IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 12, 2019, accepted April 23, 2019, date of publication May 2, 2019, date of current version May 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914515

Weighted Secret Image Sharing for a (k, n) Threshold Based on the Chinese Remainder Theorem

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

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

This work is 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 In general, in a secret image sharing (SIS) scheme with a (k, n) threshold, the participants have equal weights, and their shares have the same average light transmission. No share can reveal any information about the secret. Only when the number of participants involved in restoration is greater than or equal to k can the secret image be revealed. However, on some occasions, the participants' weights need to be set differently, and their shares have different effects on the restoration of the secret image. Therefore, there are many studies of weighted SIS, including schemes based on visual secret sharing using random grids (VSSRG). However, they can only share binary images, not grayscale images. Therefore, we propose a scheme based on the Chinese remainder theorem (CRT) for sharing grayscale images. The shares are generated with different weights. When the threshold is reached and shares with higher weights are involved in restoration, the quality of the restored image is higher. As the number of participating shares increases, the quality of the recovered secret image increases, and if all the shares are involved, lossless restoration can be achieved.

INDEX TERMS (k, n) threshold, secret image sharing, the Chinese remainder theorem, weighted secret image sharing.

I. INTRODUCTION

Secret sharing (SS) was proposed by Shamir [1] and Blakley [2] separately in 1979 to protect the key. The secret image sharing (SIS) scheme is the extension of SS to images. In SIS, the secret image is split into n noise-like shadow images, i.e., shares or shadows, which are then distributed to n different participants. The secret image can be reconstructed from k or more shadow images, while combining fewer than k shadow images reveals nothing about the secret image. This scheme is called the (k, n)-threshold scheme. Shamir proposed polynomial-based SS for the (k, n)-threshold scheme. Thien and Lin [3] extended the SS scheme of Shamir to digital images, which was the first (k, n)-threshold SIS. Shamir's polynomial-based SS can also be used with digital images since the secret image is divided into $(k - 1)$ random polynomial coefficients to obtain n shares. The recovered secret images in Shamir's and Thien and Lin's schemes are lossy.

Noar and Shamir [4] were the first to propose threshold-based VSS, which is also called visual cryptography (VC), in 1995. The ability to superimpose a qualified number of shares to recover the secret image without computation or cryptographic knowledge is the advantage of VSS. However, the pixel expansion problem and its codebook (basic matrices) design are the inevitable defects of the scheme.

Random grid (RG)-based VSS [5], [6] was proposed by Kafri and Keren; this approach avoids pixel expansion, and codebook design is not necessary. However, as increasing numbers of shares are stacked to reveal the secret image, the background of the reconstructed secret image becomes darker.

VSS is often used to share binary images, while SIS based on the CRT (CRTSIS) is used to share grayscale images. Compared to polynomial-based SIS, CRTSIS has the advantages of lossless recovery and low computational complexity. Mignotte put forward the first (k, n)-threshold SS scheme

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

based on the CRT in 1982 [7]. Asmuth and Bloom [8] proposed a threshold SS scheme based on the CRT with random factors, which Mignotte's scheme lacks. Yan *et al.* first [9] introduced the CRT in a SIS, which may have slight information leakage and lossy recovery. Shyu and Chen [10] proposed a threshold CRTSIS based on Mignotte's scheme using a pseudo-random number generator with auxiliary encryption. Yan *et al.* [11] implemented a (k, n)-threshold CRTSIS and lossless recovery for grayscale images without auxiliary encryption. The size of the shares was decreased based on the CRT by adding random bits in the study of Chen *et al.* [12]. Yan and Lu [13] proposed a general SIS construction method by using meaningful shares without pixel expansion. Yan *et al.* proposed a two-in-one SIS scheme with three decoding options based on the CRT [14].

In the above schemes, the number of participants is very important for the restoration of secrets. Participants have the same importance and weight. Weighted SS was first proposed by Shamir in [1], in which the participants do not have the same status. Iftene and Boureanu [15] proposed a weighted threshold SS based on the CRT. In the weighted threshold SS schemes, each participant is assigned a positive weight, and the secret can be reconstructed when the sum of the weights of all participants is no less than a given threshold. Weighted threshold schemes are studied in [16]–[18]. Hou *et al.* [19] implemented a $(2, n)$-threshold VSS without pixel expansion, in which a novel privilege-based VSS model was proposed that allows participants to have different weights. In the recovery phase, participants with higher priority weights recover more information about the secret image. In contrast, participants with lower priority weights reveal less information. However, a codebook is necessary, and the average light transmission of each share is not identical. Thus, the different priorities of the shares are exposed by the average light transmission. Yang *et al.* [20] modified the scheme of Hou *et al.* to make the average light transmissions of the shares identical, but their scheme requires a codebook. Chao and Fan [21] proposed a (k, n)-threshold priority RG VSS that gives each share a different priority weight. The advantages of this scheme are that no codebook is required and that the average light transmissions of the shares are the same. However, VSS schemes with different priority weights can only be used to share binary images.

On some occasions, the secret image is a grayscale image, and participants have different rights. Shares owned by heavily weighted participants greatly impact the restoration of secret images. Therefore, it is necessary to assign shares with more secret information to participants with higher weights and vice versa. When the shares are transmitted through the communication channel, the transmission quality of the communication channel is different, and the weights of the shares can be set differently to better adapt to the communication channel. In this paper, we propose a weighted SIS for a (k, n) threshold based on the CRT to share grayscale image in scenarios such as those mentioned above. In our scheme, the (k, n)-threshold CRTSIS in Yan *et al.*'s scheme [11] is used to share every pixel of a grayscale image to create k pixel values, which are assigned to the corresponding positions of k shares. Then, the k shares are selected from n participants by their weights. The same positions in the remaining $n - k$ shares are filled with their privacy moduli. In this way, our scheme has the following features. First, each share looks random, and none of the information in the secret image can be revealed from a single share. Second, the shares have different priority weights. Third, when more than a threshold number of shares are used to restore the secret, as the number increases, the quality of the restored secret image increases. When shares with higher weights participate in the restoration, the quality of the recovered secret image is higher, and when all the shares are involved, the secret image is restored losslessly.

The rest of the paper is organized as follows. The CRT, the (k, n)-threshold CRTSIS and the definition of the correct recovery probability (CRP) are introduced in Section 2. The secret image sharing and recovery algorithms are described in Section 3. Section 4 describes theoretical analyses of our proposed scheme. Section 5 presents the experimental results and comparisons. Finally, Section 6 is the conclusion of this paper.

II. PRELIMINARIES

A. CHINESE REMAINDER THEOREM (CRT)

The Chinese remainder theorem (*CRT*) is a method of solving a group of linear congruences used in ancient China, and is also known as the Sun Tzu theorem. A set of integers $m_i (i = 1, 2, \cdots, k)$ is selected and subject to $\gcd(m_i, m_j) = 1, i \neq j$.

Then, there exists only one solution $y \in [0, M-1]$ and $y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod{M}$ for the following system of linear 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 $M_i M_i^{-1} \equiv 1 \pmod{m_i}$.

$\gcd(m_i, m_j) = 1, i \neq j$; thus, no equation in Eq. (1) can be eliminated using other equations.

For any integer $a_1, a_2, \ldots, a_k$, the system of equations has solutions. In $[0, M-1]$, there exists only one solution. When we only collect the first $k-1$ equations in Eq. (1), in $[0, \prod_{i=1}^{k-1} m_i - 1]$, only one solution satisfying the first $k-1$ equations can be obtained, and we denote it as y_0. $y_0 + b\prod_{i=1}^{k-1} m_i$ in $[0, M-1]$ are also solutions for the first $k-1$ equations in Eq. (1), where $b = 1, 2, \cdots, m_i - 1$. Thus, in $[\prod_{i=1}^{k-1} m_i, M-1]$, there are $m_i - 1$ additional solutions, not just one. This conclusion is used in our proposed (k, n) threshold scheme.

B. (k, n)-THRESHOLD SIS BASED ON THE CRT (SISCRT)

The Chinese remainder theorem has many applications in the RSA decryption algorithm, the discrete logarithm algorithm and the algorithm for recovering the secret. In this paper, we use the CRT to implement our (k, n)-threshold SIS scheme.

The CRT in the scheme of Yan *et al.* [11] is used in our scheme since it has the advantages of lossless recovery, low computational complexity and no need for auxiliary encryption. The CRT in the scheme of Yan *et al.* [11] is described as follows.

A set of integers $128 \leq p < m_1 < m_2 \cdots < m_n \leq 256$ are chosen 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 to all the participants. T is public to all the participants as well; $T = \left\lfloor \frac{\left\lfloor \frac{M}{p} - 1 \right\rfloor - \left\lceil \frac{N}{p} \right\rceil}{2} + \left\lceil \frac{N}{p} \right\rceil \right\rfloor$.

For each pixel value x in the secret image, if $0 \leq x < p$, a random integer A in $\left[T+1, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ is selected, and $y = x + Ap$. Otherwise, a random integer A is selected from $\left[\left\lceil \frac{N}{p} \right\rceil, T\right)$ and $y = \text{x-p} + Ap$. Then, $a_i \equiv y \pmod{m_i}$ are computed and distributed to the corresponding participants to generate n shares.

When we are recovering the secret image, k arbitrary congruence equations are used to compute $T^* = \left\lfloor \frac{y}{p} \right\rfloor$. If $T^* \geq T$, then $x \equiv y \pmod{p}$. Otherwise, $x = y \pmod{p} + p$. Every pixel in the secret image is computed in the same way, and the secret image can be recovered losslessly.

C. CORRECT RECOVERY PROBABILITY (CRP)

Definition 1 (Correct Recovery Probability (CRP) [22]): For a grayscale secret image S and its recovered image S' with the same size, $M \times N$, the correct recovery probability of the recovered image S' is defined practically by comparing the recovered image S' with the original secret image S. It is the ratio of the number of identical pixels in the same positions in the two pictures to the total number of the pixels in the image, described by following equation, where T is the number of identical pixels in the same positions in the two pictures:

$$CRP(S) = \frac{T}{M \times N} \tag{2}$$

The (k, n)-threshold SIS based on the CRT (*CRTSIS*) and the definition of the correct recovery probability (CRP) are used in our proposed scheme.

III. PROPOSED WEIGHTED SIS SCHEME FOR A (K, N) THRESHOLD BASED ON THE CRT

A. THE MAIN IDEA

In our scheme, each participant's share is assigned a weight. The sum of the weights is equal to 1. We first use the CRTSIS in the scheme of Yan *et al.* [11] to share each pixel in the secret image to generate n values. For each position, k shares, which are selected according to their weights, are assigned k values, and the same position in the remaining $n - k$ shares is filled with the corresponding privacy modulus. The n generated shares look random.

When we recover the secret image, the secret cannot be recovered from fewer than k shares. When more than k shares are collected, the secret image is revealed. The higher the weights of the shares participating in the restoration of secret image are, the higher the quality of the recovered image is and vice versa. As the number of shares increases, the quality improves. If all the shares are collected, the secret image is recovered losslessly. Our sharing steps are described in Algorithm 1. Figure 1 shows the design concept of the sharing phase. Algorithm 2 shows the recovery phase.

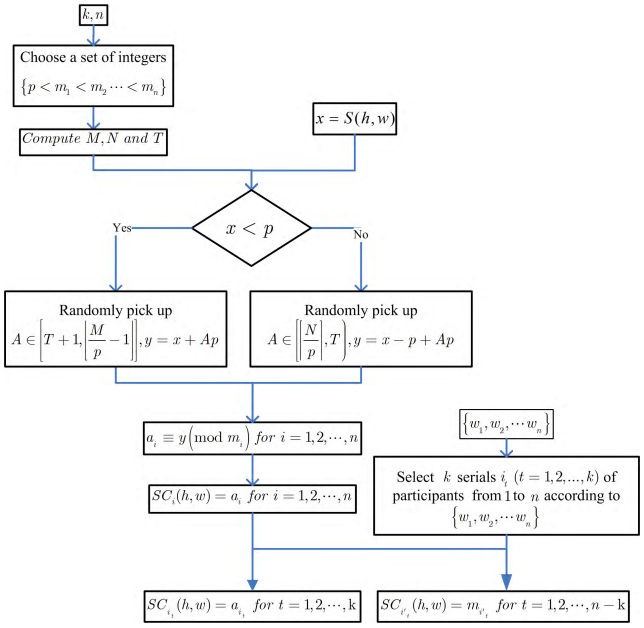


FIGURE 1. The idea behind generating shares with different weights in our (k, n)-threshold scheme.

B. THE SHARING PHASE

The corresponding algorithm steps are described in Algorithm 1. A grayscale secret image S of size $H \times W$, the threshold parameters (k, n) and the weights $W = \{w_1, w_2, \cdots w_n\}$ are the inputs to the algorithm. The outputs are n grayscale shares $SC_1, SC_2, \cdots, SC_n$.

In Algorithm 1, weight generation is performed before each share value is assigned. For the weights $W = \{w_1, w_2, \cdots w_n\}$ with $w_1 + w_2 + \cdots w_n = 1$, in line 14, we assign the weights to the corresponding participants. In line 16, we randomly select k serial numbers of participants from $\{1, 2, \cdots, n\}$ according to their weights, denoted by $i_1, i_2, \cdots i_k$.

For example, we divide the interval of [0,1) into n intervals, as shown in Figure 2, and assign w_i as the weight of each participant. When we share one pixel of the

Algorithm 1 Proposed Weighted SIS for the (k, n) Threshold Based on the CRT

Require: A grayscale secret image S of size $H \times W$; the threshold parameters (k, n); and the weights $W = \{w_1, w_2, \cdots w_n\}, w_1 + w_2 + \cdots w_n = 1$.

Ensure: n grayscale shares $SC_1, SC_2, \cdots, SC_n$.

1: Choose a set of integers $\{128 \le p < m_1 < m_2 \cdots < m_n \le 256\}$ subject to
   1) $\gcd(m_i, m_j) = 1, i \ne j$.
   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 to all the participants.

2: Compute $T = \left\lfloor \frac{\left\lfloor \frac{M}{p} - 1 \right\rfloor - \left\lceil \frac{N}{p} \right\rceil}{2} + \left\lceil \frac{N}{p} \right\rceil \right\rfloor$ and T is public to all the participants as well.

3: **for** $h = 1$ to H **do**

4: **for** $w = 1$ to W **do**

5: Let $x = S(h, w)$.

6: **if** $0 \le x < p$ **then**

7: Select a random integer A in $\left[T + 1, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ and let $y = x + Ap$.

8:

9: **else**

10: Select a random integer A in $\left[\left\lceil \frac{N}{p} \right\rceil, T\right)$ and let $y =$ x-p $+ Ap$.

11: **end if**

12: **for** $i = 1$ to n **do**

13: Compute $a_i \equiv y \pmod{m_i}$

14: Assign w_i to the weight of participant i.

15: **end for**

16: Randomly select k serial numbers for participants from $\{1, 2, \cdots, n\}$ according to their weights denoted by $i_1, i_2, \cdots i_k$; the remaining $n - k$ serial numbers of the n participants are denoted by $\{i'_1, i'_2, \cdots i'_{n-k}\} = \{1, 2, \cdots, n\} \backslash \{i_1, i_2, \cdots i_k\}$.

17: For $i_1, i_2, \cdots i_k$, let $SC_{i_1}(h, w) = a_{i_1}$, $SC_{i_2}(w, h) = a_{i_2}$, and $\cdots$ $SC_{i_k}(h, w) = a_{i_k}$. For $\{i'_1, i'_2, \cdots i'_{n-k}\}$, let $SC_{i'_1}(h, w) = m_{i'_1}$, $SC_{i'_2}(w, h) = m_{i'_2}$, $\cdots$ $SC_{i'_{n-k}}(h, w) = m_{i'_{n-k}}$.

18: **end for**

19: **end for**

20: Output n shares $SC_1, SC_2, \cdots SC_n$ with size $H \times W$ and their corresponding privacy moduli $m_1, m_2, \cdots m_n$.

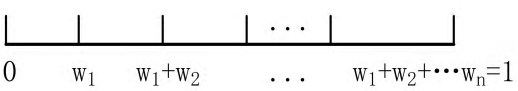


FIGURE 2. An example of weight interval partition.

secret image, we randomly generate a number x between 0 and 1. If $x \in [0, w_1)$, participant 1 is selected; if $x \in [w_1, w_1 + w_2)$, participant 2 is selected analogously; if $x \in [w_1 + w_2 + \cdots w_{i-1}, w_1 + w_2 + \cdots w_{i-1} + w_i)$, participant i is selected. This process is repeated until k different participants are selected, whose serial numbers are $i_1, i_2, \cdots i_k$. The serial numbers of the remaining $n - k$ participants are $i'_1, i'_2, \cdots i'_{n-k}$. The corresponding pixels of the shares of participants $i_1, i_2, \cdots i_k$ are assigned as $a_{i_1}, a_{i_2}, \cdots a_{i_k}$. The remaining $n - k$ corresponding pixels of the shares of participants $i'_1, i'_2, \cdots i'_{n-k}$ are assigned as their corresponding moduli $m_{i'_1}, m_{i'_2}, \cdots m_{i'_{n-k}}$. The selection of moduli is very special, and it is very important for decrypting secret images. If other values are chosen instead of the corresponding moduli, then the equation used for decryption cannot be selected, and correct decryption cannot be performed.

C. THE RECOVERY PHASE

The recovery phase is described in Algorithm 2. $t(k \le t \le n)$ arbitrary shares and their corresponding privacy moduli $m_{i_1}, m_{i_2}, \cdots m_{i_t}, p$ and T are the input parameters. The recovered image is the output. The number and weights of the shares affect the quality of the reconstructed secret image.

When we recover the secret image, we first determine whether the pixel value of each participant's shadow image is equal to its privacy moduli to select the equation involved in recovering the secret information. Then, the pixel values

Algorithm 2 Secret Image Recovery in the Proposed Scheme

Require: $t(k \le t \le n)$ shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}$ of size $H \times W$; their corresponding privacy moduli $m_{i_1}, m_{i_2}, \cdots m_{i_t}$; p and T.

Ensure: The reconstructed secret image S'.

1: **for** $h = 1$ to H **do**

2: **for** $w = 1$ to W **do**

3: **for** $j = 1$ to t **do**

4: Read pixel (h, w) of SC_{i_j}, denoted by $SC_{i_j}(h, w)$. If $SC_{i_j}(h, w) = m_{i_j}$, give up $SC_{i_j}(h, w)$.

5: **end for**

6: The remaining q $SC_{i_j}(h, w)$ are denoted by $a_{l_1}, a_{l_2}, \cdots a_{l_q} (q \ge k)$ and their corresponding privacy moduli, denoted by $m_{l_1}, m_{l_2}, \cdots m_{l_q}$, are used to solve the following linear equations with the Chinese remainder theorem.

$$\begin{aligned} y &\equiv a_{l_1} \pmod{m_{l_1}} \\ y &\equiv a_{l_2} \pmod{m_{l_2}} \\ &\cdots \\ y &\equiv a_{l_{q-1}} \pmod{m_{l_{q-1}}} \\ y &\equiv a_{l_q} \pmod{m_{l_q}} \end{aligned} \tag{3}$$

7: Compute $T^* = \left\lfloor \frac{y}{p} \right\rfloor$. If $T^* \ge T$, let $x \equiv y \pmod{p}$. Else let $x = y \pmod{p} + p$.

8: Set $S'(h, w) = x$.

9: **end for**

10: **end for**

11: Output the recovered secret image S'.

of the secret image are calculated by using the remaining congruence formula based on the CRT.

IV. THEORETICAL ANALYSES

In this section, we first prove that our method is a valid SIS construction scheme for the (k, n) threshold. Then, we define the correct recovery probability (CRP) to describe the quality of the recovered secret image and compute it as $CRP(S)$. Next, we obtain $CRP_{pro}(S)$ for each recovered secret image according to the weight of each share. Finally, we analyze the influence of the number and weights of the shares on the CRP of the corresponding recovered image.

1) (k, n) THRESHOLD FOR OUR SCHEME

Lemma 1: No share generated from our (k, n)-threshold scheme provides any clues about the original secret image.

Proof: From $y = x + Ap$ or $y =$ x-p $+ Ap$ and $a_i \equiv y \pmod{m_i}$, when A is fixed, since x represents the pixel value of the secret image, we assume that x and $x-p$ are random and in $[0, 255]$. Because $a_i \equiv (x+Ap) \pmod{m_i}$, a_i is random and in $[0, m_i)$. When we share the grayscale image, we first select k shares and set their values to $SC_{i_t}(h, w) = a_{i_t}(1 \le t \le k)$, which are random and in $[0, m_i)$. The remaining $n-k$ shares are set to their privacy moduli m_i, which are not relevant to the secret image. Therefore, the Lemma is proved. ■

Lemma 2: In the proposed scheme, $k-1$ or fewer shares give no clues about the secret image.

Proof: When $k-1$ shadow pixels $a_{i_1}, a_{i_2}, \cdots a_{i_{k-1}}$ are given, according to the CRT, 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 the one hand, the true $y \in [N, M-1]$, which is absolutely different from the above y_0. On the other hand, since $N \ge N_2$, $N \le y < M$ 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 solutions for the $k-1$ collected equations in Eq. (4). Thus, there are $m_{i_k} - 1$ more solutions in $[N_2, M-1]$, not just one. As we recover the value of each pixel in the secret image, we first screen the corresponding values in the shares used to calculate the pixel values in the secret image. The number of the remaining pixels is no less than $k-1$. Thus, $k-1$ or fewer shares give no clues about the secret image. ■

Lemma 3: In the proposed scheme, any k or more shares can reveal the secret image, and when $k = n$, the secret image can be recovered losslessly.

Proof: When we are recovering the value of each pixel in the secret image, we first screen the corresponding share values used to calculate the secret image by comparing the pixel values in the shares to their privacy moduli. Since the pixel values of the shares are selected according to the weights when they are generated, the number of remaining pixels with values greater than k accounts for a certain proportion.

When the number is less than $k-1$, the recovered pixel value in the secret image is not correct, which is proven by Lemma 2. When the number of remaining shares is greater than k, we use k $a_{i_1}, a_{i_2}, \cdots a_{i_k}$ to recover the secret. To recover x, we only need to find y due to $x \equiv y \pmod{p}$ or $x \equiv y \pmod{p} + p$. According to the CRT, there exists only one solution y modulo $N_1 = \prod_{j=1}^{k} m_{i_j}$ since $N_1 \ge M$. Finally, we can uniquely determine y and thus x based on Step 9 of our Algorithm 2. Therefore, the value of the pixel in the same position of the secret image can be recovered. A proportion of the secret information in the whole secret image can be revealed.

When $k = n$, the number of remaining pixels is never less than k. Therefore, every pixel of the secret image can be recovered. ■

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

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

2) CORRECT RECOVERY PROBABILITY (CRP) FOR OUR SCHEME

Theorem 2: In our scheme, each share has weight w_i, and $\sum_{i=1}^{n} w_i = 1$. When we recover the secret image using t arbitrary shares in Algorithm 2, we use the weights of the shares to deduce the CRP of the recovery image theoretically as $CRP_{pro}(S)$ according to Definition 1, which is computed in Eq.(4).

$$CRP_{pro}(S) = \frac{\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \tag{4}$$

Proof: The weight of share i_j is denoted by w_{i_j}, $C_t^k (k \le t \le n)$ denotes the number of combinations of k arbitrary shares of t, where t shares are used to recover the secret in Algorithm 2. C_n^k denotes the number of combinations of k arbitrary shares from n. $\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}$ denotes the probability sum of combinations of k arbitrarily selected shares from t. $\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}$ denotes the probability sum of combinations of k arbitrarily selected shares from n. Therefore, the CRP of the recovered image can be computed as shown in Eq.(4). ■

3) THE EFFECT OF THE NUMBER AND WEIGHTS OF THE SHARES ON THE CRP

When we use a set of shares to recover the secret image, its serial number is A. When we add shares to recover the image, the set of serial numbers is B. We conclude that $A \subset B$ and that $|A| < |B|$. Therefore, we use $t+1$ shares, which includes t shares, to recover the secret, supposing that share l is a newly added share. The CRP for $t+1$ shares is denoted by $(CRP^*_{pro}(S)$, which is computed as shown in Eq.(5).

$$CRP^*_{pro}(S) = \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \tag{5}$$

The result of subtracting is Eq.(6).

$$\begin{aligned} &CRP^*_{pro}(S) - CRP_{pro}(S) \\ &= \frac{\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} - \sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &= \frac{[\sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i_j^*})] - \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j}}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \\ &= \frac{w_l(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i_j^*})}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} > 0, i_j^* \neq l. \end{aligned} \tag{6}$$

In Eq.(6), the denominator of $CRP^*_{pro}(S)$ is the same as that of $CRP_{pro}(S)$, and the numerator of $CRP^*_{pro}(S)$ is $\sum_{i=1}^{C_{t+1}^k} \prod_{j=1}^{k} w_{i_j} = \sum_{i=1}^{C_t^k} \prod_{j=1}^{k} w_{i_j} + w_l(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k-1} w_{i_j^*})$, where $i_j^* \neq l$. Therefore, the numerator of $CRP^*_{pro}(S)$ is greater than that of $CRP_{pro}(S)$, and $CRP^*_{pro}(S)$ is greater than $CRP_{pro}(S)$. Therefore, the CRP increases with the number of shares.

When we keep t constant, we choose a share with a greater weight to restore the secret image. Assuming that the original weight of the share is w_u and replacing it with a larger weight w_v, where $w_u < w_v$, the original CRP is denoted by Eq.(7).

$$CRP^b_{pro}(S) = \frac{(\sum_{i=1}^{C_{t-1}^k} \prod_{j=1}^{k} w_{i_j^*} + w_u(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k} w_{i_j^*}))}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \tag{7}$$

In Eq.(7), $i_j^* \neq u$. The new expression for the CRP is given in Eq.(8).

$$CPR^a_{pro}(S) = \frac{(\sum_{i=1}^{C_{t-1}^k} \prod_{j=1}^{k} w_{i_j^*} + w_v(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k} w_{i_j^*}))}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} \tag{8}$$

In Eq.(7), $i_j^* \neq u$. The result of subtracting is given in Eq.(6).

$$\begin{aligned} &CPR^a_{pro}(S) - CPR^b_{pro}(S)) \\ &= \frac{(w_v - w_u)(\sum_{i=1}^{C_{t-1}^{k-1}} \prod_{j=1}^{k} w_{i_j^*})}{\sum_{i=1}^{C_n^k} \prod_{j=1}^{k} w_{i_j}} > 0 \end{aligned} \tag{9}$$

From Eq.(9), we see that $CPR^a_{pro}(S)$ is greater than $CPR^b_{pro}(S)$. Therefore, when the number of shares t is the same, the CRP of the secret image restored by choosing the share with the greater weight is higher.

In summary, the number and the weights both affect the CRP of the recovered secret image.

V. EXPERIMENTS AND COMPARISONS

In this section, experiments and comparisons with others' schemes are described to illustrate the effectiveness of our scheme.

A. IMAGE ILLUSTRATION

In this subsection, three experimental examples with $(2, 4)$, $(3, 4)$, and $(2, 3)$ thresholds are given, which prove that our scheme implements a (k, n) threshold. Figure 3 illustrates our $(2, 4)$-threshold scheme for $(p, m_1, m_2, m_3, m_4) = (131, 247, 249, 251, 253)$. The weights of the shares are $W = [0.1, 0.2, 0.3, 0.4]$. Figure 3a presents a grayscale secret image of size 256*256. Figures 3$b - e$ show the shares. Figures 3$f - k$ show the recovered images reconstructed from two shares. Figures 3$l - o$ show the recovered images reconstructed from three shares. Figure 3p presents the recovered image reconstructed from all the shares. The serial numbers of the shares involved are subscripted to the names. Starting with Figure 3f, the secret image has been partially revealed, and the quality gradually improves with the increasing number and weight of the shadow images involved in the restoration.

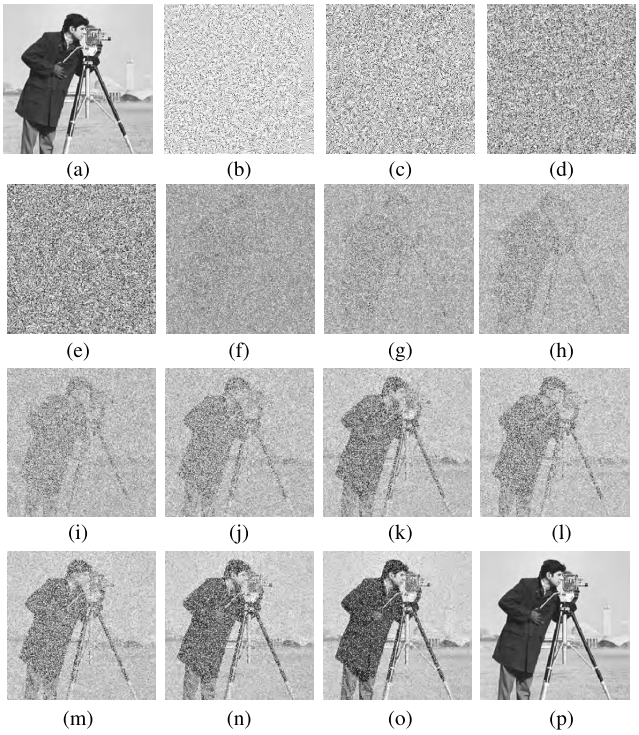


FIGURE 3. Our (2, 4)-threshold weighted SIS based on the CRT. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) S_{12}. (g) S_{13}. (h) S_{14}. (i) S_{23}. (j) S_{24}. (k) S_{34}. (l) S_{123}. (m) S_{124}. (n) S_{134}. (o) S_{234}. (p) S_{1234}.

Figure 4 displays our $(3, 4)$-threshold scheme with $(p, m_1, m_2, m_3, m_4) = (131, 247, 249, 251, 253)$. The weights of the shares are $W = [0.1, 0.2, 0.3, 0.4]$. Figure 4a depicts a grayscale secret image of size 256*256. Figures 4$b-e$ present the shares. Figures 4$f - k$ show the recovered images reconstructed from two shares. Figures 4$l - o$ show the recovered images reconstructed from three shares. Figure 4p presents the recovered image reconstructed from all the shares. The serial numbers of the shares involved are subscripted to the names. From Figure 4, we see that when fewer than three shares are involved in the recovery phase, the secret image

TABLE 1. The $CRP_{pro}(S)$ and $CRP(S)$ of recovered secret images for different combinations of t shares for the (2, 4) threshold.

(2,4) threshold	(1,2)	(1,3)	(1,4)	(2,3)	(2,4)	(3,4)	(1,2,3)	(1,2,4)	(1,3,4)	(2,3,4)	(1,2,3,4)
$\text{CRP}_{pro}(S)$	0.057	0.086	0.114	0.171	0.229	0.343	0.314	0.400	0.543	0.743	1
CRP(S)	0.050	0.079	0.114	0.164	0.232	0.374	0.288	0.391	0.562	0.765	1

TABLE 2. The $CRP_{pro}(S)$ and $CRP(S)$ of recovered secret images for different combinations of t shares for the (3, 4) threshold.

(3,4) threshold	(1,2)	(1,3)	(1,4)	(2,3)	(2,4)	(3,4)	(1,2,3)	(1,2,4)	(1,3,4)	(2,3,4)	(1,2,3,4)
$\text{CRP}_{pro}(S)$	-	-	-	-	-	-	0.120	0.160	0.240	0.480	1
CRP(S)	0.002	0.002	0.001	0.001	0.001	0.001	0.078	0.128	0.241	0.553	1

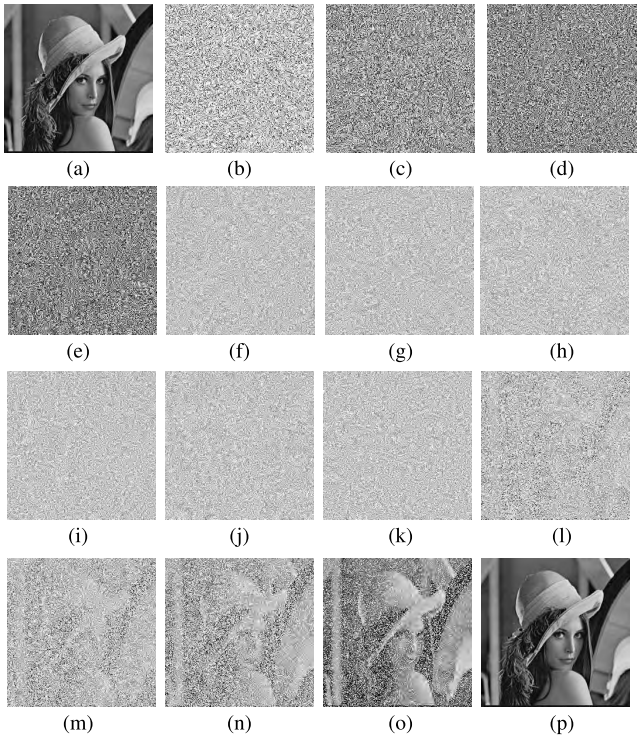


FIGURE 4. Our (3, 4)-threshold weighted SIS based on the CRT. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) SC_4. (f) S_{12}. (g) S_{13}. (h) S_{14}. (i) S_{23}. (j) S_{24}. (k) S_{34}. (l) S_{123}. (m) S_{124}. (n) S_{134}. (o) S_{234}. (p) S_{1234}.

is not revealed. When three or more shares participate in the restoration, the secret image is gradually revealed.

Figure 5 displays our $(2, 3)$-threshold scheme with $(p, m_1, m_2, m_3, m_4) = (128, 247, 251, 253)$. The weights of the shares are $W = [0.2, 0.3, 0.5]$. Figure $5a$ depicts a grayscale secret image of size 512*512. Figures $5b-d$ show the shares. Figures $5e-g$ present the recovered images reconstructed from two shares. Figure $5h$ displays the recovered image reconstructed from all the shares. The serial numbers of the shares involved subscripted to the names. The secret image restoration also has progressive characteristics. All the final recovered images in Figure 3, Figure 4 and Figure 5 are lossless.

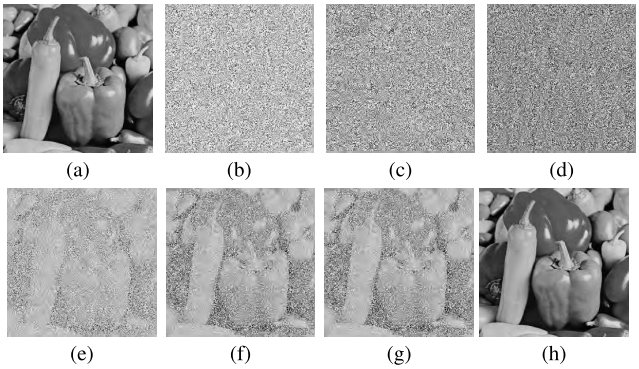


FIGURE 5. Our (2, 3)-threshold weighted SIS based on the CRT. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) S_{12}. (f) S_{13}. (g) S_{23}. (h) S_{123}.

TABLE 3. The $CRP_{pro}(S)$ and $CRP(S)$ of recovered secret images for different combinations of t shares for the (2, 3) threshold.

(2,3) threshold	(1,2)	(1,3)	(2,3)	(1,2,3)
$\text{CRP}_{pro}(S)$	0.194	0.323	0.484	1
CRP(S)	0.163	0.326	0.516	1

B. QUALITY OF THE IMAGES RECOVERED WITH OUR SCHEME

We use the CRP to evaluate the quality of our recovered images. The effectiveness of our scheme in terms of the CRP is analyzed in the following experimental results.

We use Eq.(2) to compute $CRP(S)$ and Eq.(4) to compute $CRP_{pro}(S)$ for the recovered images in Figures 3, 4 and 5. The results are displayed in Tables 1, 2 and 3. The first row of each table is the combination of different shares involved in restoring the secret image. The second row is the theoretical result calculated with Eq.(2) according to the weights of the shares, and the third row is the practical result calculated with Eq.(4) according to Definition 1. From these tables, we note that the following:

1. The practical results for $CRP(S)$ are very close to the theoretical results for $CRP_{pro}(S)$.

TABLE 4. Comparisons of the characteristics of other schemes and ours.

	Hou *et al.*'s scheme [19]	Yang *et al.*'s scheme [20]	Chao *et al.*'s scheme [21]	Yan *et al.*'s scheme [11]	Ours
Secret image format	Binary image	Binary image	Binary image	Grayscale image	Grayscale image
Encryption and decryption methods	VSS	VSS	VSS	CRT	CRT
Additional information	codebook	codebook	weight generation and RG	modulus	weight generation and modulus
Shares with equal average light transmission	No	Yes	Yes	Yes	No
priority	Yes	Yes	Yes	No	Yes
threshold	(2,n)	(2,n)	(k,n)	(k,n)	(k,n)
Is lossless?	No	No	No	Yes	Yes

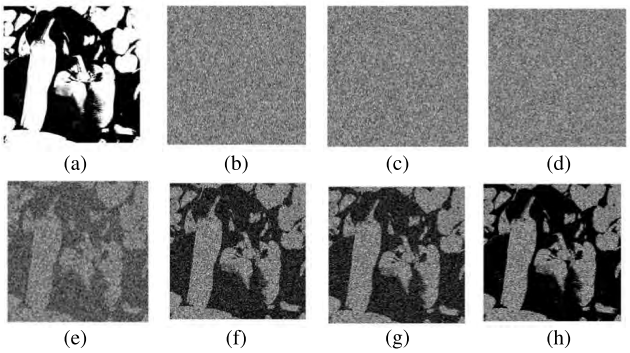


FIGURE 6. Chao's (2, 3)-threshold VSS based on RG. (a) S. (b) SC_1. (c) SC_2. (d) SC_3. (e) S_{12}. (f) S_{13}. (g) S_{23}. (h) S_{123}.

2. As the weight of the shares involved in the restoration of the secret image increases, the CRP of the recovered image also increases. The greater the weight of the share is, the stronger its impact on the recovered image is, and vice versa. This result is consistent with the conclusion of Section IV-.3.

3. When all the shares are involved in the restoration of the secret image, compared to the original secret image, the recovered image is lossless.

4. In the (3, 4)-threshold scheme, when we only use two images, that is, t is equal to 2, the CRP of the recovered image is very low; therefore, we cannot reveal the secret image. The formula for calculating the CRP does not apply when t is less than k; therefore, the corresponding value is empty. When three or more shares are involved in recovering the secret image, we can reveal partial secret information about it. This result just meets the threshold requirement. Three different thresholds were achieved in the experiment. Therefore, (k, n) thresholds can be achieved.

C. COMPARISON WITH RELATED SCHEMES

In this section, we compare our scheme to other schemes and related analyses. Figure 6 shows Chao's (2, 3)-threshold scheme. The weights of the shares are also $W = [0.2, 0.3, 0.5]$. Figure 6a is a binary secret image of size 512*512. Figure 6$b - d$ are shares. Figure 6$e - g$ are the recovered images reconstructed by stacking two shares. Figure 6h is the recovered image reconstructed by stacking all the shares. The indexes of the shares involved are subscripted to the names.

In Figure 6 and Figure 5, the same threshold and weights are used. In Figure 6, the secret image is a binary image, and the recovered image is lossy. In contrast, in Figure 5 for our scheme, the secret image is a grayscale image, and grayscale images are more widely used in natural pictures than binary images. When all the shares are involved in the recovery phase, the image is recovered losslessly. These two features are advantages of our scheme. The average light transmission of the shares in Figure 6 are the same, but ours is different. When the shares are in the hands of different participants, they do not know the other's share; therefore, this has little effect in practical applications.

Table 4 provides detailed comparisons of the characteristics of other schemes and our SS scheme. The images used in the schemes from Hou *et al.*, Yang *et al.* and Chao *et al.* are binary images, and the encryption and decryption methods are from VSS. However, the images used in the scheme of Yan *et al.* and our scheme are grayscale images, and the corresponding encryption and decryption methods are based on the CRT. When the secret image is shared, a codebook is needed in the schemes of Hou *et al.* and Yang *et al.* Weight generation and VSS based on RG operations are added in the scheme of Chao *et al.* The modulus operation is essential in the scheme of Yan *et al.* Our scheme also requires weight generation and the modulus operation. The shares have equal average light transmission in the schemes of Yang *et al.*, Chao *et al.* and Yan *et al.*, but the average light transmission of the shares in the other schemes varies. The shares generated in the schemes of Hou *et al.*, Yang *et al.*, and Chao *et al.* and in our scheme have priority weights. In contrast, the shares in the scheme of Yan *et al.* do not possess priority weights. The threshold in the schemes of Hou *et al.* and Yang *et al.* is $(2, n)$. We, Chao *et al.* and Yan *et al.* implement (k, n)-threshold schemes. When all the shares are involved in restoration, we and Yan *et al.* can achieve lossless restoration, but the other schemes cannot.

VI. CONCLUSION

In this paper, we propose a (k, n)-threshold scheme. This scheme divides a grayscale image into n shares with different weights. When k or more shares are involved in the restoration, the secret is revealed. As the number and weights of the shares increase, the correct recovery probability (CRP) of the recovered secret images increases. When all the shares are involved, the reconstructed secret image is lossless. Effectiveness analyses and comparisons with other schemes are performed. As the experimental results demonstrate, the (k, n) threshold can be implemented, shares can have different weights and lossless restoration can be achieved. However, the average light transmission is different, which needs to be improved in future work.

ACKNOWLEDGMENT

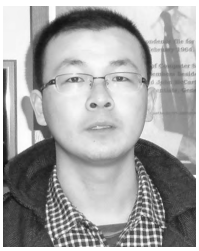
The authors are thankful to the reviewers for their comments and suggestions to improve the quality of the manuscript.

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 Nat. Comput. Conf.*, vol. 48, 1979, pp. 313–317.
[3] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.
[4] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science). Perugia, Italy: Springer, May 1995, pp. 1–12.
[5] 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.
[6] 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.
[7] M. Mignotte, "How to share a secret," in *Proc. EUROCRYPT*, 1982, vol. 149, no. 4, pp. 371–375.
[8] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 208–210, Mar. 1983.
[9] 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.
[10] 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.
[11] 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 *Proc. Int. Conf. Cloud Comput. Secur.*, 2017, pp. 433–440.
[12] J. Chen, K. Liu, X. Yan, L. Liu, X. Zhou, and L. Tan, "Chinese remainder theorem-based secret image sharing with small-sized shadow images," *Symmetry*, vol. 10, no. 8, pp. 340–345, 2018.
[13] X. Yan, Y. Lu, and L. Liu, "General meaningful shadow construction in secret image sharing," *IEEE Access*, vol. 6, pp. 45246–45255, 2018.
[14] 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.
[15] S. Iftene and I. C. Boureanu, "Weighted threshold secret sharing based on the Chinese remainder theorem," *Sci. Ann. Cuza Univ.*, vol. 15, pp. 161–172, Jan. 2005.
[16] A. Beimel, T. Tassa, and E. Weinreb, "Characterizing ideal weighted threshold secret sharing," *SIAM J. Discrete Math.*, vol. 22, no. 1, pp. 360–397, 2005.
[17] A. Beimel and E. Weinreb, "Monotone circuits for monotone weighted threshold functions," *Inf. Process. Lett.*, vol. 97, no. 1, pp. 12–18, 2006.
[18] P. Morillo, C. Padró, G. Sáez, and J. L. Villar, "Weighted threshold secret sharing schemes," *Inf. Process. Lett.*, vol. 70, no. 5, pp. 211–216, 1999.
[19] Y.-C. Hou, Z.-Y. Quan, and C.-F. Tsai, "A privilege-based visual secret sharing model," *J. Vis. Commun. Image Represent.*, vol. 33, pp. 358–367, Nov. 2015.
[20] C.-N. Yang, J.-K. Liao, and D.-S. Wang, "New privilege-based visual cryptography with arbitrary privilege levels," *J. Vis. Commun. Image Represent.*, vol. 42, pp. 121–131, Jan. 2017.
[21] H.-C. Chao and T.-Y. Fan, "Priority visual secret sharing of random grids for threshold access structures," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11867–11882, 2017.
[22] L. Liu, Y. Lu, X. Yan, and H. Wang, "Greyscale-images-oriented progressive secret sharing based on the linear congruence equation," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 20569–20596, 2017.

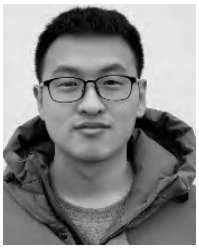
LONGDAN TAN was born in China, in 1987. She received the B.Sc. degree (Hons.) in computer application, in China, in 2008, and the M.Sc. degree in information security from the Hefei Electronic Engineering Institute, in 2011. She is currently pursuing the Ph.D. degree with the National University of Defense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

YULIANG LU was born in China, in 1964. He received the B.Sc. degree (Hons.) in computer application, in China, in 1985, and the M.Sc. degree in computer application from Southeast University, in 1988. 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 and calculate science, in China, in 2006, the M.Sc. degree in computational mathematics, in 2008, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, in 2015. 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, in China, in 2012, and the M.Sc. degree in information security from the National University of Defense Technology, Hefei, China, in 2015, where he is currently pursuing the Ph.D. degree. His research interests include cryptography, multimedia security, and biometrics.



LONGLONG LI was born in China, in 1995. He received the B.Sc. degree in automation from the University of Science and Technology of China, in 2017. He is currently pursuing the master's degree with the National University of Defense Technology, Hefei, China. His research interest includes multimedia security.