Mathematical Biosciences and Engineering

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

MBE, 16(6): 6350–6366.
DOI: 10.3934/mbe.2019317
Received: 18 March 2019
Accepted: 02 July 2019
Published: 09 July 2019

Research article

A novel secret sharing scheme using multiple share images

Xiaoping Li [1], Yanjun Liu [2,*], Hefeng Chen [3] and Chin-Chen Chang [2]

[1] School of Mathematical Science, University of Electronic Science and Technology of China, Chengdu 611731, China.

[2] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan.

[3] Computer Engineering College, Jimei University, Xiamen 361021, China.

* **Correspondence:** yjliu104@gmail.com; Tel: +886-4-2451-7250 ext. 3790; Fax: +886-4-2706-6495.

Abstract: Secret image sharing has been widely applied in numerous areas, such as military imaging systems, remote sensing, and so on. One of the problems for image sharing schemes is to efficiently recover original images from their shares preserved by the shareholders. However, most of the existing schemes are based on the assumption that the shares are distortion-free. Moreover, the correspondence between secret images and their shares is definite. To overcome these shortcomings, we propose a novel secret sharing scheme using multiple share images based on the generalized Chinese remainder theorem (CRT) in this paper, where all of the shares are needed to recover the original images. Two categories of distortions are considered. In the first category, some pairs of shares with the same moduli are exchanged, while in the second category, some of pixels in the pairs of shares with the same moduli are exchanged. Based on these two sharing methods, we propose a generalized CRT based recovery method. Compared with the existing CRT based methods as well as combinatorial based methods, the proposed approach is much more efficient and secure. Furthermore, the conditions for successful recovery of two images from the given distorted shares are obtained. Simulations are also presented to show the efficiency of the proposed scheme.

Keywords: secret image sharing; Chinese remainder theorem (CRT); generalized CRT; share image; reconstruction

1. Introduction

With the rapid development of technologies of the Internet of Things (IoT) and cloud computing, the protection of information in storage as well as in transmission becomes more and more urgent.

For secure transmission of digital information, various different technologies, such as steganography, encryption, secret image sharing, and digital watermarking [1, 2], have been proposed to prevent lawless user causing the data leak. Among these techniques, secret sharing schemes attracted the great interest of many scientists because they are best suited for storing highly confidential and vital data. The basic idea of the secret sharing scheme is to split a secret into several parts and share them among a group of shareholders. To determine the secret, all the authorized users must pool their shares together. This scheme was first independently proposed by Shamir and Blakley [3, 4] in 1979 and further studied in [5, 6]. It plays a critical role in numerous applications, such as in bank accounts, missile launch codes, threshold cryptography, access control, cloud computing, and data hiding [7–9].

Secret sharing schemes have been widely applied in the construction of cryptographic primitives. In 1994, Naor and Shamir introduced a new cryptographic technique called visual cryptography [10], where a digital image is splitted into several meaningless share images and then distributed securely among a set of participants. The proposed secret image sharing (SIS) scheme has two advantages: firstly, it is perfectly secure; secondly, it is very easy to implement because the concealed images are without any cryptographic computations. Therefore, the SIS scheme can be applied in numerous scenarios [11, 12], such as information hiding, authentication, key management, distributed storage in computing, access control, etc. In 2002, Thien and Lin [13] proposed a secret sharing scheme for digital images based on Shamir's scheme [3], where the share images are obtained by modulo a polynomial with finite degree and random coefficient for each pixel. This scheme has a loss of information when the pixels of the image are between 251 and 255 because the most suitable option of modulus is the prime 251. In 2006, Meher and Patra [14] proposed a Chinese remainder theorem (CRT) based secret image sharing scheme. This scheme not only has a low load of computation, but also provides lossless recovery of images. Besides, there are some other secret image sharing schemes, such as the scalable scheme [15], the geometry-based scheme [16], the Sudoku-based scheme [17] and the two-in-one image secret sharing [18]. All the above schemes are efficient in sharing one image and inefficient in sharing multiple images, since the participants have to keep so many shares for different secret images.

Multiple images sharing, which aims to share more than one secret image among a set of participants, can overcome above drawback. In 2002, Tasi et al. [19] proposed a method to share multi-secret in digital images, where there are only two shares for each secret. In 2005, Wu and Chang [20] proposed a $(2, 2)$-visual secret scheme. Although it is more efficient than some previous schemes, it works only when two secret images are shared. In 2011, Chen and Wu [21] proposed a Boolean-based algorithm to share $n - 1$ secret images among a set of n shares. Although this scheme does not require any pixel expansion, it has a poor randomness quality since the obtained shares are not completely randomized. In 2008, Alvarez [22] proposed a cellular automata based scheme. Later on, this scheme was further studied by Eslami [23]. Although these approaches have linear computational complexity, they are impractical due to the fact that they need multiple consecutive shares in order to successfully reconstruct the secret. In 2014, Chang [24] proposed a CRT and Lagrange interpolation based scheme, where the shares are errorless, and the correspondence between the shares and multiple images is assumed to be definite. Under these assumptions, any secret image can be recovered efficiently without recovering all the other images. Another advantage of this method is that it can be used for many formats, such as binary, grayscale and color images. In 2015, Guo et al. [25] proposed a multi-threshold secret image sharing scheme based on an extension of the

CRT, where secret values are produced according to the associated access structures.

The above works consider the case when the shares are without any distortion. Moreover, the correspondence between images and their shares is definite. As far as we know, there is no literature that has considered the recovery of sharing images from their distorted share groups. This paper considers a secret sharing scheme with distorted shares. In this scheme, n different share images are shared and the successful reconstruction of the original images is possible only if all the shares are pooled together. The reconstruction will fail if the number of the shares is equal to or less than $n-1$. Two categories of distortion are considered. In the first category, some pairs of shares with the same moduli are exchanged. In the second category, some of pixels in the pairs of shares with the same moduli are exchanged. To this aim, we innovatively use generalized CRT to recover two images simultaneously from their distorted groups of shares. To be clear, two pixels of two images at the same position are determined simultaneously. The two shares with the same moduli are viewed as a pair and their pixels at the same position are viewed as the residue sets of two images modulo by some given moduli. It is noted that the correspondence between the two images and the shares is not known. Hence, the problem of recovering two images can be modeled as determining two integers (pixels) from their unordered residue sets. This problem was first studied in [26], and further studied in [27, 28]. Based on these works, we propose a secret sharing scheme using multiple share images based on the generalized CRT in this paper. The sharing and recovering algorithms of the proposed approach are also given. Furthermore, we give the condition for successful recovery of two images from their two groups of shares with distortion. Compared with the existing secret image sharing schemes, the proposed scheme has four advantages. First, since the shares are obtained only by partially exchanging each remainder pairs of the pixels, the secret image sharing process is simple and convenient to implement. Second, the secret image sharing algorithm creates no redundancy at all, since no other images are introduced. Third, the recovering of two images from the distorted shares is more secure than that of a simple image. Fourth, the proposed generalized CRT recovering method is more efficient than the combinatorial based method and the searching method. In short, the proposed scheme is more effective and has a wider application in secret communication.

The rest of the paper is organized as follows. In Section 2, we introduce the multi-image sharing problem and then model it as the generalized CRT. In Section 3, we present the generalized CRT based secret image sharing algorithm and its improvement. In Section 4, we give an efficient reconstruction algorithm. Moreover, the conditions of leading to a successful recovery of images are also given. In Section 5, some simulations as well as security analysis of the proposed approach are presented. In Section 6, we conclude this paper.

2. Multiple images sharing problem and Generalized CRT

In this section, we first recall the basic idea of the image sharing problem based on the CRT. Then, we introduce the multiple images sharing problem and model it as the generalized CRT. Some existing results of the generalized CRT are also introduced.

2.1. Chinese Remainder Theorem based image sharing

The earliest known example of CRT can be found in The Mathematical Classic of Sunzi, which is written by Chinese mathematician Sun Tzu in the fifth century. Another Chinese mathematician

Jiushao Qin, in Song Dynasty, generalized this problem into a simultaneous congruence and provided the complete solution. It tells us that a positive integer N can be uniquely reconstructed from its remainders $r_1, r_2, \ldots, r_n$ modulo a set of moduli $m_1, m_2, \ldots, m_n$ if and only if N is less than the least common multiple (lcm) of the moduli [29]. To be specific, if $0 < N < \text{lcm}(m_1, m_2, \ldots, m_n)$, then the simultaneous congruence

$$\begin{cases} N \equiv r_1 \bmod m_1 \\ N \equiv r_2 \bmod m_2 \\ \cdots \\ N \equiv r_n \bmod m_n \end{cases} \tag{2.1}$$

has a unique solution

$$N \equiv \sum_{i=1}^{n} M_i \overline{M}_i r_i \bmod M, \tag{2.2}$$

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 to transmit information confidentially by sharing a secret to different shareholders with partial information, where the unknown integer N can be viewed as the secret, and the remainders $r_1, r_2, \ldots, r_n$ can be viewed as n shares for the shareholders.

One of the extensions for this secret sharing approach is to the image domain. As shown in Figure 1, each pixel p_i in the image of "Lena" (denoted as A for short) is viewed as a secret and then shared by five shareholders with the pairwise coprime moduli 4, 5, 7, 11, 13, respectively, where $i = 1, 2, \ldots, P$ and P is the total number of pixels. All the remainders of p_i with the same moduli m_j can constitute a new image called share A_j of A. Clearly, we cannot obtain any information of the image from any share. Now, we consider the sharing problem of two images simultaneously.

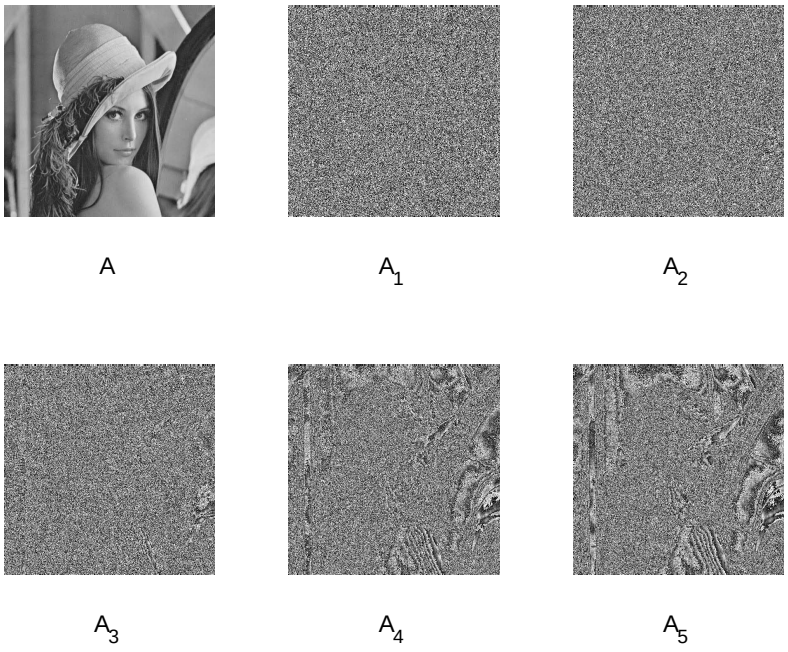

Figure 1. Image "Lena" and its shares.

2.2. Multiple images sharing problem

Figure 2 gives image of "Zelda" (denoted as B for short) and its five shares $B_1, B_2, \ldots, B_5$ with the same moduli as the image of "Lena". By the CRT, we know that image B can also be successfully recovered from its all shares. Also, we know that two images can be successfully recovered from their shares if the correspondence between the two images and their shares is correct. For example, given two groups of shares

$$I: \ A_1, \ A_2, \ A_3, \ A_4, \ A_5 \tag{2.3}$$

and

$$II: \ B_1, \ B_2, \ B_3, \ B_4, \ B_5, \tag{2.4}$$

the two images A and B can be separately recovered from their five shares by using the CRT. However, it is not easy to recover the two images when some pairs of shares with the same modulus are exchanged between the two groups. We will illustrate this by an example below. For convenience, the above two groups of shares are called the standard groups.

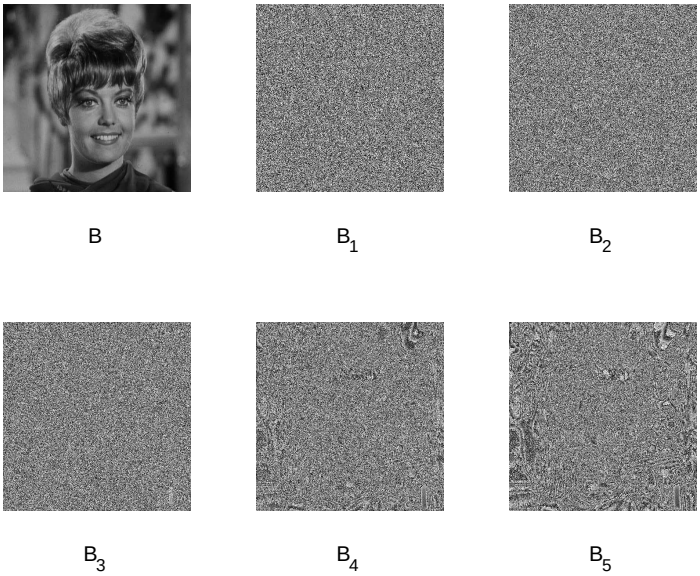

Figure 2. Image "Zelda" and its shares.

Suppose that two groups of the shares are

$$I: \ A_1, \ B_2, \ A_3, \ A_4, \ B_5 \tag{2.5}$$

and

$$II: \ B_1, \ A_2, \ B_3, \ B_4, \ A_5. \tag{2.6}$$

Compared with the standard groups of shares, two pairs of shares with the same modulus are exchanged between the two groups: A_2 and B_2, A_5 and B_5. The exchanged share images are also called distorted shares. Figure 3 gives the illustration of the two groups described in (2.5) and (2.6).

After recovering all the pixels of two images by using the CRT for each group, we obtain two recoveries, which are shown in Figure 4. Clearly, the recovery of two images is a failure. Hence, the CRT method is invalid to recover the two images from their shares when one or more pairs of shares with the same modulus are exchanged between the two groups. The reason is that the CRT is sensitive to the remainder error, where a small amount of errors for any remainder may lead to a large reconstruction error. Here, exchanging two shares of the two images results in errors for the remainders. Motivated by this, we propose a generalized CRT based secret image sharing scheme, which is more secure than the CRT based schemes. By using the generalized CRT proposed in [27], two pixels can be recovered from their shares even if the correspondences between two pixels and their remainders are unknown. Therefore, the two images can be successfully recovered from their shares.

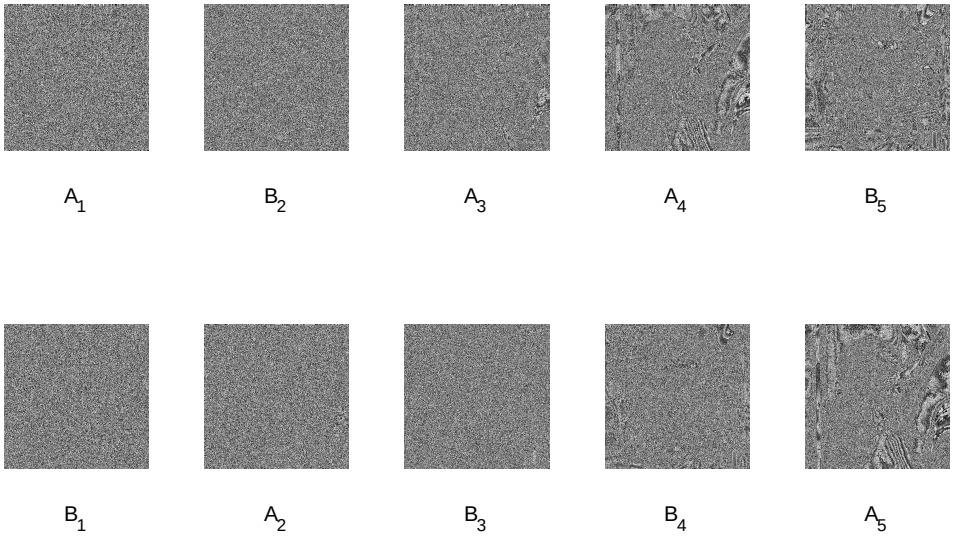

Figure 3. Two groups of the shares in (2.5) and (2.6).

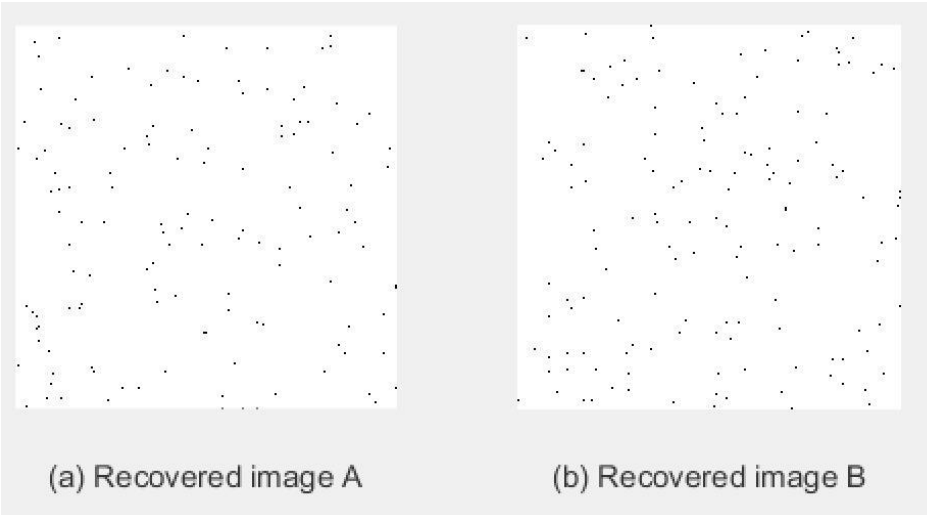

Figure 4. Recovery failure by the CRT.

2.3. Generalized CRT based model

First, we model the secret image sharing and recovering problem as a generalized CRT. Let the pixels of the two images A and B be p_i and q_i, respectively. The i-th pixel of the shares $A_1, A_2, \ldots, A_n$ of A is assumed to be $a_{i,1}, a_{i,2}, \ldots, a_{i,n}$, and the i-th pixel of $B_1, B_2, \ldots, B_n$ of B is assumed to be $b_{i,1}, b_{i,2}, \ldots, b_{i,n}$. In order to recover the image A from the given shares A_1, B_2, A_3, A_4, B_5, all the pixels p_i's should be recovered from the remainders $a_{i,1}, b_{i,2}, a_{i,3}, a_{i,4}, b_{i,5}$ of the shares A_1, B_2, A_3, A_4, B_5, respectively. The similar processes are needed for recovering the image B.

Notice that some pairs of shares with the same modulus are exchanged between the two groups. Hence, pixels in the two images cannot be separately recovered, as shown in Figure 4. We have two steps to recover the two images. The first step uses the generalized CRT to determine each pair of pixels $\{p_i, q_i\}$ simultaneously from all the pairs of pixels $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$, $\ldots$, $\{a_{i,5}, b_{i,5}\}$ of the two groups. Then, determine the correspondences between the two images and their pixels $\{p_i, q_i\}$. For convenience, we briefly recall the basic idea of the generalized CRT below.

Different from the CRT, two pixels $\{p_i, q_i\}$ are simultaneously determined from their residue sets. The problem has two difficulties: one is that the correspondence between the integers $\{p_i, q_i\}$ and their remainders in the residue sets $\{a_{i,j}, b_{i,j}\}$ is unclear; the other is that how large the two pixels can be uniquely determined from their residue sets for the given moduli. It is known that the largest integer uniquely recovered from its remainders is the least common multiple 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 $\{4, 5\}$ and the corresponding moduli 5, 7 and 11, we have four candidates when the two integers are less than $\mathrm{lcm}(5, 7, 11) = 385$, i.e., $\{26, 38\}$, $\{103, 346\}$, $\{136, 313\}$ and $\{213, 236\}$. If the two integers are less than 39, we have only one solution $\{26, 38\}$. In other words, the two integers can be recovered within the range of $(0, 39)$. More generally, the definition of the dynamic range is introduced, which is a range that any multiple integers within it can be uniquely determined from their residue sets modulo the given moduli. In [27], the largest dynamic range $D(\mathcal{M})$ for two integers was obtained, where $\mathcal{M}$ denotes the set of the moduli $\{m_1, m_2, \ldots, m_n\}$. For convenience, we introduce two conclusions below.

Proposition 1. Let n pairwise coprime integers be $2 \le m_1 < m_2 < \cdots < m_n$. If $m_{n-1} \ge 3$, then

$$D(\mathcal{M}) = \min_{I \subseteq \{1,2,\ldots,n\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \bar{I}} m_i \right\}, \tag{2.7}$$

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

For example, given moduli set $\mathcal{M} = \{m_1, m_2, m_3, m_4, m_5\} = \{4, 5, 7, 11, 13\}$, we have

$$D(\mathcal{M}) = 4 \times 5 \times 7 + 11 \times 13 = 283. \tag{2.8}$$

Proposition 2. Let n pairwise coprime integers be $m_1, m_2, \ldots, m_n$. If $N_1, N_2 < D(\mathcal{M})$, then two unordered integers $\{N_1, N_2\}$ can be uniquely determined from their residue sets $\{r_{1,1}, r_{2,1}\}$, $\{r_{1,2}, r_{2,2}\}$, $\ldots$, $\{r_{1,n}, r_{2,n}\}$ with moduli set $\mathcal{M} = \{m_1, m_2, \ldots, m_n\}$.

More details we refer the readers to [27, 28]. In what follows, $\lceil X \rceil$ denotes the least integer greater than or equal to X.

3. The proposed secret image sharing algorithm and its improvement

In this section, we propose a secret image sharing algorithm based on the generalized CRT. Moreover, the improved sharing algorithm is also given.

For a given moduli set $\mathcal{M} = \{m_1, m_2, \ldots, m_n\}$, the largest dynamic range $D(\mathcal{M})$ of $\mathcal{M}$ can be determined. To successfully recover the two images from their shares, $\mathcal{M}$ should satisfy

$$D(\mathcal{M}) > 256. \tag{3.1}$$

By the CRT, we can obtain the i-th pixel $a_{i,j}$ of the j-th share A_j, i.e.,

$$a_{i,j} \equiv p_i \bmod m_j,\ \ j = 1, 2, \ldots, n. \tag{3.2}$$

When there is no confusion, we denote A_j as the matrix of the share A_j. Then, we have the matrix of A_j:

$$A_j = (a_{i,j})_{P\times 1},\ \ i = 1, 2, \ldots, P,\ \ j = 1, 2, \ldots, n. \tag{3.3}$$

Similarly, the i-th pixel $b_{i,j}$ of the share B_j can be obtained by

$$b_{i,j} \equiv q_i \bmod m_j,\ \ j = 1, 2, \ldots, n. \tag{3.4}$$

Hence, the matrix of the share B_j can be described as

$$B_j = (b_{i,j})_{P\times 1},\ \ i = 1, 2, \ldots, P,\ \ j = 1, 2, \ldots, n. \tag{3.5}$$

After determining all the pixels $a_{i,j}$'s and $b_{i,j}$'s, the pair of shares A_j and B_j are obtained. For the two images A and B, the obtained shares are

$$I:\ A_1,\ A_2, \ldots,\ A_n \tag{3.6}$$

and

$$II:\ B_1,\ B_2, \ldots,\ B_n, \tag{3.7}$$

with the moduli $m_1, m_2, \ldots, m_n$, respectively.

Now, we suppose that t pairs of shares are exchanged between the two groups: A_{j_1} and B_{j_1}, A_{j_2} and B_{j_2}, …, A_{j_t} and B_{j_t}. That is, the two groups of shares are

$$I:\ A_1, \ldots, B_{j_1}, \ldots, B_{j_t}, \ldots, A_n \tag{3.8}$$

and

$$II:\ B_1, \ldots, A_{j_1}, \ldots, A_{j_t}, \ldots, B_n, \tag{3.9}$$

with moduli $m_1, m_2, \ldots, m_n$, respectively, where $1 \le j_k \le n$ for $k = 1, 2, \ldots, t$. To obtain a successful recovery of the two images, t should be restricted by $t < \lceil \frac{n}{2} \rceil$, which will be proven in the following section. To sum up, we have the following generalized CRT based image sharing algorithm, which is shown in Table 1.

Table 1. Algorithm 1.

Generalized CRT Based Sharing Algorithm
Step 1. Choose positive pairwise coprime integers $m_1, m_2, \ldots, m_n$ satisfying (3.1).
Step 2. For $j = 1, 2, \ldots, n$, calculate $a_{i,j} \equiv p_i \bmod m_j$ for image A, where $i = 1, 2, \ldots, P$.
Step 3. Obtain A_j of A from the remainders $a_{1,j}, a_{2,j}, \ldots, a_{P,j}$.
Step 4. For $j = 1, 2, \ldots, n$, calculate $b_{i,j} \equiv q_i \bmod m_j$ for image B, where $i = 1, 2, \ldots, P$.
Step 5. Obtain B_j of B from the remainders $b_{1,j}, b_{2,j}, \ldots, b_{P,j}$.
Step 6. Obtain n shares $A_1, \ldots, B_{j_1}, \ldots, B_{j_t}, \ldots, A_n$ of A.
Step 7. Obtain n shares $B_1, \ldots, A_{j_1}, \ldots, A_{j_t}, \ldots, B_n$ of B.

In Algorithm 1, some pairs of the shares with the same modulus are exchanged between the two groups. According to Proposition 2, if $p_i < D(\mathcal{M})$ and $q_i < D(\mathcal{M})$ hold simultaneously, then $\{p_i, q_i\}$ can be recovered from their residue sets $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$, $\ldots$, $\{a_{i,n}, b_{i,n}\}$ modulo $m_1, m_2, \ldots, m_n$, respectively. Note that the remainders in residue sets are unordered. Hence, exchanging the pixels in the pairs A_{j_k} and B_{j_k} is also leading to a successful recovery of the two pixels $\{p_i, q_i\}$, where $1 \le k \le t$. Motivated by this, we propose the following improved image sharing algorithm, where pixels in the shares A_{j_k} and B_{j_k} are partially exchanged. Let

$$A'_j = (a'_{i,j})_{P\times 1},\ i = 1, 2, \ldots, P,\ j = 1, 2, \ldots, n \tag{3.10}$$

and

$$B'_j = (b'_{i,j})_{P\times 1},\ i = 1, 2, \ldots, P,\ j = 1, 2, \ldots, n, \tag{3.11}$$

where

$$a'_{i,j} \in \{a_{i,j},\ b_{i,j}\},\ b'_{i,j} \in \{a_{i,j}, b_{i,j}\} \setminus \{a'_{i,j}\}. \tag{3.12}$$

Then, A_{j_k} and B_{j_k} in the steps 3 and 5 of Algorithm 1 can be substituted by A'_{j_k} and B'_{j_k}, respectively. Hence, the two groups of shares are

$$I:\ A_1, \ldots, A'_{j_1}, \ldots, A'_{j_t}, \ldots, A_n \tag{3.13}$$

and

$$II:\ B_1, \ldots, B'_{j_1}, \ldots, B'_{j_t}, \ldots, B_n \tag{3.14}$$

with moduli $m_1, m_2, \ldots, m_n$, respectively.

Let us consider an example. Suppose the first pixels of A and B are $p_1 = 124$ and $q_1 = 243$, respectively. Under the modular operation, we have

$$a_{1,1} = 0, a_{1,2} = 4, a_{1,3} = 5, a_{1,4} = 3, a_{1,5} = 7$$

from image A with moduli $4, 5, 7, 11, 13$, respectively. Similarly, we have

$$b_{1,1} = 3, b_{1,2} = 3, b_{1,3} = 5, b_{1,4} = 1, b_{1,5} = 9$$

from image B. Suppose the first pixels of the second and the fifth pairs of shares in (3.13) and (3.14) are exchanged. Then, the first pixels of shares in groups I and II are 0, 3, 5, 3, 9, and 3, 4, 5, 1, 7, respectively.

To sum up, we have the following improved image sharing algorithm, which is shown in Table 2. Note that Algorithm 2 is a generalization of Algorithm 1. If all the pixels of pairs A_{j_k} and B_{j_k} are exchanged, then the two shares become B_{j_k} and A_{j_k}, respectively. If all pixels of the shares A_{j_k} and B_{j_k} are exchanged for $j_1, j_2, \ldots, j_t$, then the two groups in (3.13) and (3.14) are changed into (3.8) and (3.9), respectively. Therefore, Algorithm 1 is a special case of Algorithm 2.

Table 2. Algorithm 2.

Improved Image Sharing Algorithm
Step 1. Choose positive pairwise coprime integers $m_1, m_2, \ldots, m_n$ satisfying (3.1).
Step 2. For $i = 1, 2, \ldots, P$, calculate $a_{i,j} \equiv p_i \bmod m_j$ for image A, where $j = 1, 2, \ldots, n$.
Step 3. For $i = 1, 2, \ldots, P$, calculate $b_{i,j} \equiv q_i \bmod m_j$ for image B, where $j = 1, 2, \ldots, n$.
Step 4. Obtain A'_{j_k} with $j_k \in \{j_1, j_2, \ldots, j_t\}$ by (3.10), while others A_j are obtained by Algorithm 1.
Step 5. Obtain B'_{j_k} with $j_k \in \{j_1, j_2, \ldots, j_t\}$ by (3.11), while others B_j are obtained by Algorithm 1.
Step 6. Obtain n shares $A_1, \ldots, A'_{j_1}, \ldots, A'_{j_t}, \ldots, A_n$ of A.
Step 7. Obtain n shares $B_1, \ldots, B'_{j_1}, \ldots, B'_{j_t}, \ldots, B_n$ of B.

4. Secret image reconstruction

In this section, we propose a generalized CRT based secret image reconstruction method. It contains two main contents: the reconstruction algorithm and some results of successful recovery. For convenience, the remainder of x modulo y is denoted as $\langle x \rangle_y$.

4.1. Reconstruction algorithm

The proposed algorithm contains two main parts. Firstly, all of the pairs $\{p_i, q_i\}$ of the two images are reconstructed from the given shares described in (3.13) and (3.14). To be specific, by using the generalized CRT for two unordered integers [27], the i-th pair of pixels $\{p_i, q_i\}$ can be successfully reconstructed from $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$, $\ldots$, $\{a_{i,n}, b_{i,n}\}$ with moduli $m_1, m_2, \ldots, m_n$, respectively. Since the obtained two pixels $\{p_i, q_i\}$ are unordered, we cannot determine which one belongs to A and which to B. Hence, the latter half of the proposed algorithm (steps 5-7) is to determine the correspondence between the two images and two pixels $\{p_i, q_i\}$. More details can be seen in Table 3, where steps 1-6 are performed for all $i = 1, 2, \ldots, P$. From Table 3 one can find that the computational complexity of the proposed reconstruction method is $O(nP)$.

Table 3. Algorithm 3.

Reconstruction Algorithm for Two Images
Step 1. Compute $c_{i,j} = \left\langle a_{i,j} + b_{i,j} \right\rangle_{m_j}$ for $j = 1, 2, \ldots, n$.
Step 2. Compute $\xi_{i,1} = \left\langle \sum_{j=1}^{n} M_j \overline{M}_j c_{i,j} \right\rangle_M$.
Step 3. Compute $\xi_{i,2} = \left\langle \sum_{j=1}^{n} M_j \overline{M}_j (a_{i,j} - s_i)(b_{i,j} - s_i) \right\rangle_M$, where $s_i = \max\{0, \lceil \xi_{i,1} - 2\sqrt{M} \rceil\}$.
Step 4. Obtain two solutions $\{x_{i,1}, x_{i,2}\}$ by solving $(x - s_i)^2 - (\xi_{i,1} - 2s_i)(x - s_i) + \xi_{i,2} = 0$.
Step 5. For $j = 1, 2, \ldots, n$, determine $e_{i,j} = \begin{cases} 1, & \text{if } \langle x_{i,1} \rangle_{m_j} = b_{i,j} \\ 0, & \text{otherwise.} \end{cases}$
Step 6. Determine two pixels: $p_i = \begin{cases} x_{i,1}, & \text{if } \sum\limits_{j=1}^{n} e_{i,j} < \left\lceil \frac{n}{2} \right\rceil \\ x_{i,2}, & \text{otherwise} \end{cases}$ and $q_i \in \{x_{i,1}, x_{i,2}\} \setminus \{p_i\}$.
Step 7. Recover the two images A and B after determining all the pixels p_i and q_i.

4.2. Conditions of successful recovery

Theorem 1 gives the conditions of successful recovery of two images from their shares described in (3.13) and (3.14).

Theorem 1. Let n pairwise coprime integers be $2 \leq m_1 < m_2 < \cdots < m_n$ satisfying (3.1). Two groups of shares for two images are given in (3.13) and (3.14), respectively. If

$$t < \left\lceil \frac{n}{2} \right\rceil \tag{4.1}$$

holds, then the two images A and B can be successfully recovered.

Proof. By Proposition 2, we know that the two pixels $\{p_i, q_i\}$ can be successfully recovered from their residue sets $\{a_{i,1}, b_{i,1}\}$, $\{a_{i,2}, b_{i,2}\}$, $\ldots$, $\{a_{i,n}, b_{i,n}\}$ with moduli $m_1, m_2, \ldots, m_n$, respectively. Let the two reconstructions be $\{x_{i,1}, x_{i,2}\}$. That is,

$$\{p_i, q_i\} = \{x_{i,1}, x_{i,2}\}. \tag{4.2}$$

Next, we will prove that the correspondence between the two reconstructions $\{x_{i,1}, x_{i,2}\}$ and the two images A and B can be correctly determined. We have two cases below.

Case I: $x_{i,1} = x_{i,2}$.

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

$$p_i = q_i = x_{i,1} = x_{i,2}. \tag{4.3}$$

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

In this case, $p_i \neq q_i$. Define

$$e_{i,j} \triangleq \begin{cases} 1, & \text{if } \langle x_{i,1} \rangle_{m_j} = b_{i,j}, \\ 0, & \text{otherwise,} \end{cases} \tag{4.4}$$

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

1) $p_i = x_{i,1}$ and $q_i = x_{i,2}$.

It follows from (3.13) that

$$e_{i,j} = \begin{cases} 1, & \text{if } j \in \{j_1, j_2, \ldots, j_t\}, \\ 0, & \text{otherwise.} \end{cases} \tag{4.5}$$

Hence,

$$\sum_{j=1}^{n} e_{i,j} = t < \left\lceil \frac{n}{2} \right\rceil. \tag{4.6}$$

From (3.14), we have

$$e_{i,j} = \begin{cases} 0, & \text{if } j \in \{j_1, j_2, \ldots, j_t\}, \\ 1, & \text{otherwise.} \end{cases} \tag{4.7}$$

Hence,

$$\sum_{j=1}^{n} e_{i,j} = n - t > n - \left\lceil \frac{n}{2} \right\rceil. \tag{4.8}$$

2) $q_i = x_{i,1}$ and $p_i = x_{i,2}$.

From (3.13), we can obtain (4.7) and consequently (4.8).

From (3.14), we can obtain (4.5) and consequently (4.6).

Thus, two pixels $\{p_i, q_i\}$ can be correctly determined from the two reconstructions $\{x_{i,1}, x_{i,2}\}$ by any group of the given shares, i.e., (3.13) or (3.14). We explain this below.

Suppose that we consider the group of shares described in (3.13). If (4.6) holds, then we have $p_i = x_{i,1}$ and $q_i = x_{i,2}$; if (4.8) holds, then we have $q_i = x_{i,1}$ and $p_i = x_{i,2}$.

Suppose that we consider the group of shares described in (3.14). If (4.8) holds, then we have $p_i = x_{i,1}$ and $q_i = x_{i,2}$; if (4.6) holds, then we have $q_i = x_{i,1}$ and $p_i = x_{i,2}$.

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. This completes the proof of the theorem. □

5. Simulation and security analysis

In this section, we give some simulations to show the efficiency of the proposed generalized CRT based method. Moreover, security analysis of the proposed method is given.

5.1. Simulation results

We take two 512×512 images "Lena" and "Zelda" in the simulations. The moduli are set to be $\mathcal{M} = \{4, 5, 7, 11, 13\}$. By (2.8), we obtain $D(\mathcal{M}) = 283 > 256$, which satisfies the condition in (3.1). Hence, any two pixels can be recovered from their two groups of shares with the given moduli.

First, we recover the two images from two groups of shares described in (2.5) and (2.6) in Section 2. For the CRT based method, the two recoveries are failures, as shown in Figure 4. Compared with two standard groups of shares, there are two pairs exchanged between each other. Hence, $t = 2$ and then

$$t < \left\lceil \frac{n}{2} \right\rceil = \left\lceil \frac{5}{2} \right\rceil, \tag{5.1}$$

which satisfy the condition in (4.1). By Theorem 1, we know that the two images can be successfully recovered by using the generalized CRT. Figure 5 gives the simulation results, which show that the two images are successfully recovered and hence the proposed method is effective. In fact, for any two groups of shares with $t \leq 2$, the two images can be successfully recovered. Hence, the probability of recovering the two secret images from the distorted shares is

$$Pr = \frac{C_5^1 + C_5^2}{C_5^1 + C_5^2 + C_5^3 + C_5^4 + C_5^5} = \frac{15}{31}. \tag{5.2}$$

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

Figure 5. Recovered images by Algorithm 3 for two groups in (2.5) and (2.6).

Now, we give the recovery of two images from the following two groups of shares:

$$I: \ A_1, \ A_2', \ A_3, \ A_4', \ A_5' \tag{5.3}$$

and

$$II: \ B_1, \ B_2', \ B_3, \ B_4', \ B_5', \tag{5.4}$$

where the positions of exchanged pixels for the shares A_i' and B_i' are $(120, 120), (120, 121), \ldots, (120, 380), (121, 120), \ldots, (380, 380)$. For example, assume that two pixels of A and B in the position $(120, 120)$ are 146 and 222, respectively. According to (3.2) and (3.4), we have two groups of remainder sets 2, 1, 6, 6, 3 and 2, 2, 5, 2, 1 with moduli $4, 5, 7, 11, 13$, respectively. Note that three pairs of pixels are exchanged, i.e., A_2 and B_2; A_4 and B_4; A_5 and B_5. Hence, the pixels of the shares described in (5.3) and (5.4) in the position $(120, 120)$ are 2, 2, 6, 2, 1 and 2, 1, 5, 6, 3, respectively. Since three pairs of shares are exchanged, we have $t = 3$ and then

$$t > \left\lceil \frac{n}{2} \right\rceil = \left\lceil \frac{5}{2} \right\rceil. \tag{5.5}$$

Since the condition in (4.1) is not satisfied, the recovery of two images will fail according to Theorem 1. Figure 6 gives two recoveries by using the proposed generalized CRT based method. Clearly, the two recoveries are consistent with theory analysis. Compared with the CRT method, all the pairs of pixels $\{p_i, q_i\}$ of the two images are correctly reconstructed by the proposed generalized CRT based method. However, the correspondences between the two images and two reconstructions $\{p_i, q_i\}$ can

not be correctly determined in the positions of the exchanged pixels, which leads to a recovery failure. In fact, for any two groups of shares with $t \geq 3$, the two images can not be successfully recovered. By (5.2), we know that the failure probability is

$$Pr = 1 - \frac{15}{31} = \frac{16}{31}.$$

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

Figure 6. Recovered images by Algorithm 3 for two groups in (5.3) and (5.4).

5.2. Security Analysis

Now, we compare the proposed scheme with two other methods on the security issue. Consider the two groups of shares described in (3.13) and (3.14). As stated above, the two images can not be successfully recovered by the CRT method in this case. We consider two other methods, i.e., the searching method and the combinatorial based method.

Suppose that some illegal users attempt to recover the two images by using the searching method. For this kind of method, all the possible pixels (0-255) should be tested for each pixel. Hence, the probability of successfully reconstructing each image is

$$Pr = \frac{1}{256^P}, \tag{5.6}$$

which is a very small number when $P = 512 \times 512$. In other words, the computational complexity of the searching method is $O(256^P)$.

Suppose that some illegal users attempt to recover the two images by using the combinatorial based method. To recover the pixels p_i and q_i, one can firstly put the pixels of shares A_i and B_i together and obtain the residue sets

$$\{a_{i,1}, b_{i,1}\}, \ \ldots, \ \{a_{i,j}, b_{i,j}\}, \ \ldots, \ \{a_{i,n}, b_{i,n}\} \tag{5.7}$$

with moduli $m_1, m_2, \ldots, m_n$, respectively. Then, the residue sets are grouped into two sequences by choosing only one pixel for each set. If and only if the two sequences are

$$a_{i,1}, \ldots, a_{i,j}, \ldots, a_{i,n} \tag{5.8}$$

and

$$b_{i,1}, \ldots, b_{i,j}, \ldots, b_{i,n}, \tag{5.9}$$

the two pixels p_i and q_i can be separately reconstructed by the CRT. Hence, the probability of the successful reconstruction of p_i and q_i is

$$Pr = \frac{1}{2^n} \tag{5.10}$$

when the two remainders in each residue set are distinct. Note that the two secret images can be successfully recovered if all the pixels p_i and q_i are correctly determined. Hence, the probability of the successful recovery is

$$Pr = \frac{1}{2^{nP}}. \tag{5.11}$$

In other words, the computational complexity of the combinatorial based method is $O(2^{nP})$. Clearly, the probability of successfully recovering the two images depends on both the number of moduli n and P. It is unlikely that someone will exhaustively reconstruct the two images by trying all the possible combinations of shares.

6. Conclusion

In this paper, we considered the problem of secret image sharing scheme with distorted shares. Two categories of distortions were considered. The first category is that some pairs of the shares with the same moduli are exchanged, while the second category is that some of pixels in the pairs of shares with the same moduli are exchanged. Based on these distorted shares, we proposed a generalized CRT based recovery method, which is much more efficient and secure than the existing CRT based methods as well as combinatorial based methods. The conditions for successful recovery are obtained. Simulations are also presented to show the efficiency of the proposed scheme.

Acknowledgments

This work was supported in part by the National Nature Science Foundation of China (No. 61701086), the Fundamental Research Funds for the Central Universities (No. ZYGX2016KYQD143), the Natural Science Foundation of Fujian Province (Nos. 2017J01761 and 2018J01537), the Project of Ministry of Science and Technology of Taiwan (No. MOST 106-2221-E-035-013-MY3).

Conflict of interest

The authors declare no conflict of interest.

References

1. R. L. Lagendijk, Z. Erkin and M. Barni, Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation, *IEEE Signal Proc. Mag.,* **30** (2013), 82–105.

2. C. C. Chang, C. T. Li and Y. Q. Shi, Privacy-aware reversible watermarking in cloud computing environments, *IEEE Access,* **6** (2018), 70720–70733.
3. A. Shamir, How to share a secret, *Commun. ACM,* **22** (1979), 612–613.
4. G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the National Computer Conference,* (1979), 313–317.
5. E. Karnin, J. Greene and M. Hellman, On secret sharing systems, *IEEE T. Inform. Theory,* **29** (1983), 35–41.
6. W. T. Huang, M. Langberg, J. Kliewer, et al., Communication efficient secret sharing, *IEEE T. Inform. Theory,* **62** (2016), 7195–7206.
7. M. Naor and A. Wool, Access control and signatures via quorum secret sharing, *IEEE Trans. Parallel Distrib. Syst.,* **9** (1998), 909–922.
8. M. Stadler, Publicly verifiable secret sharing, in *International Conference on the Theory and Applications of Cryptographic Techniques,* (1996), 190–199.
9. J. H. Ziegeldorf, O. G. Morchon and K. Wehrle, Privacy in the Internet of Things: threats and challenges, *Security Commun. Netw.,* **7** (2014), 2728–2742.
10. M. Naor and A. Shamir, Visual cryptography, in *Workshop on the Theory and Application of Cryptographic Techniques,* Springer, (1994), 1–12.
11. X. Yan and Y. Lu, Generalized general access structure in secret image sharing, *J. Vis. Commun. Image Represent.,* **58** (2019), 89–101.
12. L. Tan, Y. Lu, X. Yan, et al. Weighted secret image sharing for a (k, n) threshold based on the Chinese remainder theorem, *IEEE Access,* **7** (2019), 59278–59286.
13. C. C. Thien and J. C. Lin, Secret image sharing, *Comput. Graph.,* **26** (2002), 765–770.
14. P. K. Meher and J. C. Patra, A new approach to secure distributed storage, sharing and dissemination of digital image, in *International Symposium on Circuits and Systems,* (2006), 373–376.
15. R. Z. Wang and S. J. Shyu, Scalable secret image sharing, *Signal Process.-Image,* **22** (2007), 363–373.
16. C. C. Chen, W. Y. Fu and C. C. Chen, A geometry-based secret image sharing approach, *J. Inf. Sci. Eng.,* **24** (2008), 1567–1577.
17. C. C. Chen, W. Y. Fu and C. C. Chen, A sudoku-based secret image sharing scheme with reversibility, *J. Commun.,* **5** (2010), 5–12.
18. X. Yan, Y. Lu, L. Liu, et al., Chinese remainder theorem-based two-in-one image secret sharing with three decoding options, *Digit. Signal Process.,* **82** (2018), 80–90.
19. C. S. Tsai, C. C. Chang and T. S. Chen, Sharing multiple secrets in digital images, *J. Syst. Softw.,* **64** (2002), 163–170.
20. H. C. Wu and C. C. Chang, Sharing visual multi-secret using circle shares, *Comput. Stand. Interfaces,* **28** (2005), 123–135.
21. T. H. Chen and C. S. Wu, Efficient multi-secret image sharing based on Boolean operations, *Signal Process.,* **91** (2011), 90–97.

22. G. Alvarez, L. H. Encinas and A. M. Del Rey, A multisecret sharing scheme for color images based on cellular automata, *Inf. Sci.,* **178** (2008), 4382–4395.

23. Z. Eslami, S. Razzaghi and J. Z. Ahmadabadi, Secret image sharing based on cellular automata and steganography, *Pattern Recognit.,* **43** (2010), 397–404.

24. C. C. Chang, N. T. Huynh and H. D. Le, Lossless and unlimitted multi-image sharing based on Chinese remainder theorem and Lagrange interpolation, *Signal Process.,* **99** (2014), 159–170.

25. C. Guo, H. Zhang, Q. Q. Song, et al., A multi-threshold secret sharing scheme based on the Chiense remainder theorem, *Multimed. Tools Appl.,* **75** (2016), 11577–11594.

26. B. Arazi, A generalization of the Chinese remainder theorem, *Pac. J. Math.,* **70** (1977), 289–296.

27. W. Wang, X. P. Li, X. G. Xia, et al., The largest dynamic range of a generalized Chinese remainder theorem for two integers, *IEEE Signal Process. Lett.,* **22** (2015), 254–258.

28. X. P. Li, X. G. Xia, W. J. Wang, et al., A robust generalized Chinese remainder theorem for two integers, *IEEE T. Inform. Theory,* **62** (2016), 7491–7504.

29. K. H. Rosen, *Elementary Number Theory and Its Applications,* 5^{th} edition, Addison-Wesley, Mass., 2010.

AIMS Press