer A in $\left[T + 1, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ and let $y = x + Ap$.
Else pick up a random integer A in $\left[\left\lceil \frac{N}{p} \right\rceil, T\right)$ and let $y = x - p + Ap$.
Step 4: Compute $a_i \equiv y \pmod{m_i}$ and let $SC_i(h, w) = a_i$ for $i = 1, 2, \cdots, n$.
Step 5: Output n shadow images $SC_1, SC_2, \cdots, SC_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots, m_n$.

The parameters of $p, m_1, m_2, \cdots, m_n$ for different thresholds we used in experiments are shown in Table 2. In the experiment, the parameters in Table 2 can guarantee the pixel values of secret shadows approximately uniform distribution in range $[0, m_i - 1]$, which tells that each shadow gives no clue about the secret image.

5. The designed scheme

In this section, we introduce the overview of the proposed scheme and try to analyze the preformance of $(2, n + 1)$ threshold VSS and (k, n) threshold CRT-based SIS.

5.1. Overview of the proposed scheme

Figure 3 shows the overall process of proposed scheme. The explicit sharing algorithm is illustrated in Algorithm 4 and its matching authentication and recovery algorithm are in Algorithm 5.

Algorithm 3 : Secret image recovery of CRTSIS.

Input: k shadow images $SC_{i_1}, SC_{i_2}, \cdots, SC_{i_k}$, their corresponding privacy modular integers $m_{i_1}, m_{i_2}, \cdots, m_{i_k}, p$ and T.

Output: A $H \times W$ recovered secret image S'.

Step 1: For each 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 $j = 1, 2, \cdots, k$. To solve the following linear equations by the Chinese remainder theorem.

$$\begin{aligned} y &\equiv a_{i_1} \pmod{m_{i_1}} \\ y &\equiv a_{i_2} \pmod{m_{i_2}} \\ &\cdots \\ y &\equiv a_{i_{k-1}} \pmod{m_{i_{k-1}}} \\ y &\equiv a_{i_k} \pmod{m_{i_k}} \end{aligned}$$

Step 3: Computer $T^* = \left\lfloor \frac{y}{p} \right\rfloor$. If $T^* \geq T$, let $x \equiv y \pmod{p}$. Else let $x = y \pmod{p} + p$. Set $S'(h, w) = x$.

Step 4: Output the recovered binary secret image S'.

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

k	n	p	$m_1, m_2, \cdots, m_n$
2	2	128	253,255
		131	253,254
2	3	128	251,253,255
		131	253,254,255
3	3	128	251,253,255
		131	253,254,255
2	4	128	247,251,253,255
		131	251,253,254,255
3	4	128	247,251,253,255
		131	251,253,254,255
4	4	128	247,251,253,255
		131	251,253,254,255
2	5	128	245,247,249,251,253
		131	247,251,253,254,255
3	5	128	245,247,249,251,253
		131	247,251,253,254,255
4	5	128	245,247,249,251,253
		131	247,251,253,254,255
5	5	128	245,247,249,251,253
		131	247,251,253,254,255

The grayscale secret image S is the same size as the binary authentication image S_1. Without lossing generality, take a secret pixel $S(h, w)$ as an example. Through the above CRTSIS method, it is split into n secret shadow pixels denoted by $SC_1(h, w), SC_2(h, w), \cdots, SC_n(h, w)$. Meanwhile, the pixel $S_1(h, w)$ in the same position as $S(h, w)$ in the binary authentication image is split into $n + 1$ binary shadow pixels by the VSS method of $(2, n + 1)$ threshold. Among them, the first n binary shadow pixels are used to guide the generation of secret shadow pixels, and the $(n + 1)$-th binary shadow pixel is used to generate binary shadow image S_1C_{n+1} for dealer to verify the authenticity of shadows. When there is no dealer, we use the $(2, n)$ threshold VSS method instead. Briefly speaking, there is no need to generate the binary shadow image S_1C_{n+1} for dealer.

Now, we have n grayscale secret shadow pixels ranging from 0 to 255 and n binary shadow pixels between 0 and 1. Different from using the lowest plane of n secret shadow pixels for screening in Jiang et al. [29], for each secret shadow pixel $SC_i(h, w)(i = 1, 2, \cdots, n)$, we transform it as eight bits in binary form. When there exists a dealer, we randomly choose four bits out of eight and get a binary value denoted by $S_2C_i(h, w)$ by doing XOR operation between them. When there is no dealer, all eight bits are used for screening. For convenience, We mark this operation as multi-bit-XOR and denote it by function ETO. So we have two binary sequences of n elements, $S_1C_i(h, w)(i = 1, 2, \cdots, n)$ and $S_2C_i(h, w)(i = 1, 2, \cdots, n)$. Here, we use Seq-1 to represent sequence $S_1C_i(h, w)(i = 1, 2, \cdots, n)$ and Seq-2 to represent sequence $S_2C_i(h, w)(i = 1, 2, \cdots, n)$. Finally, in the screening phase, when the amount of 1 in Seq-2 is equal to the amount of 1 in Seq-1, pass screening and n secret shadow pixels $SC_1(h, w), SC_2(h, w), \cdots, SC_n(h, w)$ are assigned to the corresponding positions of n secret shadow images; otherwise, pixel $S(h, w)$ is re-shared with CRTSIS method to obtain new Seq-2 until it passes screening. The sharing phase ends when all pixels of the secret image have been shared.

To be brief, a binary authentication image S_1 with the same size as the secret image was divided into $(n+1)$ binary shadows $S_1C_i(i = 1, 2, \cdots, n+1)$ through $(2, n+1)$ VSS. The secret image S was divided into n shadows $SC_i(i = 1, 2, \cdots, n)$ through CRT-based SIS. The first n binary shadows were used to screen out the secret shadows meeting the criteria and the $(n + 1)$-th binary shadow was distributed to the dealer to verify the authenticity of secret shadows. When there is no dealer involved, participants verify identities of others mutually.

Regarding Figure 3, we remark that:

- The function ETO converts the grayscale pixel value $SC_i(h, w)$ into the eight-bit binary form, and then gets a binary value $S_2C_i(h, w)$ by doing XOR operation between multiple bits.
- The function COL counts the amount of 1 in the sequence Seq.

Algorithm 4 describes the sharing phase of the proposed scheme for dealer involved. When there is no dealer, take the $(2, n)$-VSS instead and all the eight bits are used for screening.

Algorithm 5 describes the authentication and recovery phase of the proposed scheme. There are two cases here, dealer involved and dealer uninvolved. When there exists a dealer, participants do not know which four bits are used for screening, so they can not forge a fake shadow to pass verification. Dealer collects k (or more) shadows. To save time, dealer carries out restoration phase directly. If the recovery fails, dealer extracts binary authentication shadow $S_2C_1, S_2C_2, \cdots, S_2C_k$ and verifies the authenticity of shadows. Finally the fake shadow is detected and the attacker is located. When there is no dealer, participants trust each other. Since bits used for screening are fixed, participants can calculate binary authentication shadows from the secret shadows they hold. In order to prevent fake

Algorithm 4 : The sharing process of the proposed secret image sharing scheme for (k, n) threshold with shadow authentication capacity

Input: A $H \times W$ grayscale secret image S, a $H \times W$ binary authentication image S_1, the threshold parameters (k, n), where $2 \leq k \leq n$.

Output: Secret shadow images $SC_i (i = 1, 2, \cdots, n)$ for participants, a binary authentication shadow image S_1C_{n+1} for dealer.

Step 1: Choose appropriate parameters $p, m_1, m_2, \cdots, m_n$ according to the threshold parameters (k, n). For each position $(h, w) \in \{(h, w)|1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2–5.

Step 2: Utilize $(2, n + 1)$-VSS to split $S_1(h, w)$ into $n + 1$ bits, denoted by $S_1C_1(h, w), S_1C_2(h, w), \cdots, S_1C_n(h, w), S_1C_{n+1}(h, w)$. Use Seq-1 to represent sequence $S_1C_1(h, w), S_1C_2(h, w), \cdots, S_1C_n(h, w)$. $S_1C_{n+1}(h, w)$ is used to construct the binary authentication image S_1C_{n+1} for dealer.

Step 3: Utilize CRTSIS to split $S(h, w)$ into n secret shadow pixels, denoted by $SC_1(h, w), SC_2(h, w), \cdots, SC_n(h, w)$. For each $SC_i(h, w)$, let $S_2C_i(h, w) = ETO(SC_i(h, w))$. Use Seq-2 to represent sequence $S_2C_1(h, w), S_2C_2(h, w), \cdots, S_2C_n(h, w)$.

Step 4: Compare whether the amount of 1 in Seq-2 is equal to that in Seq-1. If so, go to Step 5; otherwise return to Step 3.

Step 5: Put $SC_1(h, w), SC_2(h, w), \cdots, SC_n(h, w)$ to the corresponding position of secret shadow images $SC_1, SC_2, \cdots, SC_n$.

Step 6: Output n secret shadow images $SC_1, SC_2, \cdots, SC_n$ for participants and a binary authentication shadow S_1C_{n+1} for dealer if exists.

Algorithm 5 : The authentication and recovery process of the proposed secret image sharing scheme for (k, n) threshold with shadow authentication capacity

Input: The binary authentication image S_1 and dealer's binary authentication shadow image S_1C_{n+1}, any k grayscale shadow images $SC_1, SC_2, \cdots, SC_k$.

Output: k authenticating results for k participants when there exists a dealer or $(k - 1)$ authenticating results for each participant when there is no dealer. Recoverd grayscale secret image S'.

Step 1: For each pixel $SC_i(h, w)$ of $SC_i (i = 1, 2, \cdots, k)$, let $S_2C_i(h, w) = ETO(SC_i(h, w))$, getting k binary images denoted by S_2C_i for authenticating.

Step 2: If there is a dealer, once the recovery fails, obtain the reconstructed binary authentication image S'_{1_i} through doing XOR operation of S_1C_{n+1} and $S_2C_i (i = 1, 2, \cdots, k)$. One fake shadow is identified and broadcast the attacker to public.

Step 3: If there is not a dealer involved, For participant SC_i, obtain $k - 1$ reconstructed binary authentication images $S'_{1_j} (j = 1, 2, \cdots, i - 1, i + 1, \cdots, k)$ through doing XOR operation of S_2C_i and S_2C_j. If S'_{1_j} are recognized as S_1 by Human visual system(HVS), pass the authentication and go to Step 4; otherwise a fake shadow is identified and broadcast the fake participant to public.

Step 4: Using Algorithm 3 to obtain the recovered secret image S' from k shadow images $SC_1, SC_2, \cdots, SC_k$.

participant from stealing secret, participants firstly exchange binary authentication shadows. When the verification passes, participants exchange secret shadows to reconstruct secret, otherwise the fake participant is located and notified.

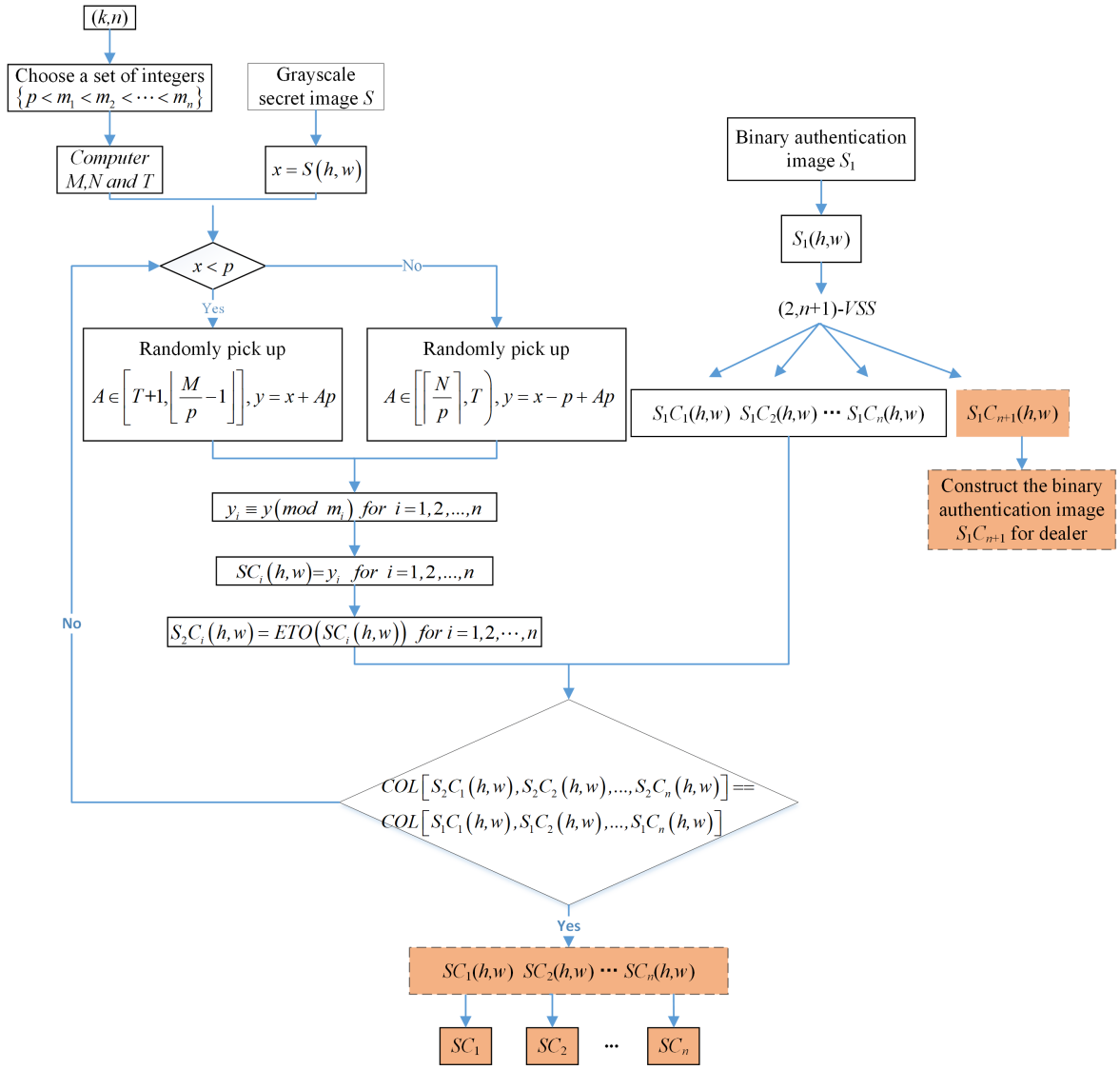


Figure 3. The proposed scheme.

5.2. *Image quality analysis and security analysis*

5.2.1. Analysis for the quality of recovery image using $(2, n)$ VSS algorithm

According to Algorithm 1, we can theoretically derive the expected quality of recovery image. In order to show the derivation process more clearly and verify the correctness of the derivation, we take $(2, 5)$ threshold as an example. Divide into two cases to discuss when the origin pixel is 0 or 1.

When the origin pixel is 0:

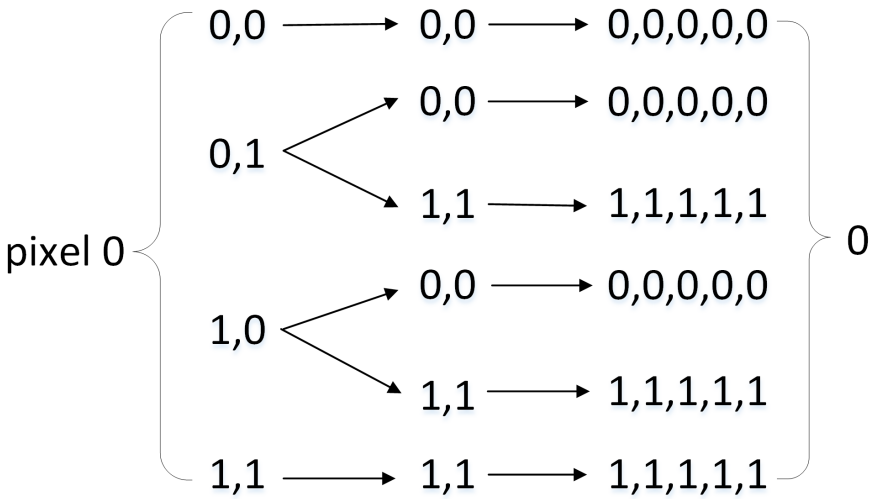


Figure 4. Origin pixel 0 for $(2, 5)$ threshold.

As described in Figure 4 ,when the origin pixel is 0, according to Algorithm 1, we have 50% chance to get the sequence $(0, 0, 0, 0, 0)$, similarly, we have 50% chance to get another sequence $(1, 1, 1, 1, 1)$. In the recovery phase, we need choose two values from sequence $(0, 0, 0, 0, 0)$ or $(1, 1, 1, 1, 1)$ randomly and do XOR operation between them. Since these two sequences are made of the same elements, we must get the result 0 in the recovery phase. That is to say the origin pixel 0 can always be restored losslessly.

When the origin pixel is 1 :

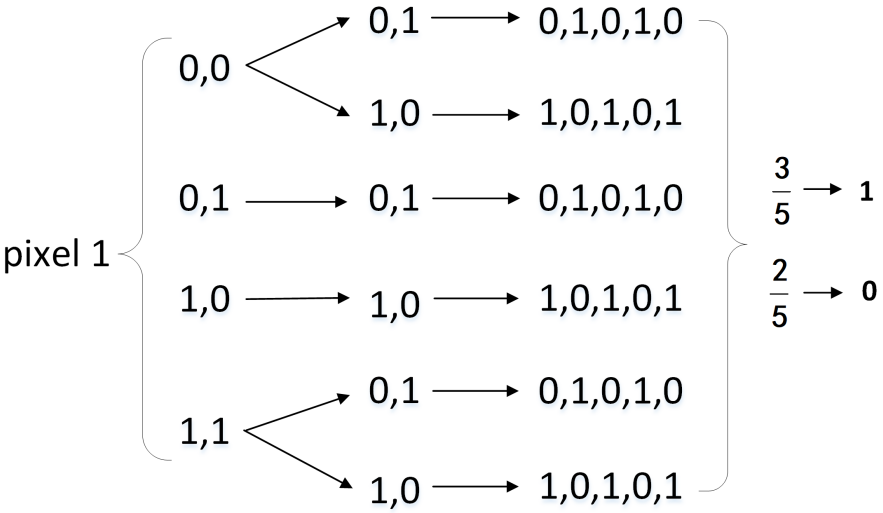
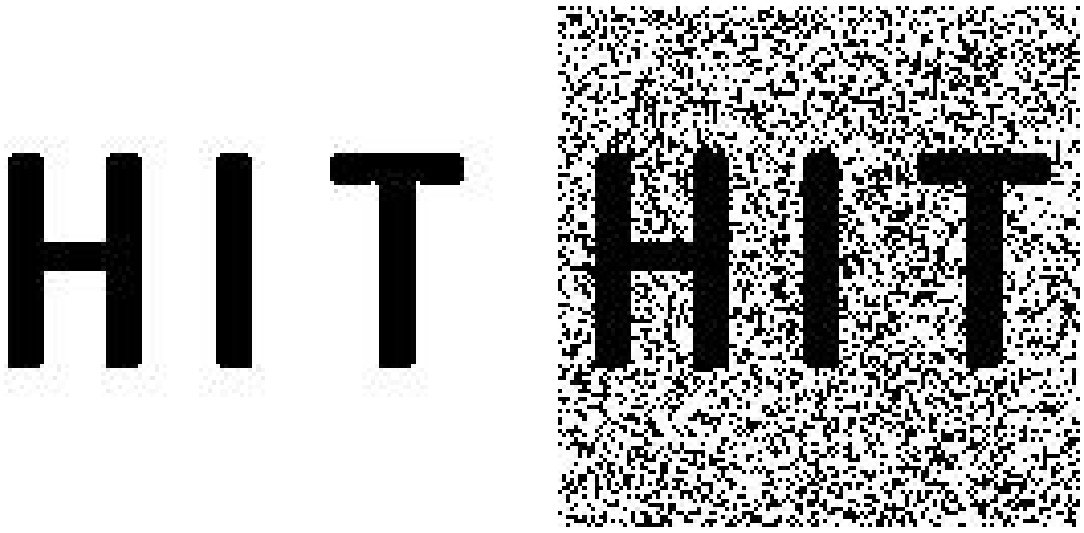


Figure 5. Origin pixel 1 for $(2, 5)$ threshold

As shown in Figure 5, when the origin pixel is 1, according to Algorithm 1, we have 50% chance to get the sequence $(0, 1, 0, 1, 0)$, similarly, we have 50% chance to get another sequence $(1, 0, 1, 0, 1)$.

For the sequence $(0, 1, 0, 1, 0)$, we choose two values randomly and do XOR operation in the recovery phase. If we want to get result 1, the two values must be different and we can calculate the probability as $\frac{C(3,1)\times C(2,1)}{C(5,2)} = \frac{3}{5}$. On the contrary, the probability we get the result 0 is $\frac{2}{5}$. And it is the same for the sequence $(1, 0, 1, 0, 1)$.

In conclusion, for the $(2, 5)$ threshold, theoretically, we can recover pixel 0 losslessly and recover pixel 1 with the probability of 60%.



(a) S_1 (b) S^*

Figure 6. Example for $(2, 5)$ threshold. (a) The original image S_1; (b) The reconstructed image S^*.

To verify the conclusion, we did an experiment based on the Algorithm 1 and took the threshold as $(2, 5)$. As demonstrated in the Figure 6, S_1 represents the original image and S^* represents the reconstructed image by doing XOR operation between any two of the five shadows. S_1 has the size of 128×128 and consists of 14195 white pixels and 2189 black pixels. We use 0 to represent black pixels and 1 to represent white pixels. According to the conclusion, the white pixels should be $14195 \times 0.6 = 8517$, and the black pixels should be $2189 + 14195 \times 0.4 = 7867$ in S^*. In the experimental results, the amount of white pixels is 8580 and for black pixels is 7804. Considering the uncertainty of random events, the experimental results are consistent with the derived conclusion.

In conclusion, for the origin pixel 0, we can always recover it losslessly. For the origin pixel 1, if n is even, let $n = 2t$, then we can get the probability recovering the value correctly as $\frac{C(t,1)\times C(t,1)}{C(2t,2)} = \frac{t}{2t-1}$. Similarly, when n is odd, let $n = 2t + 1$, we have the probability as $\frac{C(t,1)\times C(t+1,1)}{C(2t+1,2)} = \frac{t+1}{2t+1}$.

In the proposed scheme, we use 0 to represent black pixels and 1 to represent white pixels. The reasons are as follows:

- In general, for a binary image, the secret information is denoted by black, so it is in line with human senses to recover the secret information losslessly.
- The screening times for pixel 0 are more than those for pixel 1 in our scheme. And the black pixels of the binary authentication image "hit" are much less than the white pixels in our experiment. Therefore, the use of 0 to represent black pixel can reduce the times of screening operation to

improve generation efficiency. On the contrary, if the authentication image contains more black pixels, we can use 0 to represent white pixels to improve generation efficiency.

5.2.2. Security analysis of $(2, n+1)$ threshold VSS and (k, n) threshold CRT-based SIS

In [35], we can find the security analysis for (k, n) threshold VSS. And in our scheme, the value of k is fixed at 2 which is one of the cases in [35] and the analysis process is consistent. As for (k, n) threshold CRT-based SIS, we adopt the method CRTSIS proposed in [17] which contains the security analysis. However, Okeya et al. [34] mention a side channel attack(SCA) which is valid to CRT-based cryptosystems. Since the principle of CRT is the same, our scheme is not resistant to this type of attack. And the security analysis and enhancements will be future work.

6. Experimental results and analysis

6.1. Experimental illustration

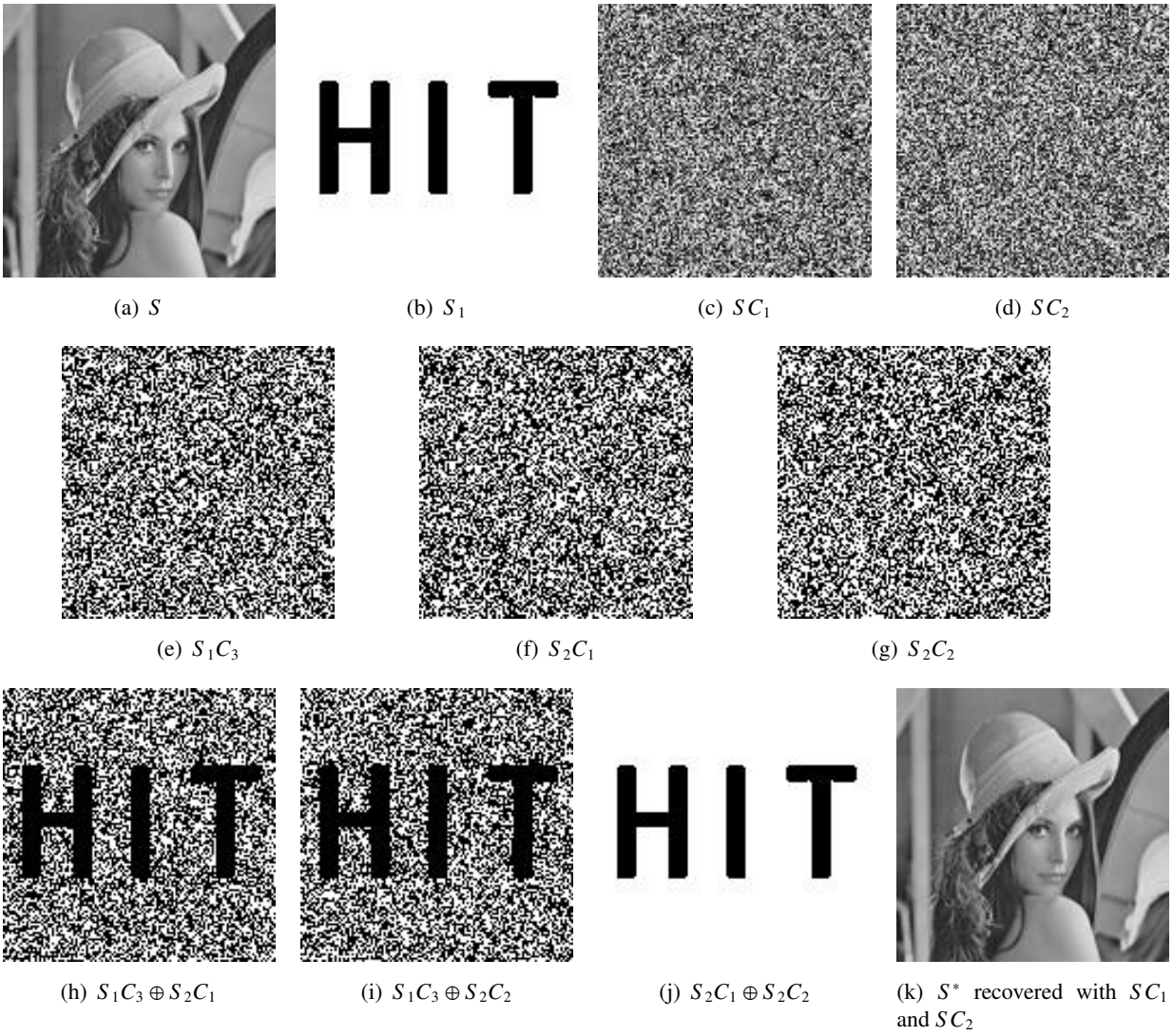
In the experiment, we select $p = 131$ and $2 \leq k \leq n \leq 5$. Secret image S has the same size of 128×128 as the binary authentication image S_1. Here we introduce the experimental results of $(2, 2)$ threshold and $(3, 4)$ threshold with dealer involved and dealer uninvolved. Figure 7 exhibits the results of $(2, 2)$ threshold. S and S_1 represent the grayscale secret image and binary authentication image respectively. SC_1, SC_2 denote the secret shadow images calculated by Algorithm 4. S_1C_3 represents the binary authentication shadow image for dealer and S_2C_1, S_2C_2 denote the binary authentication shadow images calculated from SC_1, SC_2 by multi-bit-XOR operation. When there exists a dealer, he\she can verify the authenticity of shadows SC_1, SC_2. Figure 7 (h),(i) shows the authentication results. When there is no dealer, two participants verify identities mutually. Figure 7 (j) exhibits the authentication result. According to section 5.2.1, it is lossless recovery for pixel 0 (black area) regardless of the value of n. For the pixel 1 (white area), when there is dealer involved, $n = 3, t = 1$, the probability recovering the pixel 1 correctly is $\frac{1+1}{2\times1+1} = \frac{2}{3}$; when there is no dealer involved, $n = 2, t = 1$, the probability recovering the pixel 1 correctly is $\frac{1}{2\times1-1} = 1$. Fig 7 (k) represents the recovered image calculated from SC_1 and SC_2.

Figure 8 exhibits the results for $(3, 4)$ threshold. Figure 8 (i)–(j) show the authentication results when there exists a dealer. Figure 8 (k) show the authentication result when there is no dealer. Similarly, for the pixel 0, it can be recovered losslessly. For the pixel 1, when there is dealer involved, $n = 5, t = 2$, the probability recovering the pixel 1 correctly is $\frac{2+1}{2\times2+1} = \frac{3}{5}$; when there is no dealer involved, $n = 4, t = 2$, the probability recovering the pixel 1 correctly is $\frac{2}{2\times2-1} = \frac{2}{3}$. Figure 8 (l) represents the recovered image calculated from SC_1, SC_2 and SC_3.

6.2. Analysis for Multi-Bit-XOR for screening

6.2.1. Efficiency

In the experiment, $p = 131$ and $2 \leq k \leq n \leq 5$, for each set of parameter pairs (k, n), we recorded the screening times and formed Figure 9. As shown in Figure 9, the X-axis represents the amount of bits used for the screening operation. We use symbol s to denote it. In Jiang et al. [29], $s = 1$ and in our scheme, $s = 4$ for dealer involved and $s = 8$ for dealer uninvolved. The Y-axis represents the times of screening operation. When n is determined, the times of screening do not change significantly

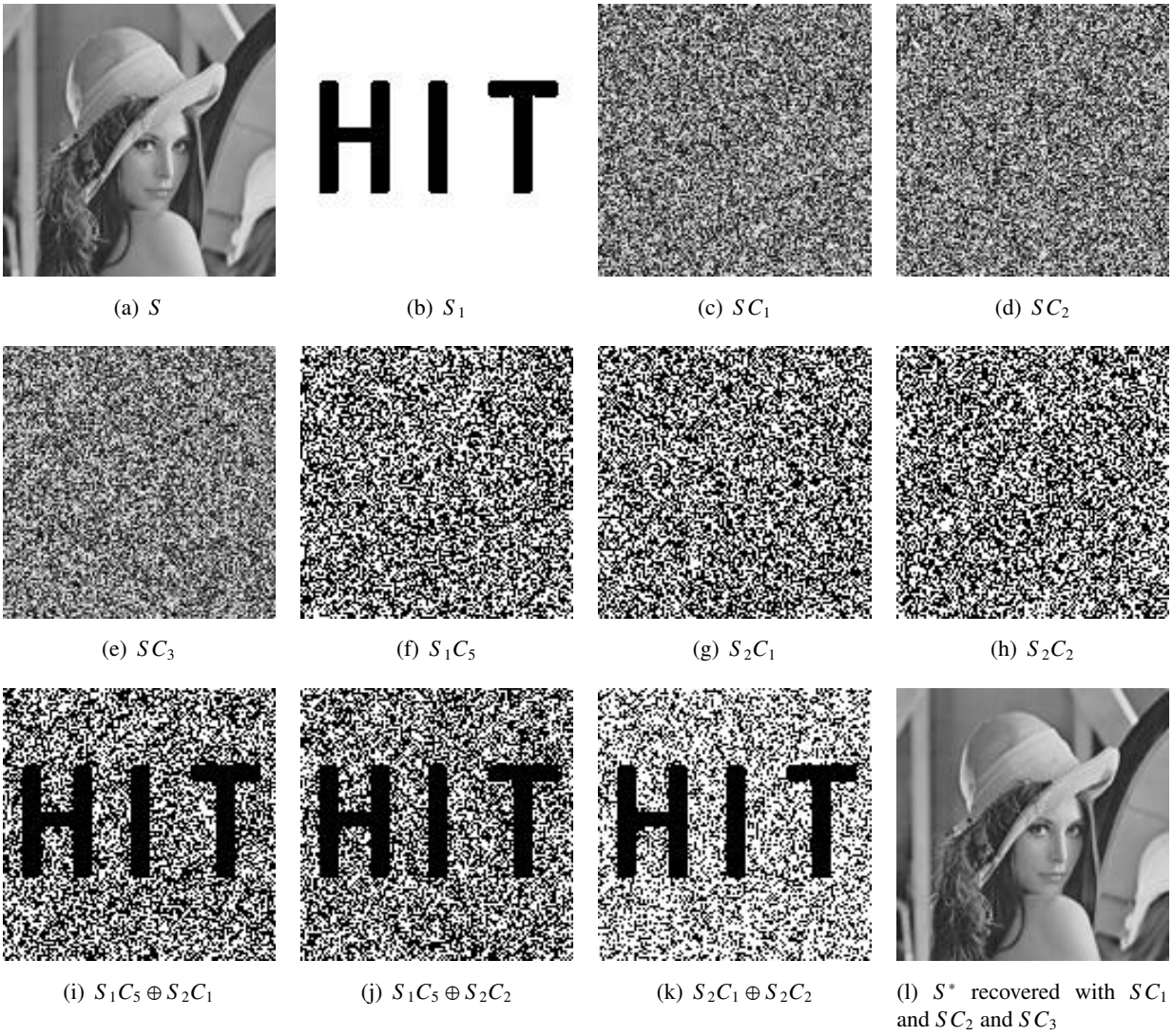


(a) S (b) S_1 (c) SC_1 (d) SC_2

(e) S_1C_3 (f) S_2C_1 (g) S_2C_2

(h) $S_1C_3 \oplus S_2C_1$ (i) $S_1C_3 \oplus S_2C_2$ (j) $S_2C_1 \oplus S_2C_2$ (k) S^* recovered with SC_1 and SC_2

Figure 7. Experiments of the designed scheme for $(2, 2)$ threshold, where $p = 131, m_1 = 253, m_2 = 255$. (a) The secret image S; (b) the authentication image S_1; (c)–(d) the secret shadow images SC_1, SC_2; (e) the binary authentication shadow image S_1C_3 for dealer; (f)–(g) the binary shadow images S_2C_1, S_2C_2 calculated from SC_1, SC_2 for authentication; (h)–(i) the authentication result with dealer; (j) the authentication result with non-dealer; (k) recovered secret image S^* from SC_1 and SC_2.



(a) S (b) S_1 (c) SC_1 (d) SC_2

(e) SC_3 (f) S_1C_5 (g) S_2C_1 (h) S_2C_2

(i) $S_1C_5 \oplus S_2C_1$ (j) $S_1C_5 \oplus S_2C_2$ (k) $S_2C_1 \oplus S_2C_2$ (l) S^* recovered with SC_1 and SC_2 and SC_3

Figure 8. Experiments of the designed scheme for $(3, 4)$ threshold, where $p = 131, m_1 = 247, m_2 = 251, m_3 = 253, m_4 = 255$. (a) The secret image S; (b) the authentication image S_1; (c)–(e) the secret shadow images SC_1, SC_2, SC_3; (f) the binary authentication shadow image S_1C_5 for dealer; (g)–(h) the binary authentication shadow images S_2C_1, S_2C_2 obtained from SC_1, SC_2 for authentication; (i)–(j) the authentication result with dealer; (k) the authentication result with non-dealer; (l) recovered secret image S^* from SC_1, SC_2 and SC_3.

with the increase of k. And when n increases, the times of screening increase. More importantly, when the parameter pairs (k, n) is determined, the times of screening do not change significantly with the increase of s, that is to say that the efficiency of screening is almost independent of parameter s. To be brief, whether s is 1 or 4 or 8 has little impact on the screening efficiency.

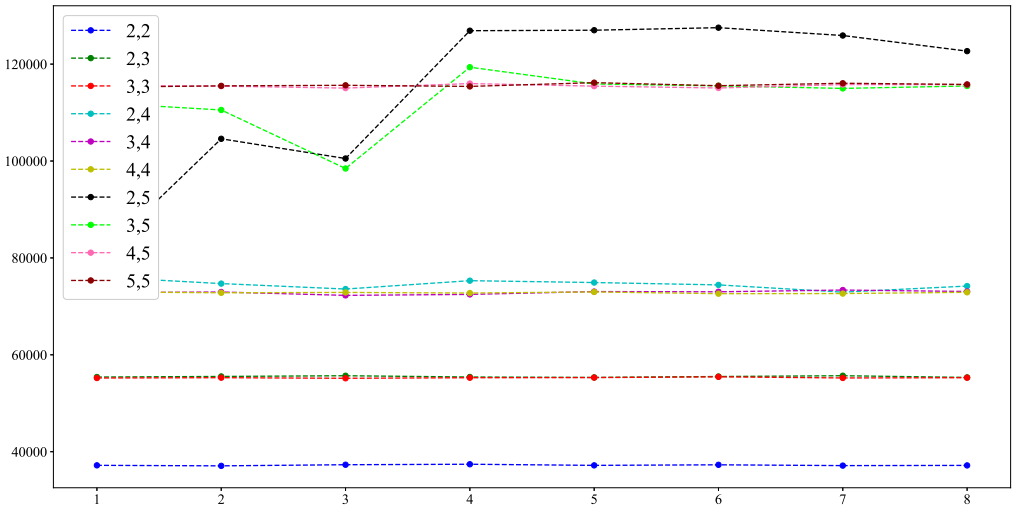


Figure 9. Screening times of parameter pairs (k, n).

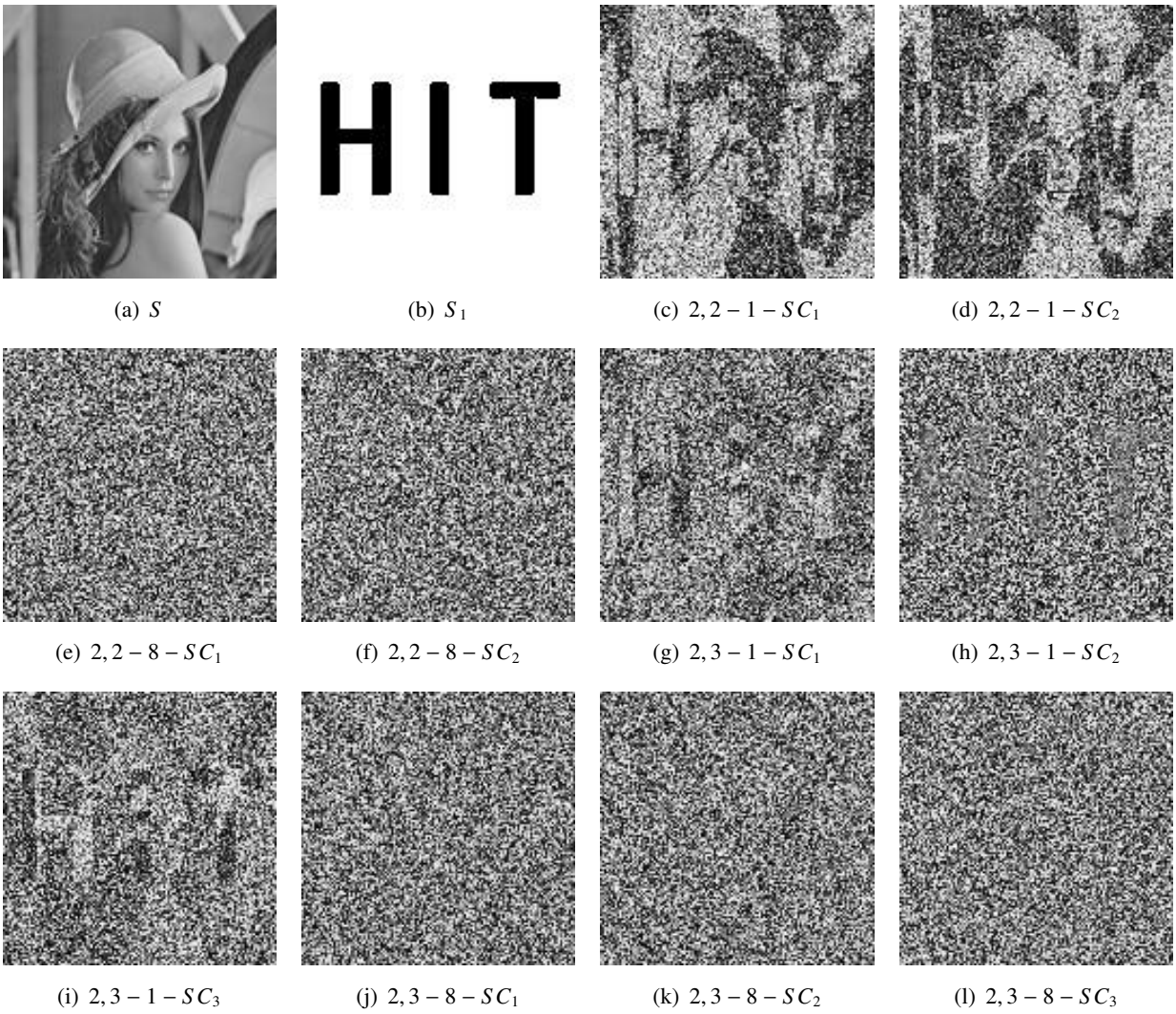
6.2.2. Security

In the experiment, when k is fixed at 2 and use the lowest bit for screening operation (i.e. $s = 1$), no matter which value n is taken in interval $[2, 5]$, we find that the secret shadow images reveal the information of binary authentication image S_1. More seriously, when the threshold is $(2, 2)$, we can even see the secret information from the secret shadow images. However, when we use the multi-bit-XOR operation for screening(e.g. $s = 8$), secret shadow images do not reveal any information of authentication image or even secret image. As demonstrated in Figure 10, for $s = 1$ and $s = 8$, we enumerate the thresholds $(2, 2)$ and $(2, 3)$ respectively. Figure 10 (c) and Figure 10 (d) reveal both the information of secret image S and authentication image S_1 for $(2, 2)$ threshold, $s = 1$. In contrast, while $s = 8$, we cannot derive useful information from Figure 10 (e) and Figure 10 (f). For the threshold $(2, 3)$, it is the same except that the secret shadow images do not reveal secret information. The reason why the information of authentication image is disclosed in the secret shadow images for $k = 2$ can be future work.

On the other hand, if bits used for screening are certain, such as $s = 8$, the participants can extract the binary authentication shadows embedded in secret shadows. However, if the participant is dishonest, he\she can easily forge a fake shadow which can pass verification. Therefore, when we can not determine whether all the participants are honest, we need a credible third-party dealer. In this case, the amount of bits used for screening is fixed at 4, but there are $C(8, 4) = 70$ choices, which

means that dishonest participant can hardly forge a fake shadow passing verification.

In conclusion, considering both efficiency and security, we adopt multi-bit-XOR operation for screening.



(a) S (b) S_1 (c) $2,2-1-SC_1$ (d) $2,2-1-SC_2$

(e) $2,2-8-SC_1$ (f) $2,2-8-SC_2$ (g) $2,3-1-SC_1$ (h) $2,3-1-SC_2$

(i) $2,3-1-SC_3$ (j) $2,3-8-SC_1$ (k) $2,3-8-SC_2$ (l) $2,3-8-SC_3$

Figure 10. Experiments of the designed scheme for $(2,2)$ threshold and $(2,3)$ threshold where $s = 1$ and 2 respectively. (a) The secret image S; (b) the authentication image S_1; (c)–(f) the secret shadow images for $(2,2)$ threshold; (g)–(l) the secret shadow images for $(2,3)$ threshold.

6.3. Comparison with related works

Yan et al. [27], Yang et al. [28] and Jiang et al. [29] aim to detect fake participants in SIS. Their works are all based on polynomial, and the screening criterion is bitwise comparison. Our scheme is much more efficient in the shadow generation process and the computation complexity of recovery phase is relatively low. We make quantitative comparison with Jiang's work in Figure 11. More detailed comparison can be seen in Table 3.

Jiang et al. [29] proposed a SIS method for a (k, n) threshold with dealer-participatory and non-dealer-participatory mutual shadow authentication capabilities which integrates polynomial-based SIS and visual secret sharing through using the result of VSS to guide the polynomial-based SIS by a screening operation. The scheme proposed in [29] has no pixel expansion, lossless recovery and a 100% detection rate. However, the execution time of the scheme algorithm is mainly consumed on the screening operation. Figure 11 exhibits the comparison of screening efficiency between Jiang et al. [29] and our scheme.

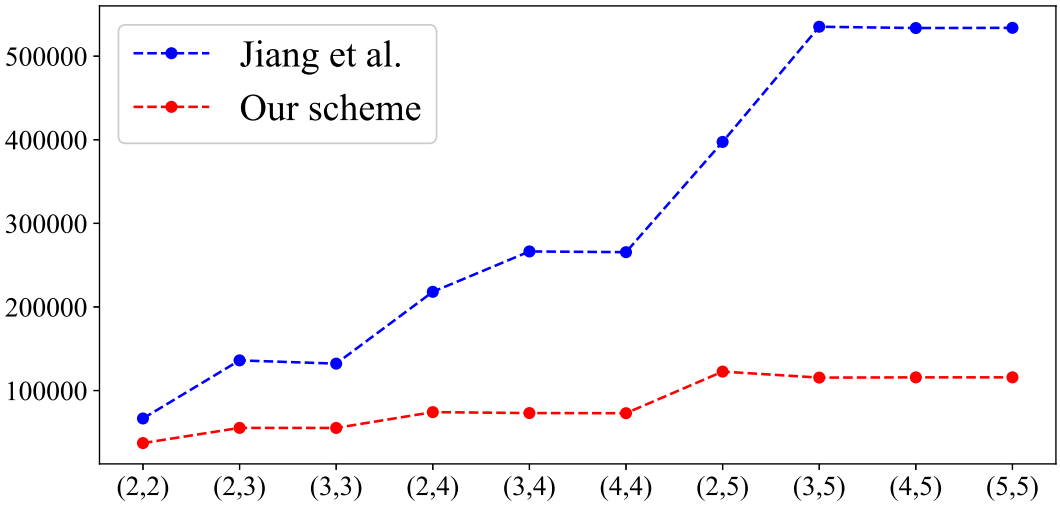


Figure 11. Comparison with Jiang et al. shceme.

As shown in Figure 11, we can find that the screening efficiency of Jiang et al. [29] is much lower than ours. Furthermore, with the increase of n, the gap of screening efficiency between the two schemes also increases. Regarding the difference in efficiency between these two schemes, some reasons are listed as below:

- Differences in secret image sharing algorithms. Our scheme is based on Chinese remainder theorem while Jiang et al. [29] is based on polynomial.
- Differences in the representation of black and while pixels. In our scheme, we use 0 to denote black pixel and 1 to denote while pixel. But it is opposite in Jiang et al. [29]. In the experiment, the binary authentication image we use consists of more white pixels than black pixels. However, the fact is that the screening times of pixel 0 is more than that of pixel 1 in our scheme.
- Differences in screening criterion. In Jiang et al. [29], for one binary authentication sharing shadow sequence $S_1C_1(h, w), S_1C_2(h, w), \cdots, S_1C_n(h, w)$, it requires each element for the corresponding position in the binary secret sharing shadow sequence $S_2C_1(h, w), S_2C_2(h, w), \cdots, S_2C_n(h, w)$ to be equal to it. In other words, screening bit by bit. In contrast, we only need the amount of 1 in the binary secret sharing shadow sequence be equal to that in binary authentication sharing shadow sequence in our scheme. Take the sequence $(0, 1, 0, 1)$ as an example, in Jiang et al. [29] the binary secret sharing shadow sequence must be the same. However, in our scheme, there are 6 kinds of sequences that meet the screening

criterion denoted as $(0,0,1,1),(0,1,0,1),(1,0,0,1),(1,0,1,0),(1,1,0,0)$ and $(0,1,1,0)$. In addition, the two screening criterion are consistent in terms of authentication effectiveness and security.

Table 3. Comparison between related schemes.

Properties	**Our Scheme**	**Yan et al. [27]**	**Yang et al. [28]**	**Jiang et al. [29]**
Technology	CRT-based SIS and $(2, n+1)$ RG-VSS	Polynomial-based SIS and $(2,2)$ RG-VSS	Polynomial-based SIS and $(2,2)$ RG-VSS	Polynomial-based SIS and $(2, n+1)$ RG-VSS
Screening criterion	COL	bitwise comparison	bitwise comparison	bitwise comparison
Shadow generating efficiency	high	low	low	low
Recovery computation complexity	$O(k)$	$O(klog^2k)$	$O(klog^2k)$	$O(klog^2k)$
Dealer participatory	No	Yes	Yes	No
Locating dishonest participant	Yes	No	No	No

7. Conclusions

In this paper, we proposed a verifiable SIS scheme combining (k,n) threshold CRT-based SIS and $(2,n+1)$ threshold VSS. In our scheme, a binary authentication image with the same size as the secret image was divided into $n+1$ binary shadows through $(2,n+1)$ threshold VSS. The first n binary shadows were used to guide the CRT-based SIS and the $(n+1)$-th binary shadow was distributed to dealer to verify the authenticity of secret shadows. When there is no dealer involved, participants verify identities of others mutually. The main contributions of this paper can be summarized as two points. First, compared with the schemes proposed by Yan et al, our scheme utilizes the uncertainty of the bits used for screening to realize not only the detection of fake participants, but also the location of dishonest participants when there is a dealer involved. Sencond, loose screening criterion and efficient encoding and decoding rate of CRT-based SIS guarantee high-efficiency shadows generation and low recovery computation complexity. In addition, our scheme has the advantages of lossless recovery, no pixel expansion and 100% detection rate. We will pay attention to future work as following. First, the theoretical analysis of the leakage of the binary authentication image in secret shadows for $k=2$. Second, the security analysis of the CRT-based SIS to resist to the side channel attack(SCA) mentioned in [34].

Acknowledgements

This work is funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (Number: 61602491).

Conflict of interest

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

1. Y. Luo, X. Ouyang, J. Liu, L. Cao, An image encryption method based on elliptic curve elgamal encryption and chaotic systems, *IEEE Access*, **7** (2019), 38507–38522.
2. G. Ye, K. Jiao, H. Wu, C. Pan, X. Huang, An asymmetric image encryption algorithm based on a fractional-order chaotic system and the rsa public-key cryptosystem, *Int. J. Bifurcation Chaos*, **30** (2020), 2050233.
3. Q. Su, G. Wang, S. Jia, X. Zhang, Q. Liu, X. Liu, Embedding color image watermark in color image based on two-level DCT, *Signal, Image Video Process.*, **9** (2015), 991–1007.
4. N. M. Makbol, B. E. Khoo, T. H. Rassem, Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics, *IET Image process.*, **10** (2016), 34–52.
5. N. R. Zhou, A. W. Luo, W. P. Zou, Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm, *Multimedia Tools Appl.*, **78** (2019), 2507–2523.
6. N. R. Zhou, A. W. Luo, W. P. Zou, Compressed sensing, *IEEE Trans. Inf. Theory*, **52** (2006), 1289–1306.
7. E. J. Candes, J. Romberg, T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, *IEEE Trans. Inf. Theory*, **52** (2006), 489–509.
8. G. Ye, C. Pan, Y. Dong, K. Jiao, X. Huang, A novel multi-image visually meaningful encryption algorithm, based on compressive sensing and Schur decomposition, *Trans. Emerg. Telecommun. Technol.*, **32** (2021), e4071.
9. G. R. Blakley, Safeguarding cryptographic keys, in *1979 International Workshop on Managing Requirements Knowledge (MARK)*, (1979), 313–318.
10. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.
11. A. Gutub, N. Al-Juaid, E. Khan, Counting-based secret sharing technique for multimedia applications, *Multimedia Tools Appl.*, **78** (2019), 5591–5619.
12. M. Al-Ghamdi, M. Al-Ghamdi, A. Gutub, Security enhancement of shares generation process for multimedia counting-based secret-sharing technique, *Multimedia Tools Appl.*, **78** (2019), 16283–16310.

13. A. Gutub, M. Al-Ghamdi, Image based steganography to facilitate improving counting-based secret sharing, *3D Res.*, **10** (2019), 6.

14. A. Gutub, M. Al-Ghamdi, Hiding shares by multimedia image steganography for optimized counting-based secret sharing, *Multimedia Tools Appl.*, **79** (2020), 1–35.

15. M. Naor, A. Shamir, Visual cryptography, in *Workshop on the Theory and Application of of Cryptographic Techniques*, (1994), 1–12.

16. C. C. Thien, J. C. Lin, Secret image sharing, *Comput. Graphics*, **26** (2002), 765–770.

17. X. Yan, Y. Lu, L. Liu, S. Wan, H. Liu, Chinese remainder theorem-based secret image sharing for (k, n) threshold, in *Cloud Computing and Security*, Springer, **10603** (2017), 433–440.

18. X. Yan, Y. Lu, L. Liu, X. Song, Reversible image secret sharing, *IEEE Trans. Inf. Forensics Secur.*, **15** (2020), 3848–3858.

19. B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, in *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science 1985*, (1985), 383–395.

20. P. Li, P. Ma, X. Su, Image secret sharing and hiding with authentication, in *2010 First International Conference on Pervasive Computing, Signal Processing and Applications*, (2010), 367–370.

21. G. Ulutas, M. Ulutas, V. V. Nabiyev, Secret image sharing scheme with adaptive authentication strength, *Pattern Recognit. Lett.*, **34** (2013), 283–291.

22. C. C. Lin, W. H. Tsai, Secret image sharing with steganography and authentication, *J. Syst. Software*, **73** (2004), 405–414.

23. C. C. Chang, Y. P. Hsieh, C. H. Lin, Sharing secrets in stego images with authentication, *Pattern Recognit.*, **41** (2008), 3130–3137.

24. M. T. Parvez, A. Gutub, Vibrant color image steganography using channel differences and secret data distribution, *Kuwait J. Sci. Eng.*, **38** (2011), 127–142.

25. Y. Liu, C. C. Chang, A turtle shell-based visual secret sharing scheme with reversibility and authentication, *Multimedia Tools Appl.*, **77** (2018), 25295–25310.

26. A. Gutub, K. Alaseri, Hiding shares of counting-based secret sharing via Arabic text steganography for personal usage, *Arabian J. Sci. Eng.*, **45** (2019), 2433–2458.

27. X. Yan, Q. Gong, L. Li, G. Yang, Y. Lu, J. Li, Secret image sharing with separate shadow authentication ability, *Signal Process. Image Commun.*, **82** (2020), 115721.

28. G. Yang, L. Liu, X. Yan, A compressed secret image sharing method with shadow image verification capability, *Math. Biosci. Eng.*, **17** (2020), 4295–4316.

29. Y. Jiang, X. Yan, J. Qi, Y. Lu, X. Zhou, Secret Image Sharing with Dealer-Participatory and Non-Dealer-Participatory Mutual Shadow Authentication Capabilities, *Mathematics*, **8** (2020), 234.

30. X. Yan, Y. Lu, C. N. Yang, X. Zhang, S. Wang, A Common method of share authentication in image secret sharing, *IEEE Trans. Circuits Syst. Video Technol.*, (2020), 1–1.

31. S. M. Yen, S. Kim, S. Lim, S. J. Moon, RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis, *IEEE Trans. Comput.*, **52** (2003), 461–472.

32. W. Wang, X. G. Xia, A closed-form robust Chinese remainder theorem and its performance analysis, *IEEE Trans. Signal Process.*, **58** (2010), 5655–5666.
33. C. Li, Y. Liu, L. Y. Zhang, K. W. Wong, Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem, *Signal Process. Image Commun.*, **29** (2014), 914–920.
34. K. Okeya, T. Takagi, Security analysis of CRT-based cryptosystems, in *International Conference on Applied Cryptography and Network Security*, (2004), 383–397.
35. X. Yan, X. Liu, C. N. Yang, An enhanced threshold visual secret sharing based on random grids, *J. Real-Time Image Process.*, **14** (2018), 61–73.

AIMS Press