Received May 16, 2019, accepted June 1, 2019, date of publication June 7, 2019, date of current version June 21, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921612

Lossless (k, n)-Threshold Image Secret Sharing Based on the Chinese Remainder Theorem Without Auxiliary Encryption

LONGLONG LI, YULIANG LU, XUEHU YAN, LINTAO LIU, AND LONGDAN TAN
College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China

Corresponding author: Yuliang Lu (publicluyl@126.com)

This work was supported by the National Natural Science Foundation of China (grant number: 61602491) and the Key Program of the National University of Defense Technology (grant number: ZK-17-02-07).

ABSTRACT A typical Chinese remainder theorem (CRT)-based secret sharing (SS) scheme has been proposed by Asmuth and Bloom for several decades, with lower computation complexity compared to Shamir's original polynomial-based SS. But when applied to images, CRT-based image secret sharing (CRTISS) shows many problems, such as lossy recovery, auxiliary encryption, and extra parameters requirement. We analyze the characteristics of images and ISS and propose a (k, n)-threshold CRTISS based on the Asmuth and Bloom's scheme by sharing the high 7 bits of a grayscale secret pixel and embedding the least significant bit (LSB) into the random integer. The pixel values of a grayscale image are divided into two parts, which make it possible to share all the secret pixels with no expansion. Our method has the advantages of (k, n) threshold, lossless recovery, and no auxiliary encryption. The parameters requirement is the same as that in the Asmuth and Bloom's original method. Analysis and experiments are provided to validate the effectiveness of the proposed method.

INDEX TERMS Image secret sharing, Chinese remainder theorem, lossless recovery, (k, n) threshold.

I. INTRODUCTION

Nowadays, people often take many photos and share them using many social softwares, such as Twitter and Facebook, or upload them to cloud servers. But the storage of these private images brings a significant security problem. If stored in a single information-carrier, they are easily lost or corrupted. And storing multiple copies of these images increases the danger of security breaches. Image secret sharing (ISS) provides a solution to the problem. In a (k, n)-threshold ISS scheme, a secret image is split into n shares, i.e., shadow images or shadows, which are then distributed to n different participants. The secret image can be recovered by at least any k shares while less than k shares give no clues about the secret, even with the most powerful computing device in the world. Secret sharing (SS) is also applied to other scenarios, such as digital watermarking, key management, identity authentication, access control, password transmission and block chain [1]–[5]. ISS schemes chiefly include visual secret sharing(VSS) [6]–[8], polynomial-based scheme [9] and the Chinese remainder theorem-based ISS (CRTISS) [10]–[12].

VSS, also known as visual cryptography (VC), has the advantage of low computing requirement in the recovery phase, where we can stack any k or more shares to get the secret image by naked human eyes. An attacker can only get a noise-like image with less than k shares. However, conventional VSS schemes have some drawbacks, e.g., low image quality, pixel expansion, codebook design and so on, which are studied in the following works [13]–[17].

Polynomial-based secret sharing (SS) scheme was first proposed by Shamir [9], encoding the secret via constructing a $k-1$ degree polynomial to generate n shares. When gathering k or more shares, one can reconstruct the polynomial by Lagrange interpolation to decode the secret. Inspired by Shamir's work, Thien and Lin [18] applied the Polynomial-based SS to images. Differently, they utilized all the k coefficients to embed the secret image pixels and reduced the share size to $1/k$ of the secret image size. Then, some researchers carried on the study of polynomial-based ISS to realize more features, such as multiple decoding options, lossless recovery and differently weighted shares [19]–[22]. However, for the sake of some special image features, there still exist challenges in Shamir's polynomial-based ISS, including lossy

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

recovery, high computation complexity and auxiliary encryption. Image pixel values range from 0 to 255 and the chosen modulus in the decoding phase is 251, which means five pixel values cannot be recovered. So in general there is a little bit loss in the recovered image. Due to Lagrange interpolation in the recovery phase, the computation complexity is $O(k\log^2 k)$ [10]. Auxiliary encryption is usually needed before sharing to eliminate the correlation of image pixels.

Because the modular method needs only $O(k)$ operations [10] to recover every secret pixel, CRTISS has the advantage of low computation cost, which is important when considering the big amount of image pixels. Asmuth and Bloom [10] and Mignotte [11] proposed (k, n)-threshold SS based on CRT respectively in 1983. Yan *et al.* [12] firstly introduced CRT into ISS, which may have a little information leakage and recovery loss. Shyu and Chen [23] extended Mignotte's method to ISS, utilizing a PRNG to encrypt the pixel values so as to eliminate image pixel correlation. Ulutas *et al.* [24] proposed a CRTISS based on Asmuth and Bloom's scheme by dividing pixel values into two intervals. Since they didn't give precise restrictions on the parameters, the (k, n) threshold may be not achieved when the random number is too small. Furthermore, it doesn't consider pixel value 2 times or more to the interval boundary. Chunqiang *et al.* [25] proposed a CRTISS based on the chaotic map, involving auxiliary encryption. Chuang *et al.* extended the CRTISS proposed by Ulutas to design a (k, n)-threshold ISS via only sharing the most significant 7 bits to satisfy the restrictions of CRT. They stored and transmitted the least significant bit (LSB) of secret image pixels independently or just threw them away. So the drawback of their method is that the recovery secret image is lossy or high transmission cost is needed. Yan *et al.* [26], [27] proposed a CRTISS by dividing the value of the grayscale pixel into two intervals with similar size and provided precise restrictions and applicable explicit parameters for the implementations. Their method is with (k, n)-threshold, no auxiliary encryption and lossless. But they have to transmit an extra parameter to identify the two intervals.

In this paper, we propose a (k, n)-threshold CRTISS based on the Asmuth and Bloom's method through sharing the high 7 bits of the grayscale secret pixels and embedding their LSBs to the lowest bits of the random numbers. Our method realizes lossless recovery for grayscale image without auxiliary encryption. Compared to Yan *et al.*' scheme, there is no extra parameter needed to be transformed in our method. The shares are all noise-like, and the recovered image from any $k-1$ or less shares is still noise-like. Pixel values in shares are approximatively uniformly distributed, which illustrates the security of our method. Analysis and experiments are provided to indicate the effectiveness of the proposed method.

The rest of the paper is organized as follows. Some basic requirements are introduced for the proposed method in section II. In section III, the proposed method is presented in detail. Then we give the experimental results and comparisons in section IV. Finally, section V concludes this paper.

II. PRELIMINARIES

In this section, we give some preliminaries for our work, including the Chinese remainder theorem, image characteristics and the Asmuth and Bloom's CRT-based SS scheme. For (k, n) threshold ISS, the original secret image S is encrypted to n shares $SC_1, SC_2, \cdots, SC_n$, and the decrypted secret image S' is reconstructed from t $(k \le t \le n, t \in Z^+)$ shares.

In general, a valid ISS construction for (k, n) threshold should satisfy the following conditions [7].

1) Security condition: $k-1$ or less shares give no clue about the secret.
2) Recognition condition: any k or more shares can recover the secret.

A. CHINESE REMAINDER THEOREM (CRT)

CRT aims to solve a set of simultaneous linear congruence equations. A set of positive integers $m_i (i = 1, 2, \cdots, k)$ is chosen subject to $\gcd\left(m_i, m_j\right) = 1, i \ne j$. Then there exists only one solution

$$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod M,$$

$y \in [0, M-1]$ for the following linear congruence equations.

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

where $M = \prod_{i=1}^{k} m_i$, $M_i = {}^{M}\!/_{m_i}$ and $M_i M_i^{-1} \equiv 1 \pmod{m_i}$.

$\gcd\left(m_i, m_j\right) = 1, i \ne j$ ensure every equation in Eq. (1) will not be eliminated by other equations.

It is remarkable that in $[0, M-1]$ there exists only one solution. If $k-1$ equations in Eq. (1) are collected, assuming a_j is the missing one, we can obtain only one solution satisfying the $k-1$ equations in $[0, \prod_{i=1, i\ne j}^{k} m_i - 1]$, denoted as y_0. Whereas in $[0, M-1]$, $y_0 + b\prod_{i=1, i\ne j}^{k} m_i$ for $b = 1, 2, \cdots, m_j - 1$ are also the solutions for the $k-1$ equations in Eq. (1). Thus, there are another $m_j - 1$ solutions in $[\prod_{i=1, i\ne j}^{k} m_i, M-1]$. The $m_j - 1$ solutions are corresponding to different possible a_k in range of $[0, m_j - 1]$. Therefore, any $k-1$ equations gain no clue about the exact solution y, which will be utilized in the proposed scheme to achieve (k, n) threshold.

B. THE FEATURE ANALYSIS OF AN IMAGE

Digital image has many special features due to its formats. Images are composed of pixels, and there exists some correlations between pixels, such as structure, texture, edge and other related information. Even with extreme distortion, we could get some information from a corrupted image as well. Thus, ISS should scramble not only the pixel values but also the correlations between adjacent pixels.

The pixel value of gray images ranges from 0 to 255, which brings a little difference between ISS and SS.

1) An image is composed of pixels with a certain correlation between each other, thus the security of an image protection algorithm should consider at least two aspects, i.e., single pixel security and region security. However, a data protecting algorithm in general only considers data block.
2) Because an image in general contains a big amount of pixels, the generating and recovering algorithmic efficiency is more important in ISS design.
3) Images have special storage file structure, which brings more restrictions in ISS, e.g., the limited range of pixel value. Therefore, parameters in ISS need to be carefully chosen to make sure the shares in proper pixel range.
4) As for binary images, one bit represents a pixel while one byte represent a pixel in gray scale images. It is easy to generalize ISS to digital data secret sharing, by dividing the data to single bits or bytes.
5) Secret sharing has the property of "all-or-nothing", which means loss in data blocks make them unreadable. But to ISS, lossy recovery still make sense.

C. ASMUTH AND BLOOM'S CRT-BASED SS SCHEME

Asmuth and Bloom proposed the CRT-based SS scheme in 1983, which has the advantage of low computation complexity, requiring only $O(k)$ operations.

Asmuth and Bloom's CRT-Based SS for (k, n) Threshold

Input: Secret s and threshold (k, n).

Output: n shares $sc_1, sc_2, \cdots sc_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$.

Step 1: Choose a set of integers $\{s < p < m_1 < m_2 \cdots < m_n\}$ satisfying

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: Choose a random integer A in $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ and let $y = s + Ap$.

Step 3: Compute $a_i \equiv y \pmod{m_i}$ and let $sc_i = a_i$ for $i = 1, 2, \cdots, n$.

Step 5: Output n shares $sc_1, sc_2, \cdots sc_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots m_n$.

When applied to ISS, it has the problem of only sharing a limited value range of pixels. As for grayscale image, pixel values range from 0 to 255. We have $0 \leq a_i \leq 255$ and $a_i \leq m_i$. Since $\{s < p < m_1 < m_2 \cdots < m_n\}$ in Step 1, it is easy to find $s < 255$. With the increasing of n, the range of s decrease terribly. Obviously, the essential issue is to figure out a way to share all the pixels in a grayscale image.

III. THE PROPOSED CRTISS METHOD FOR (*K*, *N*) THRESHOLD

A. OUR METHOD

Here, we propose a novel ISS scheme for (k, n) threshold based on CRT. The original grayscale secret image S is split into n shares $SC_1, SC_2, \cdots SC_n$, which will be sent to n different participants with their corresponding privacy modular integers $m_1, m_2, \cdots m_n$.

Our method is based on the Asmuth and Bloom's CRTSS scheme. In the original scheme, every share has the bigger value range than the secret, which means only a small range of pixels can be shared with the requirement of share pixel ranging in [0, 255]. We propose a solution to share the high 7 bits ([0, 127]), and embed the LSB into the random integer. The generation Steps are described in Algorithm 1, whose diagrammatic design concept is shown in Fig. 1. And the recovery steps are presented in Algorithm 2.

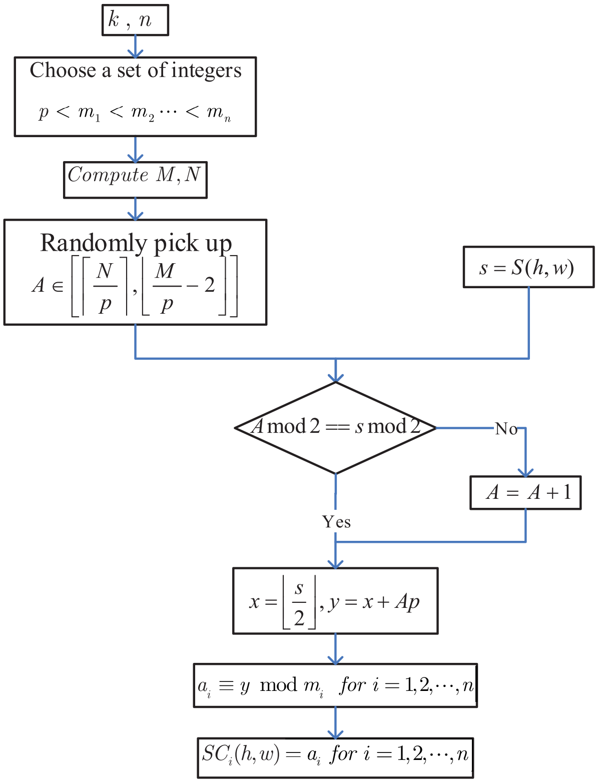

k , n
Choose a set of integers
$p < m_1 < m_2 \cdots < m_n$
$Compute\ M, N$
Randomly pick up
$A \in \left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$
$s = S(h, w)$
$A \bmod 2 == s \bmod 2$
No
$A = A + 1$
Yes
$x = \left\lfloor \frac{s}{2} \right\rfloor, y = x + Ap$
$a_i \equiv y \bmod m_i \quad for\ i = 1, 2, \cdots, n$
$SC_i(h, w) = a_i \quad for\ i = 1, 2, \cdots, n$

FIGURE 1. **Design concept for the proposed method.**

For Algorithm 1 and Algorithm 2, we remark that.

1) In Step 1 of our Algorithm 1, the condition $\{128 \leq p < m_1 < m_2 \cdots < m_n \leq 256\}$ is given by image pixel value range and $pN < M$. We suggest that p is as small as possible for security as well as m_i is as large as possible so that the pixel values in shares can randomly lie in large range.
2) $\gcd(m_i, m_j) = 1$ and $\gcd(m_i, p) = 1$ aim to satisfy CRT conditions, where m_i may be preserved as the privacy key for participant SC_i. $\gcd(m_i, p) = 1$ may be on account of not only applicable CRT but also

Algorithm 1 The Proposed CRTISS Method for (k, n) Threshold

```
Input: The original secret image $S$ with size of $H \times W$ and threshold parameters $(k, n)$.
Output: $n$ shares $SC_1, SC_2, \cdots SC_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$.
Step 1: 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.
  For each position $(h, w) \in \{(h, w)|1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2-4.
Step 2: Let $s = S(h, w)$. Pick up a random integer $A$ in $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$.
  If $A \equiv s \mod 2$, keep $A$ unchanged; otherwise let $A = A + 1$.
Step 3: Compute $x = \left\lfloor \frac{s}{2} \right\rfloor$, which means sharing the high 7 bits of the pixel. Let $y = x + Ap$.
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 $n$ aharess $SC_1, SC_2, \cdots SC_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots m_n$.
```

containing all possible pixel values in the range $[0, m_i)$ in share SC_i.

3) In Step 3 of our Algorithm 1, we know A is randomly picked up from $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$, thus $N \leq y < M$ in order to obtain (k, n) threshold for y as explained in Section II-A. A cannot equal to $\left\lfloor \frac{M}{p} - 1 \right\rfloor$ because it needs to be modified to $A + 1$ in some occasions.
4) In Step 3 of Algorithm 1, we share the high 7 bits of secret pixels and embed the LSB into the last bit of the random number. As a result, s can be losslessly recovered for arbitrary $s \in [0, 255]$.
5) In Step 3 of Algorithm 1, A is randomly picked up for every x, therefore $y = x + Ap$ can enlarge x value so as to scramble not only the pixel value but also the correlations between adjacent pixels without auxiliary encryption. Since few information can be obtained from the LSB of grayscale pixels, the correlations of pixels will not lead to information leakage.
6) In Step 3 of Algorithm 1, $y = x + Ap$ can determine only one x based on $x \equiv y \pmod{p}$.

B. PERFORMANCE ANALYSES

This subsection will show the performances of the proposed method by theoretically analyzing the security and lossless recovery. In Theorem 1, we will prove that the proposed scheme is a valid (k, n) threshold ISS construction. Prior to the proof of Theorem 1, some Lemmas are given.

Algorithm 2 Secret Image Recovery of the Proposed Scheme

```
Input:$k$ shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_k}$, their corresponding privacy modular integers $m_{i_1}, m_{i_2}, \cdots m_{i_k}$ and $p$.
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.
    $$\begin{aligned} y &\equiv a_{i_1} \pmod{m_{i_1}} \\ y &\equiv a_{i_2} \pmod{m_{i_2}} \\ &\cdots \\ y &\equiv a_{i_{k-1}} \pmod{m_{i_{k-1}}} \\ y &\equiv a_{i_k} \pmod{m_{i_k}} \end{aligned} \quad (2)$$
Step 3: Compute $A = \left\lfloor \frac{y}{p} \right\rfloor$. Let $x \equiv y \pmod{p}$. $s' = x \times 2 + (A \bmod 2)$. Set $S'(h, w) = s'$.
Step 4: Output the recovered secret image $S'$.
```

Lemma 1: Each share generated by our method gives no clue about the secret image.

Proof 1: From $y = x + Ap$ and $a_i \equiv y \pmod{m_i}$, we will prove $SC_i(h, w) = a_i$ is random in range $[0, m_i)$.

When A is fixed, since x represents the pixel value of the secret image, we can assume x is random in range $[0, 127]$. Due to $a_i \equiv (x + Ap) \pmod{m_i}$, we have a_i is random in range $[0, m_i)$.

On the other hand, when x is fixed, $\gcd(m_i, p) = 1$, thus $Ap \pmod{m_i}$ can cover all possible values in range $[0, m_i)$ as long as the continuous interval of A has the least size of m_i. Assume we have $x + Ap \equiv a_i \pmod{m_i}$ and $x + A'p \equiv a_i \pmod{m_i}$, so $Ap \equiv A'p \,(\mathrm{mod} m_i)$. Then we get that $m_i|(Ap - A'p)$, i.e., $(A - A')p$ is a multiple of m_i. Since $(p, m_i) = 1$, $(A - A')$ must be a multiple of m_i. With the A increasing, we can have $x + Ap \pmod{m_i}$ can cover all possible values in range $[0, m_i)$ as well. As a result, we have a_i is random in range $[0, m_i)$.

A special case is needed to be discussed here. When we share the high 7 bits of a grayscale pixel, i.e. x, and embed the LSB into the random integer A, every x is corresponding to two different pixels indeed. When x is fixed, to cover the range of share pixels $[0, m_i)$, the available numbers of integer A should be greater than or equal to $2m_i$. As for $(2, n)$ threshold, A ranges in $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$, i.e. $\left[\left\lceil \frac{m_n}{p} \right\rceil, \left\lfloor \frac{m_1 \times m_2}{p} - 2 \right\rfloor\right]$, which does not meet the requirement. Therefore, some pixel values will not appear in shares, while the rest values will still be shared randomly. When $k > 2$, the range of A meets the requirement and all pixel values in shares can be covered.

Thus, the Lemma is proved to be met.

Lemma 2: In the proposed scheme, any k or more shares can recover the secret losslessly.

Proof 2: Since x represents the high 7 bits of pixels in the secret image, we will prove any k or more shares can recover x losslessly.

In order to recover x, we only need to find y due to $x \equiv y \,(\text{mod } p)$ or $x \equiv y \,(\text{mod } p) + p$.

When $a_{i_1}, a_{i_2}, \cdots a_{i_k}$ are given, according to CRT, there exists only solution y modulo $N_1 = \prod_{j=1}^{k} m_{i_j}$ since $N_1 \geq M$. Finally we can uniquely determine y and x based on Step 3 of our Algorithm 2.

Lemma 3: In the proposed scheme, $k-1$ or less shares give no clue about secret.

Proof 3: When $k-1$ shares pixels $a_{i_1}, a_{i_2}, \cdots a_{i_{k-1}}$ are given, according to CRT then all we have is y_0 modulo $N_2 = \prod_{j=1}^{k-1} m_{i_j}$, where $y_0 \in [0, N_2 - 1]$. On one hand, the true $y \in [N, M-1]$, which is absolutely different from above y_0. On the other hand, since $N \geq N_2$,$N \leq y < M$ and $\gcd(N_2, p) = 1$, in $[N_2, M-1]$, $y_0 + b\prod_{j=1}^{k-1} m_{i_j}$ for $b = 1, 2, \cdots, m_{i_k} - 1$ are also the solutions for the collected $k-1$ equations in Eq. (3). Thus, there are another $m_{i_k} - 1$ solutions in $[N_2, M-1]$, corresponding to every different possible a_{i_k} in range of $[0, m_{i_k} - 1]$. Thus $k-1$ or less shares give no clue about the secret.

Theorem 1: Our method is a valid ISS construction for (k, n) threshold.

Proof 4: Based on the above Lemmas, the mentioned conditions are satisfied.

IV. EXPERIMENTAL RESULTS AND ANALYSES

In this section, experiments and analyses are performed to evaluate the effectiveness of our method.

A. IMAGE ILLUSTRATION

Fig. 2 gives the experimental results for $(2, 3)$ threshold, where $p = 128, m_1 = 251, m_2 = 253, m_3 = 255$ and the grayscale secret image is in Fig. 2 (a). Figs. 2 (b-d) illustrate the 3 shares SC_1, SC_2 and SC_3, which are noise-like. Figs. 2 (e-h) exhibit the recovered secret images with any 2 or 3 shares based on CRT, from which the secret images recovered from $k = 2$ or more shares can be recognized, where $CRT(SC_1, SC_2)$ indicates the recovered secret image S' from SC_1 and SC_2 by CRT. In addition, we have $\sum_{h=1}^{H}\sum_{w=1}^{W}\left|S(h,w) - S'(h,w)\right| = 0$, therefore the recovered secret image is lossless by CRT.

Fig. 3 shows shares histogram analysis of the proposed CRTISS method corresponding to Fig. 2. For each share, the pixel values are approximately uniform distribution in $[0, m_i - 1]$, which tells that each share gives no clue about the secret image.

Fig. 4 demonstrates the experimental results for $(4, 4)$ threshold, where $p = 131, m_1 = 247, m_2 = 251, m_3 = 253, m_4 = 255$ and the gray secret image is displayed in Fig. 4 (a). Figs. 4 (b-e) indicate the generated 4 shares, which are also noise-like. Figs. 4 (f-h) denote the recovered secret image with any $t\,(2 \leq t \leq 4)$ based on CRT recovery. When $t < 4$ shares are collected, there is no clue about the secret image. While when 4 shares are collected, the secret image are recovered losslessly according to CRT.

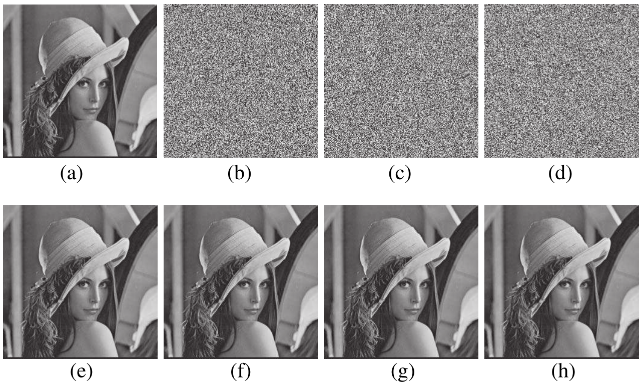


FIGURE 2. Experimental example of the proposed CRTISS method for (k, n) threshold, where $k = 2, n = 3$. (a) Secret image. (b) SC_1. (c) SC_2. (d) SC_3. (e) CRT($SC1$ $SC2$). (f) CRT($SC1$, $SC3$). (g) CRT($SC2$, $SC3$). (h) CRT($SC1$, $SC2$, $SC3$).

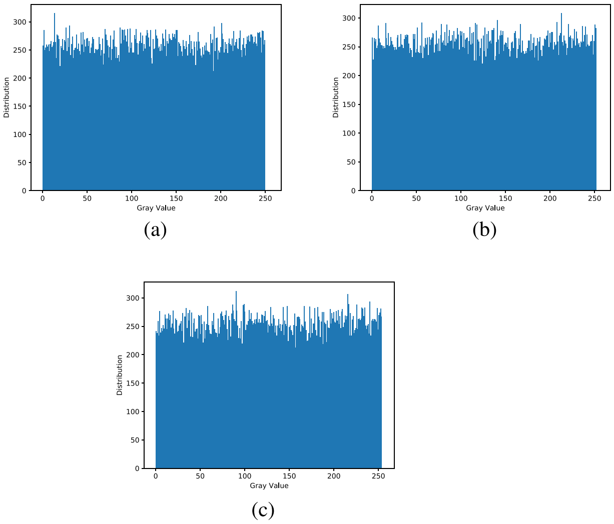


FIGURE 3. Shadow images histogram analysis of the proposed CRTISS method in Fig. 2. (a) Histogram of SC_1. (b) Histogram of SC_2. (c) Histogram of SC_3.

Fig. 5 gives the experimental results for $(3, 5)$ threshold, where $p = 128, m_1 = 245, m_2 = 247, m_3 = 249, m_4 = 251, m_5 = 253$ and the gray secret image is presented in Fig. 5 (a). Figs. 5 (b-f) show the 5 shares, which are also noise-like. Figs. 5 (g-j) illustrate the recovered gray secret image with any $t\,(2 \leq t \leq 5)$ (taking the first t shares as an example) by CRT recovery. When $t < k$ shares are collected, there is no clue about the secret image. While when k or more shares are collected, the secret image are reconstructed losslessly by CRT.

To illustrate the pixel values of shares are totally random in the range of $[0, m_i]$, we share a black image with every pixel at 0. Fig. 6 demonstrates the experimental results for $(2, 3)$ threshold, where $p = 128, m_1 = 251, m_2 = 253, m_3 = 255$. Figs. 6 (a-c) display the generated 3 shares, followed by their histogram images in Figs. 6 (d - f). It is

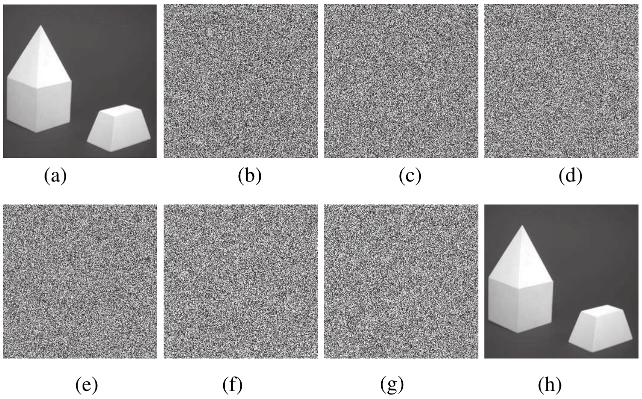


FIGURE 4. Experimental example of the proposed CRTISS method for (k, n) threshold, where $k = 4, n = 4$. (a) Secret image. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) CRT($SC1, SC2$). (g) CRT($SC1, SC2, SC3$). (h) CRT($SC1, SC2, SC3, SC4$).

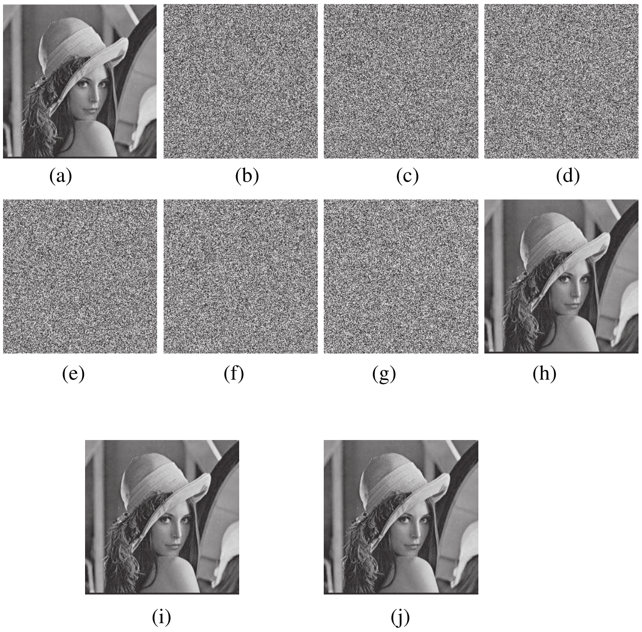


FIGURE 5. Experimental example of the proposed CRTISS method for (k, n) threshold, where $k = 3, n = 5$. (a) Secret image. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) SC_5. (g) CRT($SC1; SC2$). (h) CRT($SC1, SC2, SC3$). (i) CRT($SC1, SC2, SC3, SC4$). (j) CRT($SC1, SC2, SC3, SC4, SC5$).

noticeable that some pixel values don't appear in shares and the numbers of other values are very close, consistent with 1. What's more, when $k > 2$, the distribution of share pixels is approximately uniformly distributed, shown in Fig 7, where the black image is shared for $(3, 3)$ threshold with $p = 128, m_1 = 251, m_2 = 253, m_3 = 255$.

Based on the above results we can conclude that:

-The shares are noise-like, therefore the proposed scheme has no cross interference of secret image in single share.

-When $t < k$ shares are collected, there is no information of the secret image could be gained, which shows the security of the proposed scheme.

-When $t(k \leq t \leq n)$ shares are recovered by CRT, the secret image could be reconstructed losslessly by CRT.

-CRTISS method for (k, n) threshold is achieved.

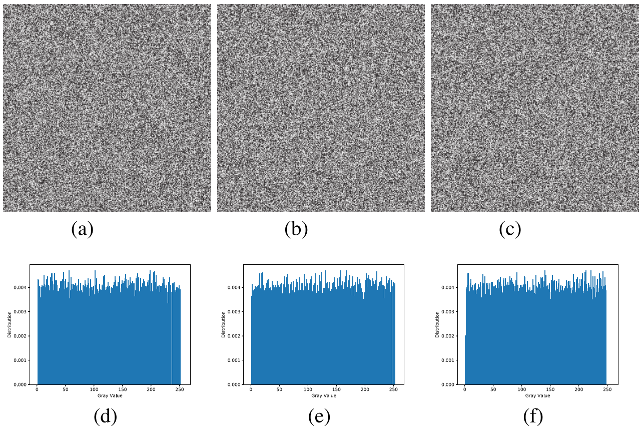


FIGURE 6. Experimental example of sharing the black image for (k, n) threshold, where $k = 2, n = 3$. (a) SC_1. (b) SC_2. (c) SC_3. (d) Histogram of SC_1. (e) Histogram of SC_2. (f) Histogram of SC_3.

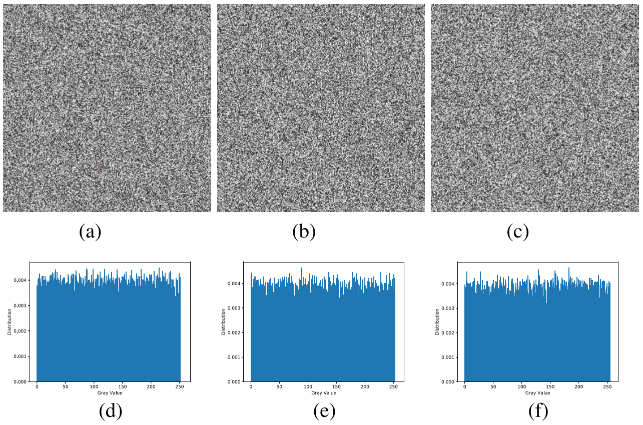


FIGURE 7. Experimental example of sharing the black image for (k, n) threshold, where $k = 3, n = 3$. (a) SC_1. (b) SC_2. (c) SC_3. (d) Histogram of SC_1. (e) Histogram of SC_2. (f) Histogram of SC_3.

TABLE 1. Available parameters of $m_1, m_2 \cdots, m_n$.

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

B. AVAILABLE PARAMETERS

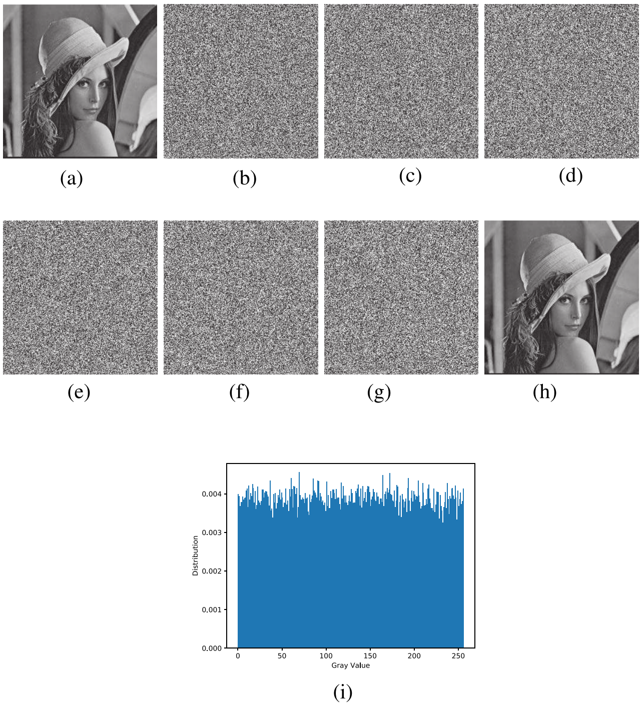
Some available parameters of $m_1, m_2 \cdots, m_n$ for different thresholds are shown in Table 1, which are applied in our above experiments as well. The parameter p is better to be 128 or 131. The user can also search other parameters according to specific applications.

C. COMPARISONS WITH RELATED WORKS

We will give the comparisons with some typical related CRTISS schemes [23]–[25], [27], [28]. We focus on the characteristics of auxiliary encryption, lossless recovery, (k, n)

TABLE 2. Comparisons with the related CRTISS schemes.

Schemes	Providing explicit parameters	Auxiliary encrpytion	Lossless recovery	(k,n)-threshold	Extra parameters transmission
Shyu *et al.* [23]	No	Yes	Yes	Yes	Yes
Hu *et al.* [25]	No	Yes	Yes	Yes	Yes
Ulutas *et al.* [24]	No	No	Yes (Conditional)	Yes (Conditional)	Yes
Chuang *et al.* [28]	No	No	No	Yes	Yes (for LSBs of pixels)
Yan *et al.* [27]	Yes	No	Yes	Yes	Yes
Our method	Yes	No	Yes	Yes	No


(a) (b) (c) (d)

(e) (f) (g) (h)

(i)

FIGURE 8. Experimental example of CRTISS method for (k, n) threshold, where $k = 3, n = 5$ and A in $\left[0, \left\lfloor \frac{M}{p} - 2\right\rfloor\right]$. (a) Secret image. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) SC_5. (g) $CRT(SC1, SC2)$. (h) $CRT(SC1, SC2, SC3)$. (i) Histogram of $CRT(SC1; SC2)$.

threshold and extra parameters transmission, which have a great influence on the applications of CRTISS. Since these characteristics are difficult to be evaluated with objective indicators, we only give the qualitative analyses to illustrate the better performance of our scheme.

In ISS, correlations between pixels have to be eliminated; otherwise, there would be information leakage in the shares, e.g., outline of objects. To scramble the pixel value as well as the correlations of adjacent pixels, Shyu *et al.* [23] and Hu *et al.* [25] both utilized auxiliary encryption in their methods. Since the computation complexity of CRT is relatively low and an image has the characteristic of big data amount, auxiliary encryption may bring unacceptable computation price. In our method, a random number A is generated to break the correlations. A is randomly picked up for every x, i.e., the high 7 bits of a pixel, and $y = x + Ap$ can enlarge x so as to scramble not only the pixel value but also the correlations between adjacent pixels without auxiliary encryption.

In Ulutas *et al.*'s ISS [24] based on the Asmuth and Bloom's scheme, the image pixels are divided into two intervals in order to obtain the lossless recovery. But they did not specify the range of the parameters. If A is in range of $\left[0, \left\lfloor \frac{M}{p} - 1\right\rfloor\right]$, x can be recovered with $k-1$ even less shares, which is not consistent with (k, n)-threshold. Furthermore, the case of $x > 2p$ is not considered, which may lead to lossy recovery. Yan *et al.*'s method [27] is also based on the Asmuth and Bloom's scheme through dividing the pixels into two intervals. They do give specific restrictions on the range of random number and p, making sure (k, n)-threshold will be achieved. But they need to share the parameter T to recover the secret image. In our method, only p, shares and their corresponding modular integers are going to be distributed, which is also required in Ulutas *et al.*'s and Yan *et al.*'s methods too.

In Chuang *et al.* [28]'s simple CRTISS, the high 7 bits of pixel are shared, the same as our method. But they have to store the LSB and distribute them to every participant, which brings a high price. Otherwise, they would suffer from a lossy recovery. We choose to embed the LSB into the last bit of the random integer, and therefore lossless recovery is achieved. Besides, they did not provide explicit restrictions on the parameters and the parameters in their experiments did not satisfy the proposed requirements. We specify the parameters and give some applicable examples in our method.

The comparison can be summarized in Table 2, and the advantages of our method are as follows:

1) It is a (k, n)-threshold ISS scheme without auxiliary encryption, which usually brings high computation complexity.
2) Less parameters need to be shared but lossless recovery is achieved, reducing the storage and transmission cost.
3) We give specific restrictions on the parameters as well as some applicable choice.

D. DISCUSSION

In the proposed scheme, the random integer A is chosen from $\left[\left\lceil \frac{N}{p}\right\rceil, \left\lfloor \frac{M}{p} - 2\right\rfloor\right]$, in order to achieve (k, n) threshold. However, in the practical ISS application, we can enlarge the interval of A to $\left[0, \left\lfloor \frac{M}{p} - 2\right\rfloor\right]$. The probability of picking up A from $\left[0, \left\lceil \frac{N}{p}\right\rceil\right]$ is $\left\lceil \frac{N}{p}\right\rceil / \left\lfloor \frac{M}{p} - 2\right\rfloor$. It approximates to $\frac{N}{M}$, which is smaller than $\frac{1}{p}$. An attacker has the probability of less than $\frac{1}{p}$ to recover a single secret pixel with $k-1$ shares. Since an image contains a large numbers of pixels, the security drawbacks can be ignored. Fig. 8 shows the sharing result for $(3, 5)$ threshold, where $p = 128, m_1 = 245, m_2 = 247, m_3 = 249, m_4 = 251, m_5 = 253$ and A ranges in $\left[0, \left\lfloor \frac{M}{p} - 2 \right\rfloor\right]$. Figs. 8(b-f) show the noise-like shares and (g) is the recovered result with only two shares, SC_1 and SC_2. Its histogram image is still approximately uniformly distributed, shown in Fig. 8 (i), which means we get nothing from the two shares. Of course, the secret image can be recovered losslessly with at least three shares, shown as Fig. 8 (h).

We suggest n less than 6. When n is bigger, it becomes harder to find suitable moduli. Since the range of shared pixels is limited to the corresponding modulus, worse distributed shares will be generated with the smaller modulus.

V. CONCLUSION

In this paper, we propose a (k, n)-threshold the Chinese remainder theorem-based image secret sharing (CRTISS) scheme. We study the features of images and analyze the obstacles to apply the Asmuth and Bloom's secret sharing (SS) method to ISS, including pixel value range, the correlations between adjacent pixels and so on. The proposed solution is to share the high 7 bits of pixels and embed the LSB into the random integer. We achieve the properties of (k, n) threshold, lossless recovery and no auxiliary encryption. Some applicable parameters are also provided. The effectiveness of our method is illustrated through theoretical proof and typical experiments. Future work may focus on using compact sequences of co-primes, which are easier to generate and may have better features.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.

[2] Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for QR code applications," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.

[3] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Exploiting the homomorphic property of visual cryptography," *Int. J. Digit. Crime Forensics (IJDCF)*, vol. 9, no. 2, pp. 45–56, 2017.

[4] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Inf. Sci.*, vol. 473, pp. 13–30, Jan. 2019.

[5] M. Fuyou, X. Yan, W. Xingfu, and M. Badawy, "Randomized component and its application to (t,m,n)-group oriented secret sharing," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 889–899, May 2015.

[6] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science). Perugia, Italy: Springer, 1995, pp. 1–12.

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

[8] G. Wang, F. Liu, and W. Q. Yan, "Basic visual cryptography using braille," *Int. J. Digit. Crime Forensics*, vol. 8, no. 3, pp. 85–93, 2016.

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

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

[11] M. Mignotte, *How to Share a Secret*. Berlin, Germany: Springer, 1983, pp. 371–375.

[12] W. Yan, W. Ding, and Q. Dongxu, "Image sharing based on Chinese remainder theorem," *J. North China Univ. Tech.*, vol. 12, no. 1, pp. 6–9, 2000.

[13] S. Wang, X. Yan, J. Sang, and X. Niu, "Meaningful visual secret sharing based on error diffusion and random grids," *Multimedia Tools Appl.*, vol. 75, no. 6, pp. 3353–3373, 2015.

[14] Z.-X. Fu and B. Yu, "Visual cryptography and random grids schemes," in *Digital-Forensics and Watermarking*. Auckland, New Zealand: Springer, 2014, pp. 109–122.

[15] T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids with improved contrast," *J. Syst. Softw.*, vol. 86, no. 8, pp. 2094–2109, 2013.

[16] Y. K. Meghrajani and H. S. Mazumdar, "Enhanced contrast of reconstructed image for image secret sharing scheme using mathematical morphology," *J. Inf. Secur.*, vol. 6, no. 4, pp. 273–279, 2015.

[17] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2653–2672, 2017.

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

[19] C.-N. Yang and C.-B. Ciou, "Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability," *Image Vis. Comput.*, vol. 28, no. 12, pp. 1600–1610, 2010.

[20] P. Li, C.-N. Yang, C.-C. Wu, Q. Kong, and Y. Ma, "Essential secret image sharing scheme with different importance of shadows," *J. Vis. Commun. Image Represent.*, vol. 24, no. 7, pp. 1106–1114, 2013.

[21] P. Li, C.-N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography," *J. Real-Time Image Process.*, vol. 14, pp. 41–50, Jan. 2018.

[22] Y.-X. Liu, C.-N. Yang, C.-M. Wu, Q.-D. Sun, and W. Bi, "Threshold changeable secret image sharing scheme based on interpolation polynomial," *Multimedia Tools Appl.*, pp. 1–15, Jan. 2019.

[23] S. J. Shyu and Y.-R. Chen, "Threshold secret image sharing by Chinese remainder theorem," in *Proc. IEEE Asia–Pacific Services Comput. Conf.*, Dec. 2008, pp. 1332–1337.

[24] M. Ulutas, V. V. Nabiyev, and G. Ulutas, "A new secret image sharing technique based on Asmuth bloom's scheme," in *Proc. Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2009, pp. 1–5.

[25] C. Hu, X. Liao, and D. Xiao, "Secret image sharing based on chaotic map and chinese remainder theorem," *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 10, no. 3, 2012, Art. no. 1250023.

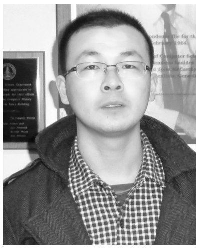
[26] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Chinese remainder theorem-based secret image sharing for (k, n) threshold," in *Cloud Computing Security*, X. Sun, H.-C. Chao, X. You, and E. Bertino, Eds. Cham, Switzerland: Springer, 2017, pp. 433–440.

[27] X. Yan, Y. Lu, L. Liu, J. Liu, and G. Yang, "Chinese remainder theorem-based two-in-one image secret sharing with three decoding options," *Digit. Signal Process.*, vol. 82, pp. 80–90, Nov. 2018.

[28] T.-W. Chuang, C.-C. Chen, and B. Chien, "Image sharing and recovering based on Chinese remainder theorem," in *Proc. Int. Symp. Comput., Consum. Control*, Jul. 2016, pp. 817–820.

LONGLONG LI was born in China, in 1995. He received the B.Sc. degree (Hons.) in automation from the University of Science and Technology of China, China, in 2017. He is currently pursuing the M.S. degree with the National University of Defense Technology, Hefei, China. His research interests include secret image sharing and steganalysis.

YULIANG LU was born in China, in 1964. He received the B.Sc. degree (Hons.) in computer application and the M.Sc. degree in computer application from Southeast University, China, in 1985 and 1988, respectively. He is currently a Professor with the National University of Defense Technology, Hefei, China. His research interests include computer application and information processing.



XUEHU YAN was born in China, in 1984. He received the B.Sc. degree (Hons.) in science in information & calculate science, the M.Sc. degree in computational mathematics, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, in China, in 2006, 2008, and 2015, respectively. He is currently an Associate Professor with the National University of Defense Technology, Hefei, China. His research interests include visual cryptography, secret image sharing, information hiding, cryptography, and multimedia security. He has published more than 100 papers in these areas. He is an Associate Editor of the *International Journal of Digital Crime and Forensics* (IJDCF).

LINTAO LIU was born in China, in 1989. He received the B.Sc. degree (Hons.) in computer application and the M.Sc. degree in information security from the National University of Defense Technology, Hefei, China, in 2012 and 2015, respectively, where he is currently pursuing the Ph.D. degree. His research interests include cryptography, multimedia security, and biometrics.

LONGDAN TAN was born in China, in 1987. She received the B.Sc. degree (Hons.) in computer application and the M.Sc. degree in information security from the Hefei Electronic Engineering Institute, China, in 2008 and 2011, respectively. She is currently pursuing the Ph.D. degree with the National University of Defense Technology, Hefei, China. Her research interest includes information security.