IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 10, 2019, accepted August 18, 2019, date of publication August 22, 2019, date of current version September 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2936824

A Secret Image Restoring Scheme Using Threshold Pairs of Unordered Image Shares

XIAOPING LI[1], YANJUN LIU[2], HEFENG CHEN[3], AND CHIN-CHEN CHANG[2], (Fellow, IEEE)

[1]School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu 610054, China
[2]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan
[3]Computer Engineering College, Jimei University, Xiamen 361021, China

Corresponding author: Yanjun Liu (yjliu104@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61701086, in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2016KYQD143, in part by the Natural Science Foundation of Fujian Province under Grant 2017J01761 and Grant 2018J01537, and in part by the Project of Ministry of Science and Technology of Taiwan under Grant MOST 106-2221-E-035-013-MY3.

ABSTRACT Secret image sharing has been widely used in numerous areas such as remote sensing and information security. The goal is to share and recover one or more images using several image shares. However, most schemes only consider ordered shares. In addition, the dependency between the images and the share is determined, that is, which image the share belongs to is determined. In this paper, by using the generalized Chinese remainder theorem method, we propose a secret image sharing scheme using threshold pairs of unordered image shares, where t out of n share pairs are needed to recover the original secret images, even if the affiliation between the shares and the images is disturbed. Compared with existing schemes, the proposed sharing algorithm is more secure and the recovery algorithm is more effective. Moreover, the conditions for the success or failure of recovering two images from their unordered shares are obtained. Simulations are also presented to show the efficiency of the proposed algorithms.

INDEX TERMS Secret image sharing, recovery, unordered share, Chinese remainder theorem (CRT), generalized CRT.

I. INTRODUCTION

In recent years, the rapid advances in network bandwidth and covert communication have promoted the development of secure transmission for digital images. The confidentiality of images can be achieved through traditional encryption. However, if a secret image is held by only one person without additional copies, there is a risk that it will be impossible to reconstruct the image successfully if it becomes lossy due to the transmission over open channels such as the Internet. Secret image sharing (SIS), with its robustness to losses, has been proposed. In SIS schemes, the secret image is converted into several shares, and it is reconstructible as long as sufficient shares are given.

SIS is developed based on the concept of secret sharing (SS). The (t, n) threshold SS schemes based on polynomial interpolation and geometry were firstly presented by Shamir [1] and Blakley [2] in 1979 independently. The basic idea of SS is to protect the privacy of information by distribution. In a (t, n) secret sharing scheme for $t \leq n$, a secret is divided into n shares such that any t or more shares can be used to reconstruct the secret, whereas any $t-1$ or fewer shares cannot. There are other types of SS, e.g., McEliece-Sarwate's scheme [3], which is based on Reed-Solomon codes; Mignotte's scheme [4]; and Asmuth-Bloom's scheme [5], which are based on the Chinese remainder theorem (CRT).

Inspired by the principle of SS, an SIS scheme generates several shares from a secret image without information leakage, and the secret image can be recovered through partial shares. There are many types of SIS techniques, among which the two most important are the visual cryptography scheme (VCS) and polynomial-based SIS [6]. VCS was the first SIS scheme introduced by Naor and Shamir [7] in 1994. VCS has the unique ability to restore secret information by stacking image shares such that humans can easily identify secret information visually and without any computations. However, because it is implemented based on OR operations, there are certain drawbacks such as pixel expansion and

The associate editor coordinating the review of this article and approving it for publication was Ke Gu.

poor visual quality of the recovered images. Later, grid-based VCS [8]–[10] and probabilistic VCS [11] were proposed to improve the performance of VCS. Derived from Shamir's (t, n) SS, polynomial-based SIS was first introduced by Thien and Lin [12] in 2002, which can reconstruct the secret image with high visual quality. That method encrypts the secret by generating a $t-1$ degree polynomial with t coefficients from t pixel values, and later, the secret can be recovered by Lagrange interpolation. Subsequent works studied the inevitable security problem whereby fewer than t shares might reveal the secret information. Therefore, some technologies for remedying the above-mentioned security problem, such as permutation [13], encryption [14], and compression [15], have been utilized in advance of sharing. Compared to Shamir's polynomial-based SS using Lagrange interpolation as a fundamental step in the reconstruction algorithm, the CRT-based SS has attracted more attention due to its low computational complexity. Hua and Liao [16] proposed an SIS scheme that combined Mignotte's approach with arithmetic compression coding based on a piecewise linear chaotic map to solve the pixel expansion problem; however, it necessitates auxiliary encryption. Yan *et al.* [17] proposed another SIS scheme for lossless recovery without auxiliary encryption based on Asmuth Bloom's approach by dividing the gray image pixel values into two available mapping intervals.

If an SIS scheme can divide multiple secret images rather than a single image into a number of shares [18], [19], it is called multi-image SIS. Multi-image SIS is the generalization of single-image SIS, and it is more efficient and applied in a wider range of applications in numerous research areas, such as military imaging systems and remote sensing. Chang *et al.* [20] proposed a multi-image SIS based on the CRT and Lagrange interpolation. Kabirirad and Eslami [21] proposed a high-performance (t, n) multi-image SIS based on Boolean operations, where $2 < t < n$, and only one secret is recovered in each stage. However, they are based on the assumption that all the shares are errorless and that the shares are obtained in an ordered manner for some given moduli.

All the aforementioned works only consider the shares in order. In addition, the correspondences between secret images and their shares are determined. In this paper, we consider the problem of a (t, n) SIS scheme using unordered pairs of image shares, and all secret images are reconstructed simultaneously. A generalized CRT based SIS scheme is proposed to share and recover two secret images from their unordered share pairs. For the sharing algorithm, the pixels of two images in the same position are kept secret simultaneously and then shared by the modular operation. For the recovery algorithm, the problem is modeled as a generalized CRT, where two secret images are reconstructed simultaneously from their unordered shares. This type of generalized CRT was first studied in [22] and later developed independently in [23], [24]. Compared with existing schemes, the proposed sharing algorithm is more secure, and the recovery algorithm is more effective.

The remainder of the paper is organized as follows. In Section II, we introduce the problem of CRT based image sharing. Sections III and IV present the sharing and recovery algorithms of the proposed generalized CRT based SIS, respectively. In Section V, we give simulation results obtained under the proposed approach. Section VI concludes this paper. For the convenience of the reader, some commonly used acronyms and notations are listed in Table 1.

TABLE 1. Acronyms and notations.

SS:	secret sharing
SIS:	secret image sharing
VCS:	visual cryptography scheme
CRT:	Chinese remainder theorem
$\mathcal{M}$:	a set of moduli $\{m_1, m_2, \ldots, m_n\}$
$D(\mathcal{M})$:	the largest dynamic range of $\mathcal{M}$

II. CHINESE REMAINDER THEOREM BASED IMAGE SHARING

CRT [4] tells us that an unknown integer can be uniquely recovered from its remainders modulo some pairwise coprime positive moduli if and only if the integer is less than the least common multiple (LCM) of these moduli. Let the unknown integer be x and the pairwise coprime moduli be $m_1, m_2, \ldots, m_n$. The remainders of x modulo $m_1, m_2, \ldots, m_n$ are $r_1, r_2, \ldots, r_n$, respectively. In other words, the unknown integer x satisfies

$$\begin{cases} x \equiv r_1 \bmod m_1 \\ x \equiv r_2 \bmod m_2 \\ \cdots \\ x \equiv r_n \bmod m_n. \end{cases} \tag{1}$$

According to the CRT, x can be reconstructed by the following formula:

$$x \equiv \sum_{i=1}^{n} M_i \overline{M}_i r_i \bmod M, \tag{2}$$

where $M = m_1 m_2 \ldots m_n$, $M_i = M/m_i$, and $\overline{M}_i$ satisfies $M_i \overline{M}_i \equiv 1 \bmod m_i$ for $i = 1, 2, \ldots, n$.

It makes sense that CRT can be used in SS for confidential information transmissions, where the unknown integer x in (1) can be viewed as the secret, and its remainders $r_1, r_2, \ldots, r_n$ with moduli $m_1, m_2, \ldots, m_n$ can be viewed as n shares for the shareholders, respectively. This CRT based SS scheme was proposed in [4] and well studied in [5]. Next, we will briefly recall the basic idea of two well-known CRT based SS schemes, i.e., Mignotte's sharing scheme [4] and Asmuth-Bloom's sharing scheme [5]. For convenience, the remainder of the x modulo y is denoted as $\langle x \rangle_y$.

A. MIGNOTTE'S SHARING SCHEME

Without loss of generality, we suppose that the moduli m_i satisfy $1 < m_1 < m_2 < \cdots < m_n$. Let the threshold be t $(1 < t < n)$ and satisfy

$$m_{n-t+2}m_{n-t+3}\cdots m_n < m_1m_2\cdots m_t. \tag{3}$$

Then, a (t, n)-threshold Mignotte's sharing scheme contains three main steps, described below [4].

1) Determine the range of a uniquely recovered secret s as

$$s \in (m_{n-t+2}m_{n-t+3}m_n,\ m_1m_2\cdots m_t). \tag{4}$$

2) Obtain n shares r_i by

$$s \equiv r_i \bmod m_i, \quad i = 1, 2, \ldots, n. \tag{5}$$

3) Recover the secret s by using the CRT with at least t distinct shares.

In this scheme, the share r_i of the i-th shareholder can be obtained directly, which leads to the imperfectness for SS. To overcome this drawback, Asmuth-Bloom's sharing scheme was proposed and is briefly described below.

B. ASMUTH-BLOOM'S SHARING SCHEME

The main idea of this scheme is to obtain a pseudo random share in a finite range by the modular operation. The sharing process contains the following four steps.

1) Determine a positive integer m_0 satisfying

$$m_0m_{n-t+2}m_{n-t+3}\cdots m_n < m_1m_2\cdots m_t. \tag{6}$$

2) Determine the range of the secret $s \in (0,\ m_0)$.

3) Choose an arbitrary integer α satisfying

$$x = s + \alpha m_0 \in (m_{n-t+2}m_{n-t+3}\cdots m_n, m_1m_2\cdots m_t). \tag{7}$$

4) Obtain n shares by

$$x \equiv r_i \bmod m_i, \quad i = 1, 2, \ldots, n. \tag{8}$$

Clearly, the i-th share is

$$r_i = \langle x \rangle_{m_i} = \langle s + \alpha m_0 \rangle_{m_i}, \tag{9}$$

which is different from the $\langle s \rangle_{m_i}$ obtained by Mignotte's sharing scheme. Hence, the information of the secret is not leaked. In other words, Asmuth-Bloom's sharing scheme is perfect.

The recovery of the secret s contains two steps. First, we reconstruct x by using the CRT through at least t distinct shares. Then, the secret s can be recovered by

$$x \equiv s \bmod m_0. \tag{10}$$

Obviously, the SS schemes discussed above can be applied in the image domain, where the pixels of the image are viewed as basic elements of the secret image to be shared. Suppose a secret image A with P pixels, p_i for $i = 1, 2, \ldots, P$, is split into n image shares, $A_1, A_2, \ldots, A_n$, distributed among n shareholders using Asmuth-Bloom's sharing scheme. Each share, A_j, for $j = 1, 2, \ldots, n$, is composed of P pixels $a_{i,j}$ such that

$$p_i \equiv a_{i,j} \bmod m_j, \quad i = 1, 2, \ldots, P. \tag{11}$$

When there is no confusion, we also denote the share A_j as a matrix as

$$A_j = (a_{i,j})_{P\times 1}. \tag{12}$$

As shown in Fig. 1, we choose the 512×512 "Lena" image as image A and illustrate its five shares with moduli 247, 251, 253, 254 and 255. Clearly, each of the shares is meaningless in that no information about A will be revealed.

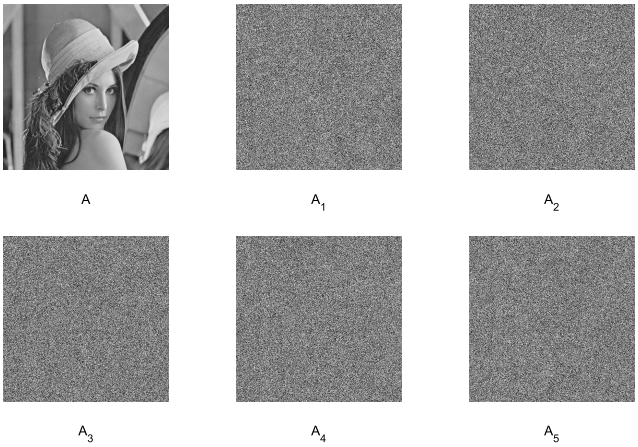


FIGURE 1. Image "Lena" and its five shares.

Now, we consider the recovery of the secret image. Suppose that the image can be successfully recovered from any t shares. The recovery process contains two main steps. First, each pixel p_i should be properly reconstructed from any t remainders $a_{i,j}$ using Asmuth-Bloom's method. Then, the image is recovered successfully after all the pixels are assembled. This (t, n) SIS is for a single image, and we will consider a (t, n) SIS for two images in the next section.

III. GENERALIZED CRT BASED SECRET IMAGE SHARING

In this section, we first introduce the problem of sharing two images simultaneously. Then, we briefly recall the basic idea of the generalized CRT and present some results. Finally, the SIS algorithm based on the generalized CRT is proposed.

A. TWO-IMAGE SHARING PROBLEM

Let us consider the recovery of two images A and B from their corresponding shares simultaneously. Similar to image A, image B is divided into n image shares: $B_1, B_2, \ldots, B_n$. Assume that the pixel in B is denoted as q_i and that the share B_j for $j = 1, 2, \ldots, n$ consists of P pixels $b_{i,j}$ such that

$$q_i \equiv b_{i,j} \bmod m_j, \quad i = 1, 2, \ldots, P. \tag{13}$$

Consequently, the matrix of B_j is

$$B_j = (b_{i,j})_{P\times 1}. \tag{14}$$

Additionally, we suppose that image B can be successfully recovered from any t shares. In Fig. 2, the "Zelda" image with a size of 512×512, is selected as image B. Five shares, B_1, B_2, B_3, B_4 and B_5 are generated by moduli 247, 251, 253, 254 and 255, respectively. Now, we discuss how to restore A and B simultaneously from two groups of shares with t shares each.

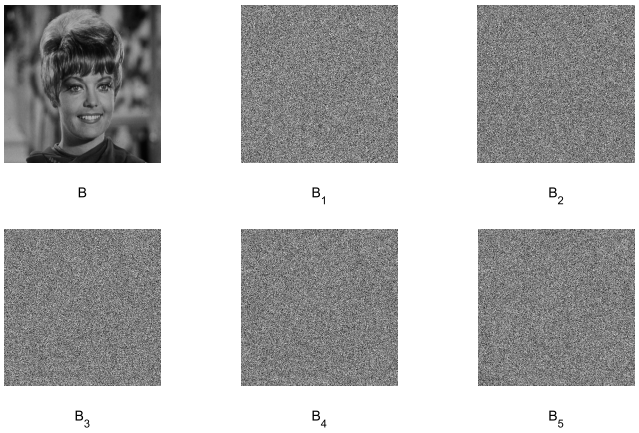


FIGURE 2. Image "Zelda" and its five shares.

Suppose that two groups of image shares are

$$I : A_1, A_2, \ldots, A_n \tag{15}$$

and

$$II : B_1, B_2, \ldots, B_n \tag{16}$$

for images A and B, respectively. This is referred to as a proper correspondence between an image and its share group such that all the shares in group I correspond to image A and those in group II correspond to image B. Here, $\{A_i, B_i\}$ is called a share pair. Clearly, the two images can be separately recovered from their t shares in I and II, respectively. However, we will explain below that it is difficult to recover them due to an incorrect correspondence when some shares of the two groups are exchanged. In what follows, the exchanged image shares are called unordered shares.

As shown in Fig. 3, the two images, A and B, are divided into five shares, $A_1, A_2, \ldots, A_5$, by (12) and $B_1, B_2, \ldots, B_5$ by (14), respectively. We want to recover A and B from

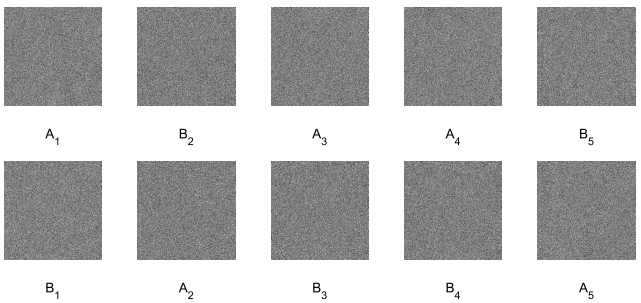


FIGURE 3. Unordered shares of "Lena" and "Zelda".

any three share pairs. However, there exists an incorrect correspondence whereby A_2 and B_2 are exchanged in the share pair $\{A_2, B_2\}$, and A_5 and B_5 are exchanged in $\{A_5, B_5\}$. In detail, for the first group, the shares are A_1, B_2, A_3, A_4, B_5; for the second group, the shares are B_1, A_2, B_3, B_4, A_5. The moduli for pairs of shares are $m_1, m_2, \ldots, m_5$.

Given three shares A_1, B_2, and A_3 of the first group and B_1, A_2, and B_3 of the second group, by using the CRT method, we obtain recoveries for A and B shown in Fig. 4. This implies that it fails to reconstruct both of the original images using unordered shares by the CRT, and hence, the CRT is ineffective for this type of problem.

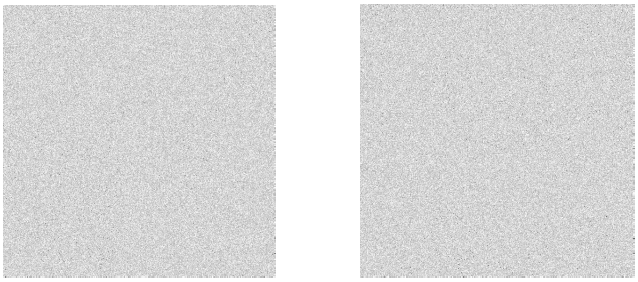


FIGURE 4. Recovered images by the CRT.

The two-image sharing and recovering problem can be modeled as a generalized CRT. For better understanding, we first introduce some notations. The pixels of the two images A and B are denoted as p_i and q_i, respectively, where $i = 1, 2, \ldots, P$. Given n image shares $A_1, A_2, \ldots, A_n$ for A, and the i-th pixel of the share A_j for $j = 1, 2, \ldots, n$ is denoted as $a_{i,j}$. Similarly, there are n image shares $B_1, B_2, \ldots, B_n$ for B, and the i-th pixel of the share B_j for $j = 1, 2, \ldots, n$ is denoted as $b_{i,j}$. Hence, the recovery of A from A_1, B_2, A_3 and B from B_1, A_2, B_3 means to reconstruct all the pixels p_i of A and q_i of B from the pixels $a_{i,1}, b_{i,2}, a_{i,3}$ and $b_{i,1}, a_{i,2}, b_{i,3}$, respectively. Without considering the correspondence between a share's pixel and an original image, the problem is to determine $\{p_i, q_i\}$ from their pixel pairs $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$ and $\{a_{i,3}, b_{i,3}\}$ of the three shares with moduli m_1, m_2, and m_3, respectively. This can be solved by the generalized CRT, which was first studied in [22] and later developed in [23], [24]. Inspired by these works, in this paper, we apply the generalized CRT to share and recover two images.

B. BASIC IDEA OF GENERALIZED CRT

Now, consider the problem of reconstructing the pixel pair $\{p_i, q_i\}$ from the pixel pairs $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$, $\ldots$, $\{a_{i,n}, b_{i,n}\}$ with moduli $m_1, m_2, \ldots, m_n$, respectively. This problem is equivalent to reconstructing two integers from their residue sets modulo the given moduli. To obtain a unique reconstruction, first, the largest range for the two integers should be determined. For the CRT, this largest range is the

LCM of all the given moduli. However, this conclusion may not be true for the generalized CRT. For example, given three residue sets $\{1, 3\}$, $\{3, 5\}$, and $\{4, 5\}$ with moduli 5, 7, and 11, respectively, if the largest range of the two integers are $\text{lcm}(5, 7, 11) = 385$, then we have four candidates, i.e., $\{26, 38\}$, $\{103, 346\}$, $\{136, 313\}$, and $\{213, 236\}$. Hence, the two integers cannot be uniquely determined under this restriction. To overcome this drawback, the dynamic range that leads to a unique reconstruction was considered. In [23], the largest dynamic range $D(\mathcal{M})$ of moduli $\mathcal{M} = \{m_1, m_2, \ldots, m_n\}$ for two integers was obtained, as shown in Proposition 1 below.

Proposition 1: Let n pairwise coprime integers be $1 < m_1 < m_2 < \cdots < m_n$. If $m_{n-1} \geq 3$, then

$$D(\mathcal{M}) = \min_{I \subseteq \{1,2,\ldots,n\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \bar{I}} m_i \right\}, \tag{17}$$

where $\bar{I}$ is the complement of I in $\{1, 2, \ldots, n\}$.

For more details, the readers are suggested to consult [23], [24].

C. GENERALIZED CRT BASED IMAGE SHARING ALGORITHM

Let $\mathcal{M}$ be the set of moduli $\{m_1, m_2, \ldots, m_n\}$. For a given threshold t, we denote

$$\begin{aligned} \mathcal{M}_1 &= \{m_{n-t+2}, m_{n-t+3}, \ldots, m_n\}, \\ \mathcal{M}_2 &= \{m_1, m_2, \ldots, m_t\}. \end{aligned} \tag{18}$$

Define

$$i_0 \triangleq \min \left\{ i : \prod_{j=i}^{n} m_j < D(\mathcal{M}_2),\ 1 \leq i \leq n \right\}. \tag{19}$$

Then, we can determine

$$D_L = \max \left\{ \prod_{j=i_0}^{n} m_j,\ D(\mathcal{M}_1) \right\}. \tag{20}$$

Select a proper integer m_0 satisfying

$$(m_0, m_j) = 1, \quad j = 1, 2, \ldots, n \tag{21}$$

and

$$m_0\, D_L < D(\mathcal{M}_2). \tag{22}$$

For a pair of pixels p_i and q_i, select two positive integers k_p and k_q satisfying

$$p_i + k_p m_0,\ q_i + k_q m_0 \in (D_L, D(\mathcal{M}_2)), \quad i = 1, 2, \ldots, P. \tag{23}$$

Then, the i-th pixel of the j-th share for the two images can be generated by

$$\{p_i + k_p m_0,\ q_i + k_q m_0\} \equiv \{a_{i,j}, b_{i,j}\} \bmod m_j. \tag{24}$$

Specifically,

$$\{a_{i,j}, b_{i,j}\} = \left\{ \langle p_i + k_p m_0 \rangle_{m_j},\ \langle q_i + k_q m_0 \rangle_{m_j} \right\}. \tag{25}$$

Note that the remainders in each residue set are unordered. According to the generalized CRT, the two pixels $\{a_{i,j}, b_{i,j}\}$ can be reconstructed simultaneously from their unordered residue sets with moduli $m_1, m_2, \ldots, m_n$. Hence, exchanging pixels in A_j and B_j between each other leads to a successful recovery of the two pixels $\{p_i, q_i\}$. Motivated by this, we propose the following image sharing algorithm, where some of pixels in A'_j and B'_j for $j = 1, 2, \ldots, n$ are exchanged between each other, i.e.,

$$A'_j = (a'_{i,j})_{P \times 1}, \quad i = 1, 2, \ldots, P \tag{26}$$

and

$$B'_j = (b'_{i,j})_{P \times 1}, \quad i = 1, 2, \ldots, P \tag{27}$$

with

$$a'_{i,j} \in \{a_{i,j},\ b_{i,j}\},\ b'_{i,j} \in \{a_{i,j}, b_{i,j}\} \setminus \{a'_{i,j}\}. \tag{28}$$

Consequently, we have two groups containing unordered shares

$$I:\ A_1, \ldots, A'_{j_1}, \ldots, A'_{j_v}, \ldots, A_n \tag{29}$$

and

$$II:\ B_1, \ldots, B'_{j_1}, \ldots, B'_{j_v}, \ldots, B_n \tag{30}$$

with moduli $m_1, m_2, \ldots, m_n$, respectively, where $1 \leq j_i \leq n$ and $i = 1, 2, \ldots, v$.

To summarize, we demonstrate the following generalized CRT based (t, n) image sharing algorithm shown in Algorithm 1.

Algorithm 1 : (t, n) Image Sharing Algorithm

Input: Two images A and B, moduli $m_1, m_2, \ldots, m_n$.

Output: Two groups of shares:
$A_1, \ldots, A'_{j_1}, \ldots, A'_{j_v}, \ldots, A_n$; $B_1, \ldots, B'_{j_1}, \ldots, B'_{j_v}, \ldots, B_n$.

1: Compute $D(\mathcal{M}_2)$ and D_L by (17) and (20), respectively.
2: Determine m_0 by (21) and (22).
3: Choose two integers k_p and k_q satisfying (23).
4: **for** $i = 1, 2, \ldots, P, j = 1, 2, \ldots, n$, **do**
5: Calculate $p_i + k_p m_0 \equiv a_{i,j} \bmod m_j$ for image A.
6: Calculate $q_i + k_q m_0 \equiv b_{i,j} \bmod m_j$ for image B.
7: **end for**
8: Obtain n shares $A_1, \ldots, A'_{j_1}, \ldots, A'_{j_v}, \ldots, A_n$ of A, where A'_j are defined in (26).
9: Obtain n shares $B_1, \ldots, B'_{j_1}, \ldots, B'_{j_v}, \ldots, B_n$ of B, where B'_j are defined in (27).

Fig. 5 shows the group of five shares of A and B, containing unordered shares as $A'_2 = B_2, B'_2 = A_2; A'_5 = B_5, B'_5 = A_5$.

IV. IMAGE RECONSTRUCTION

In this section, we give the generalized CRT based image reconstruction. First, we address the image reconstruction algorithm. Then, we discuss the condition for successful reconstruction.

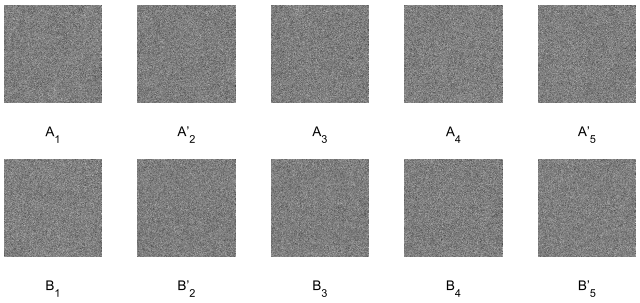


FIGURE 5. Unordered shares of "Lena" (A) and "Zelda" (B).

A. RECONSTRUCTION ALGORITHM

Now, we consider the recovery of the two images from two groups of shares with l shares in each group, i.e.,

$$I:\ A_1,\ldots,A'_{j_1},\ldots,A'_{j_\iota},\ldots,A_l \tag{31}$$

and

$$II:\ B_1,\ldots,B'_{j_1},\ldots,B'_{j_\iota},\ldots,B_l, \tag{32}$$

where $1 \le j_i \le l$ for $i = 1,2,\ldots,\iota$. For convenience, we consider the recovery of two images when $m_0 \ge 256$ in what follows. For the case of $m_0 < 256$, an integral multiple of m_0 should be considered if the pixel is larger than m_0. To explain this more clearly, we give an example for $m_0 = 90$ in Section V.

The process of recovering all the pairs of pixels from the given shares contains two parts. The first part is to determine two pixels $\{\langle x_{i,1}\rangle_{m_0}, \langle x_{i,2}\rangle_{m_0}\}$ from the given shares by using generalized CRT. The latter half is to determine which pixel in $\{\langle x_{i,1}\rangle_{m_0}, \langle x_{i,2}\rangle_{m_0}\}$ belongs to A and which pixel belongs to B. Algorithm 2 gives the (t,n) image reconstruction algorithm, where $m_0 \ge 256$. The two groups of shares are described in (31) and (32), with $l = t$ and $\iota < \lceil \frac{t}{2} \rceil$.

B. CONDITION FOR SUCCESSFUL RECOVERY

Theorem 1: Let the shares of A and B be described in (31) and (32) with moduli $\mathcal{M}' = \{m_1, m_2, \ldots, m_l\}$, respectively. Then, we have the following results.

1) If $l \ge t$ and $\iota < \lceil \frac{t}{2} \rceil$, then two images A and B can be successfully recovered.

2) If $n - i_0 + 1 < l < t$ and $D(\mathcal{M}_2) < \mathrm{lcm}(\mathcal{M}')$, then the probability of successfully recovering the two images is

$$Pr = \frac{1}{2^{lP}}, \tag{33}$$

where i_0 is defined in (19), P is the total number of pixels, and the pixels of A_i and B_i in the same position are distinct.

3) If $l \le n - i_0 + 1$, then the two images A and B cannot be recovered.

proof: 1) Since $l \ge t$, we have

$$\mathcal{M}_2 \subseteq \mathcal{M}'.$$

Hence,

$$D(\mathcal{M}') > D(\mathcal{M}_2).$$

Algorithm 2 : Reconstruction Algorithm

Input: Two groups of shares $A_1,\ldots,A'_{j_1},\ldots,A'_{j_\iota},\ldots,A_n$; $B_1,\ldots,B'_{j_1},\ldots,B'_{j_\iota},\ldots,B_n$.

Output: Two images A and B.

1: Compute $c_{i,j} = \langle a_{i,j} + b_{i,j}\rangle_{m_j}$ for $j = 1,2,\ldots,t$.

2: Compute $M = m_1 m_2 \cdots m_t$, $M_j = M/m_j$, and $\overline{M}_j$ satisfying $M_j\overline{M}_j \equiv 1 \bmod m_j$.

3: Compute $\xi_{i,1} = \left\langle \sum_{j=1}^{n} M_j\overline{M}_j c_{i,j} \right\rangle_M$.

4: Let $\tau_i = \max\{0, \lceil \xi_{i,1} - 2\sqrt{M} \rceil\}$. Then compute $\xi_{i,2}$:

$$\xi_{i,2} = \left\langle \sum_{j=1}^{t} M_j\overline{M}_j(a_{i,j} - \tau_i)(b_{i,j} - \tau_i) \right\rangle_M.$$

5: Solve $(x-\tau_i)^2 - (\xi_{i,1} - 2\tau_i)(x-\tau_i) + \xi_{i,2} = 0$ and obtain two solutions $\{x_{i,1}, x_{i,2}\}$.

6: Compute $\{p_i, q_i\} = \{\langle x_{i,1}\rangle_{m_0}, \langle x_{i,2}\rangle_{m_0}\}$.

7: For $j = 1,2,\ldots,n$, determine $e_{i,j}$:

$$e_{i,j} \triangleq \begin{cases} 1, & \text{if } \langle \langle x_{i,1}\rangle_{m_0}\rangle_{m_j} = b_{i,j} \\ 0, & \text{otherwise.} \end{cases}$$

8: Determine p_i by

$$p_i = \begin{cases} x_{i,1}, & \text{if } \sum_{j=1}^{n} e_{i,j} < \left\lceil \frac{n}{2} \right\rceil, \\ x_{i,2}, & \text{otherwise.} \end{cases}$$

9: Determine q_i by

$$q_i \in \{\langle x_{i,1}\rangle_{m_0}, \langle x_{i,2}\rangle_{m_0}\} \setminus \{p_i\}.$$

10: Recover the two images A and B after all the pixels p_i's and q_i's are determined.

By (23), we have

$$D(\mathcal{M}_2) > \max\{p_i + k_p m_0,\ q_i + k_q m_0\},$$

which leads to

$$D(\mathcal{M}') > \max\{p_i + k_p m_0,\ q_i + k_q m_0\}.$$

By the generalized CRT, we can reconstruct $\{p_i + k_p m_0, q_i + k_q m_0\}$ from their shares $\{a_{i,1}, b_{i,1}\}, \{a_{i,2}, b_{i,2}\}, \ldots, \{a_{i,l}, b_{i,l}\}$. Let the two reconstructions be $\{x_{i,1}, x_{i,2}\}$. Specifically,

$$\{p_i + k_p m_0,\ q_i + k_q m_0\} = \{x_{i,1}, x_{i,2}\}.$$

Consequently,

$$\{\langle p_i + k_p m_0\rangle_{m_0},\ \langle q_i + k_q m_0\rangle_{m_0}\} = \{\langle x_{i,1}\rangle_{m_0},\ \langle x_{i,2}\rangle_{m_0}\}.$$

Hence,

$$\{p_i, q_i\} = \left\{\langle x_{i,1}\rangle_{m_0},\ \langle x_{i,2}\rangle_{m_0}\right\}.$$

Note that the two pixels $\{p_i, q_i\}$ are determined simultaneously, i.e., the two pixels are $\left\{\langle x_{i,1}\rangle_{m_0},\ \langle x_{i,2}\rangle_{m_0}\right\}$. We have two possible results:

$$p_i = \langle x_{i,1}\rangle_{m_0}, \quad q_i = \langle x_{i,2}\rangle_{m_0}$$

and

$$p_i = \langle x_{i,2}\rangle_{m_0}, \quad q_i = \langle x_{i,1}\rangle_{m_0}.$$

Next, we give an effective method to determine the two pixels.

Case I: $\langle x_{i,1}\rangle_{m_0} = \langle x_{i,2}\rangle_{m_0}$.

In this case, $p_i = q_i$. Hence,

$$p_i = q_i = \langle x_{i,1}\rangle_{m_0} = \langle x_{i,2}\rangle_{m_0}. \tag{34}$$

Case II: $\langle x_{i,1}\rangle_{m_0} \neq \langle x_{i,2}\rangle_{m_0}$.

In this case, $p_i \neq q_i$. To determine the two pixels p_i and q_i from the obtained set $\{x_{i,1}, x_{i,2}\}$, we introduce a double-value function $e_{i,j}$ as

$$e_{i,j} \triangleq \begin{cases} 1, & \text{if } \left\langle \langle x_{i,1}\rangle_{m_0}\right\rangle_{m_j} = b_{i,j} \\ 0, & \text{otherwise,} \end{cases} \tag{35}$$

where $j = 1, 2, \ldots, n$. Then, we have two subcases below.

① $p_i = \langle x_{i,1}\rangle_{m_0}$ and $q_i = \langle x_{i,2}\rangle_{m_0}$.

It follows from (31) that

$$e_{i,j} = \begin{cases} 1, & \text{if } j \in \{j_1, j_2, \ldots, j_\iota\} \\ 0, & \text{otherwise.} \end{cases} \tag{36}$$

Hence,

$$\sum_{j=1}^{t} e_{i,j} = \iota < \left\lceil \frac{t}{2} \right\rceil. \tag{37}$$

From (32), we have

$$e_{i,j} = \begin{cases} 0, & \text{if } j \in \{j_1, j_2, \ldots, j_\iota\} \\ 1, & \text{otherwise.} \end{cases} \tag{38}$$

Hence,

$$\sum_{j=1}^{t} e_{i,j} = t - \iota > t - \left\lceil \frac{t}{2} \right\rceil. \tag{39}$$

② $q_i = \langle x_{i,1}\rangle_{m_0}$ and $p_i = \langle x_{i,2}\rangle_{m_0}$.

From (29), we can obtain (38) and consequently (39).

From (30), we can obtain (36) and consequently (37).

Thus, the two pixels can be correctly determined from the two reconstructions $\{\langle x_{i,1}\rangle_{m_0},\ \langle x_{i,2}\rangle_{m_0}\}$ by the shares (29) or (30). We explain this below.

Suppose that we consider the group of shares described in (29). If (37) holds, then we have $p_i = \langle x_{i,1}\rangle_{m_0}$ and $q_i = \langle x_{i,2}\rangle_{m_0}$; if (39) holds, then we have $q_i = \langle x_{i,1}\rangle_{m_0}$ and $p_i = \langle x_{i,2}\rangle_{m_0}$.

Suppose that we consider the group of shares described in (30). If (39) holds, then we have $p_i = \langle x_{i,1}\rangle_{m_0}$ and $q_i = \langle x_{i,2}\rangle_{m_0}$; if (37) holds, then we have $q_i = \langle x_{i,1}\rangle_{m_0}$ and $p_i = \langle x_{i,2}\rangle_{m_0}$.

Therefore, p_i and q_i of the images A and B can be correctly determined, respectively. After all the pixels p_i and q_i are determined, the two images can be successfully recovered.

2) In this case, $D(\mathcal{M}') < D(\mathcal{M}_1)$. By (20), we have

$$D(\mathcal{M}_1) \leq D_L.$$

Hence,

$$D(\mathcal{M}') < D_L.$$

According to (23), we obtain

$$D(\mathcal{M}') < \min\{p_i + k_p m_0, q_i + k_q m_0\}.$$

Hence, $\{p_i + k_p m_0, q_i + k_q m_0\}$ cannot be reconstructed simultaneously in the range of $(0, D(\mathcal{M}'))$.

Fortunately, we can analyze the recovery probability of the two secrets in $(0, \text{lcm}(\mathcal{M}'))$ using the CRT. According to (25), we have l pairs: $\{a_{i,1}, b_{i,1}\}, \{a_{i,2}, b_{i,2}\}, \ldots, \{a_{i,l}, b_{i,l}\}$. Since $D(\mathcal{M}_2) < \text{lcm}(\mathcal{M}')$, we have

$$\max\{p_i + k_p m_0,\ q_i + k_q m_0\} < \text{lcm}(\mathcal{M}'). \tag{40}$$

Hence, the two secrets $p_i + k_p m_0$ and $q_i + k_q m_0$ can be reconstructed separately using the CRT when the remainders of the residue sets are properly ordered, i.e.,

$$a_{i,1}, a_{i,2}, \ldots, a_{i,l} \tag{41}$$

and

$$b_{i,1}, b_{i,2}, \ldots, b_{i,l}. \tag{42}$$

Because the pixels of A_i and B_i in the same position are distinct, we have the probability of successfully recovering p_i and q_i

$$Pr = \frac{1}{2^l}. \tag{43}$$

Note that the two images can be successfully recovered if and only if all the pixels p_i and q_i of A and B are correctly determined, respectively. Hence, the probability of successful recovery of the two images is

$$Pr = \frac{1}{2^{lP}}. \tag{44}$$

3) We consider the case of $n - i_0 + 1$ shares with moduli $\mathcal{M} = \{m_{i_1}, m_{i_2}, \ldots, m_{i_{n-i_0+1}}\}$. According to the definition of i_0 in (19), we have

$$\prod_{j=1}^{n-i_0+1} m_{i_j} \leq \prod_{i=i_0}^{n} m_i. \tag{45}$$

Note that $\text{lcm}(\mathcal{M}) \leq \prod_{j=1}^{n-i_0+1} m_{i_j}$. Hence,

$$\text{lcm}(\mathcal{M}) \leq \prod_{i=i_0}^{n} m_i. \tag{46}$$

If $D(\mathcal{M}_1) \geq \prod_{i=i_0}^{n} m_i$, then we obtain from (20) that $D_L = D(\mathcal{M}_1)$. From (46), we have

$$\text{lcm}(\mathcal{M}) \leq D(\mathcal{M}_1) = D_L. \tag{47}$$

By (23), we have

$$\text{lcm}(\mathcal{M}) < \min\{p_i + k_p m_0,\ q_i + k_q m_0\}.$$

If $D(\mathcal{M}_1) < \prod_{i=i_0}^{n} m_i$, then we obtain from (20) that $D_L = \prod_{i=i_0}^{n} m_i$. From (46), we have

$$\text{lcm}(\mathcal{M}) \leq D_L.$$

By (23), we have

$$\text{lcm}(\mathcal{M}) < \min\{p_i + k_p m_0, q_i + k_q m_0\}. \tag{48}$$

Thus, the two secrets $\{p_i + k_p m_0, q_i + k_q m_0\}$ cannot be reconstructed from $n - i_0 + 1$ with moduli $\mathcal{M}$. Therefore, the two pixels $\{p_i, q_i\}$ and the two images cannot be successfully recovered. For the case of fewer than $n - i_0 + 1$ shares, the proof is obvious and is thus omitted here.

V. SIMULATION RESULTS

In this section, we perform some simulations to verify the efficiency of the proposed generalized CRT based method. In the simulations, $\mathcal{M} = \{247, 251, 253, 254, 255\}$, and $t = 3$. According to (18), we have $\mathcal{M}_1 = \{254, 255\}$ and $\mathcal{M}_2 = \{247, 251, 253\}$. By (17), we obtain $D(\mathcal{M}_1) = 509$ and $D(\mathcal{M}_2) = 62250$. According to (20), we have $i_0 = 5$. Hence, $D_L = 509$. By (22), we have

$$m_0 < \frac{D(\mathcal{M}_2)}{D_L} \approx 122.3 < 256. \tag{49}$$

In the simulations, we set $m_0 = 90$. For the pixels of A, an arbitrary positive integer k_p in (23) is chosen by

$$k_p \in \begin{cases} [1, 40], & \text{if } p_i \in [0, 90] \\ [41, 80], & \text{if } p_i \in [91, 180] \\ [81, 120], & \text{if } p_i \in [181, 255]. \end{cases} \tag{50}$$

For the pixels of B, an arbitrary positive integer k_q is chosen as the same as k_p. After two arbitrary integers k_p and k_q are chosen, all the pixels of the shares can be determined by Steps 5 and 6 in Algorithm 1. Fig. 5 gives two groups of shares for images A and B with moduli $\mathcal{M}$ when the ranges of k_p and k_q are known. If the ranges of k_p and k_q are unknown, the process of recovering $\{p_i, q_i\}$ will become even more difficult because p_i and q_i cannot be uniquely determined.

To recover the two images from any t shares, all the pairs of pixels $\{p_i, q_i\}$ should be reconstructed by Algorithm 2. In the reconstruction process, unknown multiples of m_0 should be determined. For convenience, we denote

$$\begin{aligned} I_1 &= [m_0, 90 + 40m_0], \\ I_2 &= [91 + 41m_0, 180 + 80m_0], \\ I_3 &= [181 + 81m_0, 255 + 120m_0]. \end{aligned} \tag{51}$$

Then, unknown multiples of m_0 and consequently the two pixels $\{p_i, q_i\}$ can be determined by (52), as shown at the bottom of this page. To illustrate this, we consider an example. Let $p_1 = 89$ of image A and $p_2 = 95$ of image B. According to (50), we can choose two positive integers $k_p = 35$ and $k_q = 56$. By Steps 5 and 6 in Algorithm 1, we obtain that the first pixels of shares A_i are 28, 227, 203, 191, 179 with moduli $\mathcal{M}$, respectively. Similarly, the first pixels of shares B_i are 195, 115, 75, 55, 35. Now, we consider the reconstruction of $\{p_1, p_2\}$ from two groups of shares A_2', A_3, A_4 and B_2', B_3, B_4, where the first pixels of shares A_2' and B_2' are 115 and 227, respectively. Using the generalized CRT algorithm (Steps 1-5), we have two constructions: $\{x_1, x_2\} = \{3239, 5135\}$. Since $\{\langle x_1 \rangle_{m_0}, \langle x_2 \rangle_{m_0}\} = \{89, 5\}$, $k_1 = 35 \in [0, 40]$ and $k_2 = 57 \in [41, 80]$, we have $\{p_1, q_1\} = \{89, 95\}$. By Steps 7-9, we can obtain $p_1 = 89$ and $q_1 = 95$. Therefore, the first pixels of the two images are correctly recovered.

Fig. 6 gives the correct results for recovering the two images by using the generalized CRT based algorithm with two groups of shares A_2', A_3, A_4 and B_2', B_3, B_4. Clearly, the result is in agreement with Theorem 1 since $\iota = 1$ and since the condition $\iota < \lceil \frac{3}{2} \rceil = 2$ is satisfied. For any two groups of shares $A_{i_1}', A_{i_2}, A_{i_3}$ and $B_{i_1}', B_{i_2}, B_{i_3}$, with three distinct subscripts $i_j \in \{1, 2, \ldots, 5\}$, the two images can be correctly reconstructed by using the proposed algorithm; thus, they are the same as those in Fig. 6. For comparison purposes, we consider two other algorithms: CRT based algorithm and searching algorithm. For the CRT based algorithm,

$$\{p_i, q_i\} = \begin{cases} \{\langle x_{i,1} \rangle_{m_0},\ \langle x_{i,2} \rangle_{m_0}\}, & \text{if } x_{i,1} \in I_1,\ x_{i,2} \in I_1 \\ \{\langle x_{i,1} \rangle_{m_0},\ \langle x_{i,2} \rangle_{m_0} + m_0\}, & \text{if } x_{i,1} \in I_1,\ x_{i,2} \in I_2 \\ \{\langle x_{i,1} \rangle_{m_0},\ \langle x_{i,2} \rangle_{m_0} + 2m_0\}, & \text{if } x_{i,1} \in I_1,\ x_{i,2} \in I_3 \\ \{\langle x_{i,1} \rangle_{m_0} + m_0,\ \langle x_{i,2} \rangle_{m_0}\}, & \text{if } x_{i,1} \in I_2,\ x_{i,2} \in I_1 \\ \{\langle x_{i,1} \rangle_{m_0} + m_0,\ \langle x_{i,2} \rangle_{m_0} + m_0\}, & \text{if } x_{i,1} \in I_2,\ x_{i,2} \in I_2 \\ \{\langle x_{i,1} \rangle_{m_0} + m_0,\ \langle x_{i,2} \rangle_{m_0} + 2m_0\}, & \text{if } x_{i,1} \in I_2,\ x_{i,2} \in I_3 \\ \{\langle x_{i,1} \rangle_{m_0} + 2m_0,\ \langle x_{i,2} \rangle_{m_0}\}, & \text{if } x_{i,1} \in I_3,\ x_{i,2} \in I_1 \\ \{\langle x_{i,1} \rangle_{m_0} + 2m_0,\ \langle x_{i,2} \rangle_{m_0} + m_0\}, & \text{if } x_{i,1} \in I_3,\ x_{i,2} \in I_2 \\ \{\langle x_{i,1} \rangle_{m_0} + 2m_0,\ \langle x_{i,2} \rangle_{m_0} + 2m_0\}, & \text{if } x_{i,1} \in I_3,\ x_{i,2} \in I_3. \end{cases} \tag{52}$$

(a) Recovered image A (b) Recovered image B

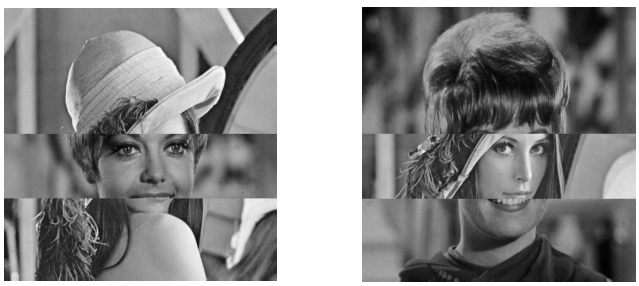
FIGURE 6. Recovered images from two groups: A'_2, A_3, A_4 and B'_2, B_3, B_4.

TABLE 2. Complexity of different algorithms.

Generalized CRT	CRT based algorithm	Searching algorithm
$\mathcal{O}(lP)$	$\mathcal{O}(2^{lP})$	$\mathcal{O}(256^P)$

all possible combinations of remainders for the shares are considered, and each pixel is reconstructed using the CRT. For the searching algorithm, all the pixels of the two images are obtained by searching all the candidates from 0 to 255. The proposed scheme has two advantages when using the generalized CRT based algorithm. First, the scheme has a much lower computational load compared to related conventional schemes since all the pairs of pixels are reconstructed simultaneously and then properly matched with the two images. Table 2 gives the computational complexity of the three algorithms, where l and P denote the number of shares and total pixels, respectively. Second, the scheme is more effective than conventional schemes, since pairs of shares are used mutually and no extra image is used.

Finally, we consider the recovery of two images from the two groups of shares, A'_2, A_4, A'_5 and B'_2, B_4, B'_5, where the positions of the exchanged pixels for A'_i and B'_i are $(240, 1), \ldots, (240, 512), \ldots, (360, 1), \ldots, (360, 512)$. Fig. 7 shows that the two recoveries are failed recoveries. This is because the correspondences between the two images and the constructions $\{p_i, q_i\}$ cannot be successfully determined, although all the pairs of pixels $\{p_i, q_i\}$ are correctly reconstructed by using the proposed generalized CRT based method.



(a) Recovered image A (b) Recovered image B

FIGURE 7. Recovered images from two groups: A'_2, A_4, A'_5 and B'_2, B_4, B'_5.

VI. CONCLUSION

In this paper, we consider the problem of a (t, n) SIS scheme with unordered image shares. The generalized CRT based image sharing and recovery algorithms are proposed. In the sharing algorithm, the pixels of two images in the same position are made secret simultaneously and then shared by the modular operation. In the recovery algorithm, the two images are recovered from any t shares by using the generalized CRT. Compared with existing algorithms, the proposed sharing algorithm has two advantages. First, it has a much lower computational load. Second, it is more efficient than conventional algorithms. Simulations are presented to show the efficiency of the proposed algorithms. The conditions for the success and failure of recovering two images are also given. In future work, we will consider SIS schemes for three or more groups.

REFERENCES

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS Conf.*, New York, NY, USA, vol. 48, 1979, pp. 313–317.

[3] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed–Solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[4] M. Mignotte, "How to share a secret," in *Workshop on Cryptography*. Berlin, Germany: Springer, 1983, pp. 371–375.

[5] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 208–210, Mar. 1983.

[6] M. Ghebleh and A. Kanso, "A novel secret image sharing scheme using large primes," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11903–11923, 2018.

[7] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT*, vol. 950. Berlin, Germany: Springer, 1994, pp. 1–12.

[8] X. Wu and W. Sun, "Visual secret sharing for general access structures by random grids," *IET Inf. Secur.*, vol. 6, no. 4, pp. 299–309, Dec. 2012.

[9] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 61–73, 2018.

[10] Z. Fu, Y. Cheng, and B. Yu, "Visual cryptography scheme with meaningful shares based on QR codes," *IEEE Access*, vol. 6, pp. 59567–59574, 2018.

[11] D. S. Wang, F. Yi, and X. B. Li, "Probabilistic visual secret sharing schemes for grey-scale images and color images," *Inf. Sci.*, vol. 181, no. 11, pp. 2189–2208, 2011.

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

[13] A. Kanso and M. Ghebleh, "An efficient (t, n)-threshold secret image sharing scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16369–16388, 2017.

[14] Z. Zhou, C.-N. Yang, Y. Cao, and X. Sun, "Secret image sharing based on encrypted pixels," *IEEE Access*, vol. 6, pp. 15021–15025, 2018.

[15] L. Liu, A.-H. Wang, C.-C. Chang, Z.-H. Li, and J. Liu, "A lossy secret color image sharing scheme with small shadows and error-resilient capability," *J. Inf. Hiding Multimedis Signal Process.*, vol. 6, no. 2, pp. 246–253, 2015.

[16] W. Hua and X. Liao, "A secret image sharing scheme based on piecewise linear chaotic map and Chinese remainder theorem," *Multimed Tools Appl.*, vol. 76, no. 5, pp. 7087–7103, 2017.

[17] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Chinese remainder theorem-based secret image sharing for (k, n) threshold," in *Cloud Computing Security*, vol. 10603. Cham, Switzerland: Springer, 2017, pp. 433–440.

[18] C. Blundo, A. De Santis, and U. Vaccaro, "Efficient sharing of many secrets," in *Proc. Annu. Symp. Theor. Aspects Comput. Sci.*, vol. 665, 1993, pp. 692–703.

[19] C. Blundo, A. De Santis, G. Di Crescenzo, A. G. Gaggia, and U. Vaccaro, "Multi-secret sharing schemes," in *Proc. Annu. Int. Cryptol. Conf.*, vol. 839, 1994, pp. 150–163.

[20] C.-C. Chang, N.-T. Huynh, and H.-D. Le, "Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation," *Signal Process.*, vol. 99, pp. 159–170, Jun. 2014.
[21] S. Kabirirad and Z. Eslami, "A (t, n)-multi secret image sharing scheme based on Boolean operations," *J. Vis. Commun. Image Represent.*, vol. 57, pp. 39–47, Nov. 2018.
[22] B. Arazi, "A generalization of the Chinese remainder theorem," *Pacific J. Math.*, vol. 70, no. 2, pp. 289–296, 1977.
[23] W. Wang, X. Li, X.-G. Xia, and W. Wang, "The largest dynamic range of a generalized Chinese remainder theorem for two integers," *IEEE Signal Process. Lett.*, vol. 22, no. 2, pp. 254–258, Feb. 2015.
[24] X. Li, X.-G. Xia, W. Wang, and W. Wang, "A robust generalized Chinese remainder theorem for two integers," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7491–7504, Dec. 2016.

XIAOPING LI received the B.S. degree in mathematics from Sichuan Normal University, in 2006, and the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, in 2016.

From 2006 to 2010, he was an Assistant Professor with the College of Information Engineering, Tarim University, Alar, China. From December 2013 to January 2015, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Delaware, Newark. He is currently a Lecturer with the University of Electronic Science and Technology of China. His main research interests include signal processing theory, computer cryptography, and coding theory.

YANJUN LIU received the Ph.D. degree from the School of Computer Science and Technology, University of Science and Technology of China (USTC), Hefei, China, in 2010. She was an Assistant Professor with Anhui University, China, from 2010 to 2015. She is currently a Senior Research Fellow with Feng Chia University in Taiwan. Her research interests include e-business security and electronic imaging techniques.

HEFENG CHEN received the B.S. and M.S. degrees in mathematics from Xiamen University, China, in 2005 and 2008, respectively, and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2016. Since 2016, she has been a Lecturer with the Computer Engineering College, Jimei University. Her current research interests include cryptography and information hiding.

CHIN-CHEN CHANG received the Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan, in 1982. He was the Head and a Professor with the Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the Dean of the College of Engineering, National Chung Cheng University. From August 1995 to October 1997, he was the Provost with National Chung Cheng University. From September 1996 to October 1997, he was the Acting President of National Chung Cheng University. From July 1998 to June 2000, he was the Director of the Advisory Office of the Ministry of Education, China. Since February 2005, he has been a Chair Professor with Feng Chia University. He also published several hundred papers in information sciences. In addition, he has served as a consultant for several research institutes and government departments. His current research interests include database design, computer cryptography, image compression, and data structures. He is currently a Fellow of the IEE, U.K.