This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

# Reversible Image Secret Sharing

Xuehu Yan, Yuliang Lu, Lintao Liu
National University of Defense Technology
Hefei 230037, China
Email: publictiger@126.com

Xianhua Song
Harbin University of Science and Technology
Harbin 150080, China

***Abstract*—In reversible image secret sharing (RISS), the cover image can be recovered to some degree, and a share can be comprehensible rather than noise-like. Reversible cover images play an important role in law enforcement and medical diagnosis. The comprehensible share can not only reduce the suspicion of attackers but also improve the management efficiency of shares. In this paper, we first provide a formal definition of RISS. Then, we propose an RISS algorithm for a $(k, n)$-threshold based on the principle of the Chinese remainder theorem-based ISS (CRTISS). In the proposed RISS, the secret image is losslessly decoded by a modular operation, and the original cover image is recovered by a binarization operation, both of which are just simple operations. Theoretical analyses and experiments are provided to validate the proposed definition and algorithm.**

***Index Terms*—image secret sharing, extended image secret sharing, Chinese remainder theorem, comprehensible share, reversible image secret sharing.**

## I. Introduction

Image secret sharing (ISS) divides a secret image into multiple shares, also known as shadows or shadow images, which are then sent to participants. $(k, n)$-threshold ISS has a loss-tolerant property, i.e., the dealer can reconstruct the secret with at most $n-k$ shares lost. Hence, ISS is applied to several applications, such as key management [1], digital watermarking [2], [3], identity authentication [4], [5], blockchain [6], access control [7], password transmission [8] and distributive storage for the cloud [9]–[11]. A digital image is a specific form of data, where each grayscale (binary) pixel is represented by 8 bits (1 bit); hence, ISS easily generates shares for secret sharing. The principles of conventional ISS technologies basically include visual secret sharing (VSS) [12], [13], also known as visual cryptographic scheme (VCS), the use of polynomials [14] and the Chinese remainder theorem (CRT) [15], [16].

In the $(k, n)$-threshold VCS [17], [18], the $n$ shares are first printed onto transparent films and then sent to $n$ participants. In VCS, the secret is reconstructed from $k$ or more shares by stacking them and observing them using only the naked human eye without any cryptographic devices. If an attacker collects fewer than $k$ shares, she cannot reconstruct the secret even with high computational power. However, the traditional VCS schemes have limitations of poor image quality, basic matrix design and pixel expansion, which have been further discussed and considered in follow-up studies [19]–[22].

To reconstruct a high-quality secret image, Shamir [14] introduced the first $(k, n)$-threshold polynomial-based secret sharing approach using a random $(k-1)$-degree polynomial to generate $n$ shares, which were then sent to $n$ participants. When $k$ or more shares are collected, the secret can be reconstructed according to Lagrange interpolation. Following Shamir's work, some studies [23]–[25] put forward several improved ISS schemes based on polynomials to obtain better properties. Polynomial-based ISS is advantageous because the reconstructed secret has both high quality and no pixel expansion. Unfortunately, ISS presents the drawback that either the recovered secret image is slightly distorted or that the recovery involves a high calculation of $O(k \log^2 k)$ (when there is no distortion [15]).

Since the modular approach requires only $O(k)$ operations [15] to reconstruct each secret pixel, Chinese remainder theorem-based ISS (CRTISS) achieves a lower calculation level and no distortion, which has been discussed in several other studies [26]–[31]. Chang *et al.* [31] proposed multi-image threshold ISS based on CRT and a polynomial. Their method may increase the computational complexity due to modular and Lagrange interpolation operations. Recently, Yan *et al.* [16] introduced $(k, n)$ threshold CRTISS with lossless recovery, in which the explicit parameters were given according to the image characteristics.

However, in the above traditional ISS schemes, either the cover images cannot be reconstructed or the shares are noise-like. Such limitations make these schemes inapplicable to some situations.

On the one hand, due to legal considerations or the required high-precision nature, reversible cover images play an important role in law enforcement, medical diagnosis, experimental investigations into high-energy particle physics and remote sensing [32], [33], where a reversible (distortion-free or invertible) cover image in ISS means that the share can be reversed back to the original cover image to some degree after the secret image is decoded. More scenarios presenting need for reversible cover images are further discussed as follows.

1) Reversible cover images are useful for integrity authentication and media annotation. If we select a watermark image as the secret image and the cover images are artworks, we can utilize the watermark image to authenticate the artworks and to losslessly recover the artworks (cover images) because the details of the artworks are significant.
2) With the reversible cover image, both the secret image and cover images can be restored, which is useful

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

for storage conversion and allows the cover images to function as erasable storage disks.

3) Losslessly reconstructing the cover image is important to share searching with image recognition since a searching method, such as a hash function, is generally sensitive to cover image content including even a slight distortion.
4) The reversible cover image will result in great convenience when the user may not be satisfied with the processed result in image processing. Taking image inpainting as an example, an object is first cropped out from the original cover image, and then the remaining area is inpainted to make it visually plausible. To make the operations reversible, we just need to reversibly encode the cropped object into the inpainted cover images to obtain the reversible cover image.

In addition, binary images are widely used in several applications, such as newspapers, captchas, passwords and program flowcharts. Thus, lossless reconstruction of binary cover images is also meaningful.

On the other hand, a noise-like share may raise the suspicion of attackers and reduce the management efficiency of shares. In contrast, a comprehensible share can not only reduce the suspicion of attackers but also improve the management efficiency of shares. More importantly, ISS with a comprehensible share can be applied to encrypted domain searching with image recognition, which is important in cloud computing and distributed storage. A comprehensible share is useful for homomorphic computing and searching for each secret image. In addition, a comprehensible share allows the user to search within the encrypted domain without uploading, downloading and decryption processing.

Reversible image secret sharing (RISS) can be applied to the above scenarios and exhibits features such as capability for some degree of recoverability of the cover image and a comprehensive rather than noise-like share. RISS links two or more images such that the cover image can be recovered to some degree after the secret image has been decoded, thus providing an additional method to address two or more images.

Chang *et al.* [34] presented ISS combining steganography and authentication based on CRT and a polynomial. In their scheme, the polynomial is used first to generate shares, and CRT is used to obtain authentication bits. Then, the shares and authentication bits are embedded into the cover images using steganography to output stego images. Thus, the scheme results in high visual quality of the stego images and a participant authentication ability. However, it has high computational complexity and pixel expansion and cannot losslessly recover the cover image.

Lin and Chan [35] in 2010 introduced a polynomial-based RISS scheme with high visual quality of shares and the recovered secret image following previous work [36]. Their method represents the secret image pixel values in the $GF(P)$ finite field and embeds them into the first $(k-1)$-th coefficients of the constructed polynomial, in which their optical parameter is $P = 7$. The remainder of the cover image pixel values modulo 7 is embedded into the $k$-th coefficient of the polynomial. The shared values are added to the cover image pixel values minus the remainder to output $n$ shares. Thus, the cover image pixel value is changed to within 7 to achieve high visual quality of the shares, as well as a reversible share. However, when $P = 7$, first, their method includes large pixel expansion when $k$ is small, or less pixel expansion for the $(k, n)$ threshold with a larger $k$ value. Second, overflow may occur, and both the secret image pixel and the cover image pixel are lossy when the cover image pixel value is larger than 252. Third, their input cover images are the same, which may decrease the share management efficiency. Finally, slight information leakage may occur when continuous cover image pixel values are processed [37].

Ulutas *et al.* [38] provided an RISS approach for a grayscale level or dithered cover image based on the exploiting modification direction method. Their method transforms the secret image pixel values to base 17 and embeds them into the first $(k-2)$-th coefficients of the constructed polynomial. The last two coefficients of the polynomial are used to process the cover image pixels in base 9. Thus, high visual quality of the shares as well as a reversible share are achieved. However, their method is only applicable for $(k, n)$ thresholds with $k$ equal to or greater than 3, with pixel expansion occurring with respect to the secret image. Second, their input cover image is also the same single image. Finally, slight information leakage may occur when continuous cover image pixel values are processed [37].

In a word, traditional RISS approaches have the following limitations.

1) They are not applicable for a general $(k, n)$-threshold with any $n \geq k \geq 2$.
2) They input the same cover image, resulting in shares with similar content, which will decrease the share management efficiency.
3) Their shares have high pixel expansion, which will increase the necessary storage.
4) The original cover images and the secret image may not be losslessly reconstructed.
5) The cover recovery method requires more computation.

The motivations of this paper are to address the above issues and to propose one RISS approach with the above comprehensive features.

In this paper, we first provide a formal definition of RISS. In the definition, the conditions of RISS are presented, and the quality evaluation metrics of the recovered secret image and the reversed cover image are discussed. Then, we propose one RISS algorithm for a general $(k, n)$-threshold based on the principle of CRT and random elements in CRTISS. $n$ different binary cover images are input in our method to output $n$ different grayscale shares. The cover images' pixels are fused in the process of encoding the secret image pixel based on CRT. In the recovery phase, the secret image is losslessly decoded by a modular operation, and the original cover image is losslessly recovered by only a binarization operation, both of which are simple operations. Theoretical analyses and experiments are provided to validate the proposed definition and algorithm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

The arrangement of the following sections is as follows. Section II introduces CRT. In Section III, we discuss the introduced RISS definition and our established RISS algorithm in detail. Section IV presents the security analysis and performance proof of our algorithm. Section V discusses the experimental results and comparisons, and Section VI presents the conclusion.

## II. Preliminaries

In this section, we illustrate CRT for our work.

A set of linear congruence equations can be solved by CRT.

When a set of integers $m_i (i = 1, 2, \cdots, k)$ is chosen to satisfy $\gcd(m_i, m_j) = 1, i \neq j$, we have a unique solution $y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod{M}$, $y \in [0, M-1]$ to Eq. (1).

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

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

*Proof:*

Since $\gcd(m_i, m_j) = 1, i \neq j$, $\gcd(m_i, M_i) = 1$, and we have $M_i^{-1}$ subject to $M_i M_i^{-1} \equiv 1 \pmod{m_i}$.

Considering $a_1 M_1 M_1^{-1}$, we have

$$a_i M_i M_i^{-1} \equiv a_i \pmod{m_i} \tag{2}$$

$$a_i M_i M_i^{-1} \equiv a_i \pmod{m_j}, i \neq j \tag{3}$$

From Eqs. (2) and (3), $y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod{M}$, $y \in [0, M-1]$) subject to Eq. (1).

Hence, on the one hand, $y$ is one solution to Eq. (1).

On the other hand, if $y_1$ and $y_2$ are solutions to Eq. (1), we have $y_1 - y_2 \equiv 0 \pmod{m_i}$. Since $\gcd(m_i, m_j) = 1, i \neq j$, $M$ is exactly divided by $y_1 - y_2$. In addition, $y$ is one solution to Eq. (1); therefore, the set of solutions to Eq. (1) is $\{zM + y \,|\, z \in \mathbf{Z}\}$.

Thus, there is a unique solution $y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod{M}$, $y \in [0, M-1]$) to Eq. (1).

■

## III. Introduction of the RISS Definition and Algorithm

### A. RISS Definition

**Definition 1 (Reversible image secret sharing):** When $n$ cover images with a size of $W_C \times H_C$, represented by $C_1, C_2, \cdots C_n$, are input, ISS generates a secret image, denoted by $S$, with a size of $W_S \times H_S$ into $n$ shares, which in turn are denoted by $SC_1, SC_2, \cdots SC_n$, with a size of $W_{SC} \times H_{SC}$. We say that the ISS is an RISS for the $(k, n)$-threshold subject to the following:

- **security condition.** The secret image cannot be reconstructed with fewer than $k$ shares.
- **secret recovery condition**. The secret image can be reconstructed with $k$ or more shares.
- **comprehensible condition.** $SC_i$ is similar to $C_i$ for $i = 1, 2, \cdots n$.
- **reversible condition**. $C_i'$ is similar to $C_i$ for $i = 1, 2, \cdots n$.

where

- $C_i'$ denotes the $i$-th recovered cover image from one or more shares for $i = 1, 2, \cdots n$.
- the similarity between the original image and the recovered image, i.e., image quality, can be evaluated by traditional metrics, such as the signal-to-noise ratio (*PSNR*) given in Eq. (5), weighted PSNR (WPSNR) [39], and contrast for VCS.
- the embedding capacity, denoted by $EC$, can be used to evaluate the average embedding bit rate per share bit, as shown in Eq. (4).

$$EC = \frac{w_S \times (L_S \times W_S \times H_S) + w_c \times (n_C \times L_C \times W_C \times H_C)}{n \times L_{SC} \times W_{SC} \times H_{SC}} \tag{4}$$

where $w_x, n_x, L_x, W_x$, and $H_x$ denote the weight factor, number, grayscale level, image weight, and image height of $x$, respectively. For a binary image, $L_x = 1$, whereas $L_x = 8$ for a grayscale image. If a unique cover image is input, $n_C = 1$, and hence, $EC$ is decreased. $w_x$ is used to balance the weight between the secret image and cover image according to the application scenario.

If $C_i' = C_i$ for $i = 1, 2, \cdots n$, we say that the RISS is fully RISS; otherwise, we say that the RISS is partially RISS.

The *PSNR* given in Eq. (5) between the primary image $I$ and $I'$ is used to evaluate the image similarity, where the *MSE* given in Eq. (6) indicates the mean square error.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB} \tag{5}$$

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left[I'(i,j) - I(i,j)\right]^2 \tag{6}$$

The *WPSNR* given in Eq. (7) is used to evaluate the contrast sensitivity function (CSF) to weight the spatial frequency of the error image [39].

$$WPSNR = 10\log_{10} \frac{1}{\sqrt{\sum_{i=1}^{W} \sum_{j=1}^{H} F^2(i,j) \Big/ WH}} \tag{7}$$

where $F$ denotes the filtered result of the error image $E = I' - I$ with coefficients $FC$, and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

$$FC(\omega,\theta) = \mathrm{A}(\omega)\,\mathrm{B}(\omega,\theta),$$
$$\mathrm{A}(\omega) = 1.5e^{\frac{-a^2\omega^2}{2}} - e^{-2a^2\omega^2}, a = 2, \omega = \frac{2\pi f}{60},$$
$$f = \sqrt{u^2+v^2}, u = v = -20:20,$$
$$\mathrm{B}(\omega,\theta) = \frac{1+e^{b(\omega-\omega_0)}\cos^4 2\theta}{1+e^{b(\omega-\omega_0)}}, b = 8, \omega_0 = 1.166, \theta = \tan^{-1}\frac{v}{u}.$$

We further explain and analyze Definition 1 as follows.

- The **security condition** and **secret recovery condition** are derived from ISS for the $(k,n)$-threshold.
- $C_i$, for $i = 1, 2, \cdots n$, can be a natural image or an image generated by a secure technique.
- In information hiding (IH), on the one hand, the stego image is naturally comprehensible (meaningful) so that reversible IH (RIH) does not need the **comprehensible condition**. However, ISS may generate a noise-like share. Thus, the **comprehensible condition** is considered in RISS; otherwise, the ISS belongs to multiple secret sharing. On the other hand, the stego image has high quality in IH so that RIH generally is fully RIH. However, ISS may output a comprehensible share with low quality; thus, partially RISS is considered in addition to fully RISS. In addition, we can better achieve RISS by means of ISS rather than IH.
- To compute the image quality, some images are scaled to a proper size when the pixel expansion coefficient is not 1, and the binary image is converted to a grayscale image.
- Traditional extended VCS, $a.k.a.$ VCS with a comprehensible share [18], [40], belongs to partially RISS and has a low image quality according to Definition 1.
- In Eq. (4), the numerator includes the total bits embedded in the output shares; the denominator indicates the total bits in all shares.
- If larger pixel expansion occurs in some ISS, its $EC$ is lower based on Eq. (4) due to the larger $W_{SC} \times H_{SC}$.
- $w_S = 1$ and $w_C = 1$ in this paper.

### B. Our RISS Algorithm

The design idea of the proposed RISS algorithm is presented in Fig. 1. The detailed steps are presented in Algorithm 1, which takes an original secret image and $n$ binary cover images, with a size of $W \times H$, to output $n$ shares $SC_1, SC_2, \cdots SC_n$, also with a size of $W \times H$. The recovery steps are presented in Algorithm 2.

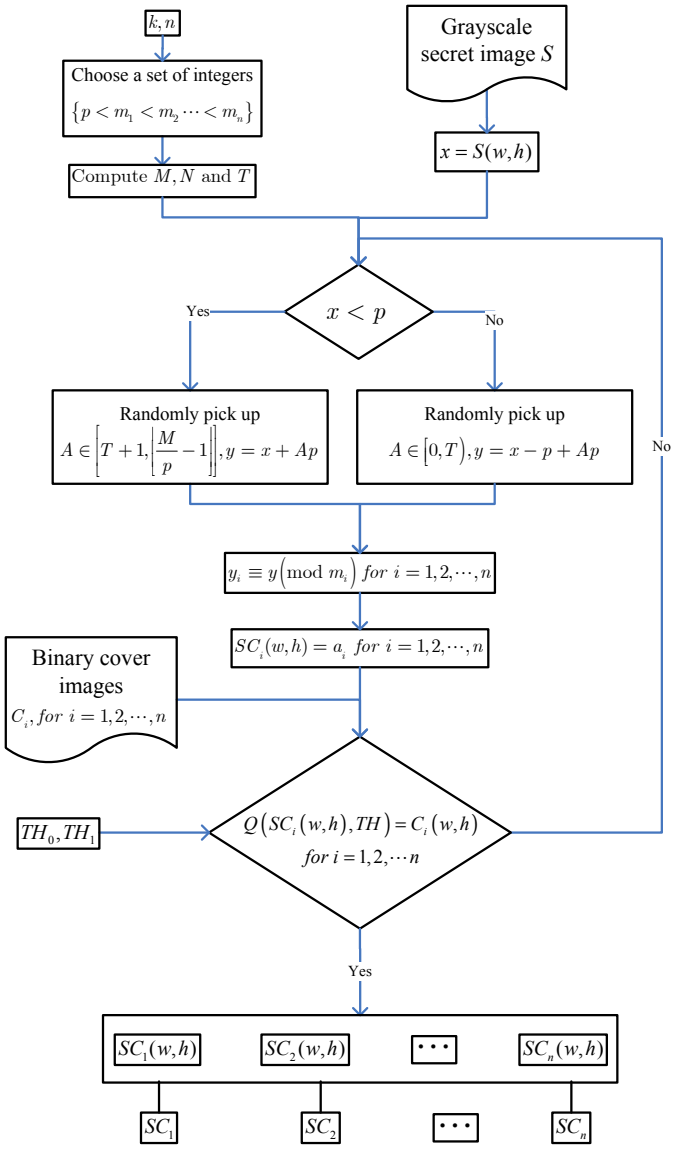



Figure 1. Design idea of the proposed reversible image secret sharing algorithm

Regarding Algorithm 1, we make the following comments.

1) The binarization processing threshold values $TH_{i0}$ and $TH_{i1}$ are input by the dealer, $i = 1, 2, \cdots n$, subject to $N_A \geq 8$, where $N_A$ denotes the number of available values of $A$ satisfying $Q(SC_i(w,h), TH_{i0}, TH_{i1}) = C_i(w,h)$ for $i = 1, 2, \cdots n$ in Step 5 of Algorithm 1 and $N_A = T \times \prod_{i=1}^{n}\left(\frac{1}{2} \times \frac{TH_{i0}}{m_i} + \frac{1}{2} \times \frac{m_i - TH_{i1}}{m_i}\right)$, which will be further analyzed in Section IV and Section V-B.
2) Compared with fixed thresholds, $TH_{i0}$ and $TH_{i1}$ can introduce dynamics into Algorithm 1 and thus improve the feasibility and security of Algorithm 1.
3) The binarization processing threshold values $TH_{i0}$ and $TH_{i1}$ play important roles in the similarity between $SC_i$ and $C_i$ under the secure condition for $i = 1, 2, \cdots n$, where $TH_{i0} \leq (m_i/2)$, and $TH_{i1} \geq (m_i/2)$. In general, larger $TH_{i1}$ and smaller $TH_{i0}$ result in better image quality for $SC_i$ as well as a smaller range of $A$ values, which will be further analyzed in Section V-B.
4) Step 1 intends to choose a set of integers to satisfy the CRT conditions. In general, $p$ is as small as possible, in consideration of security, while $m_i$ is as large as possible to achieve a large range for the distribution of the pixel values in shares.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

**Algorithm 1**. The proposed $(k,n)$ threshold reversible image secret sharing

**Input**: A secret image $S$ with a size of $W\times H$; threshold parameters $(k,n)$, where $2 \le k \le n$; $n$ binary cover images $C_1, C_2, \cdots C_n$, with a size of $W \times H$; binarization processing threshold values $TH_{i0}$ and $TH_{i1}$, corresponding to 0 and 1, respectively, for the $i$-th cover image, $i = 1, 2, \cdots n$.
**Output**: Shadow image $SC_i$, which looks similar to $C_i$, and its corresponding private integer $m_i$, $i = 1, 2, \cdots n$.

**Step 1:** Select a set of integers $\{128 \le p < m_1 < m_2 \cdots < m_n \le 256\}$ that satisfy

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 among all the participants.

**Step 2:** Calculate $T = \left\lfloor \frac{\lfloor \frac{M}{p} - 1 \rfloor}{2} \right\rfloor$, which is public.

**Step 3:** For each secret pixel position $(w,h) \in \{(w,h) | 1 \le w \le W, 1 \le h \le H\}$, repeat Steps 4-5.
**Step 4:** Let $x = S(w,h)$.

If $0 \le x < p$, select a random integer $A$ from $\left[T+1, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$, and compute $y = x + Ap$; otherwise, select a random integer $A$ from $[0, T)$and compute $y = x - p + Ap$.
Calculate $a_i \equiv y \pmod{m_i}$, and set $SC_i(w,h) = a_i$ for $i = 1, 2, \cdots, n$.
**Step 5:** If $Q(SC_i(w,h), TH_{i0}, TH_{i1}) = C_i(w,h)$, $i = 1, 2, \cdots n$, go to the next secret pixel position; otherwise, go to Step 4.
where

$$Q(SC_i(w,h), TH_{i0}, TH_{i1}) = \begin{cases} 1 \text{ if } SC_i(w,h) \ge TH_{i1} \ when \ C_i(w,h) = 1 \\ 0 \text{ if } SC_i(w,h) < TH_{i0} \ when \ C_i(w,h) = 0 \end{cases}$$

**Step 6:** Output $n$ grayscale shares $SC_1, SC_2, \cdots SC_n$.

**Algorithm 2**. The recovery in the proposed reversible image secret sharing for the $(k,n)$-threshold.

**Input**: Any $t$ grayscale shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}$ $(t \ge k)$, their private modular integers $m_{i_1}, m_{i_2}, \cdots m_{i_t}$, $p$ and T.
**Output**: Reconstructed grayscale secret image $S'$ and recovered binary cover image $C'_{i_j}$ for $j = 1, 2, \cdots, t$, with a size of $W\times H$.

**Step 1:** Compute $C'_{i_j}$ from $SC'_{i_j}$ by the binarization processing operation with threshold $(m_{i_j}/2)$ for $j = 1, 2, \cdots, t$.
**Step 2:** For each secret pixel position $(w,h) \in \{(w,h) | 1 \le w \le W, 1 \le h \le H\}$, repeat Steps 3-4.
**Step 3:** Set $a_{i_j} = SC_{i_j}(w,h)$ for $j = 1, 2, \cdots, k$. Solve Eq. (8) to obtain $y$ by CRT.

$$\begin{aligned} y &\equiv a_{i_1} \pmod{m_{i_1}} \\ y &\equiv a_{i_2} \pmod{m_{i_2}} \\ &\cdots \\ y &\equiv a_{i_{k-1}} \left(\bmod m_{i_{k-1}}\right) \\ y &\equiv a_{i_k} \left(\bmod m_{i_k}\right) \end{aligned} \tag{8}$$

**Step 4:** Calculate $T^* = \left\lfloor \frac{y}{p} \right\rfloor$.
If $T^* \ge T$, set $x \equiv y \pmod{p}$; otherwise, let $x = y \pmod{p} + p$.
Compute $S'(w,h) = x$.
**Step 5:** Output reconstructed grayscale secret image $S'$ and recovered binary cover image $C'_{i_j}$ for $j = 1, 2, \cdots, t$, with a size of $W\times H$

5) Step 4 aims to achieve the features of the $(k,n)$ threshold and lossless recovery, which will be further analyzed in Section IV.
6) Since $A$ is randomly selected in Step 4, when $N_A \ge 8$, we can search $A$ to satisfy $Q(SC_i(w,h), TH_{i0}, TH_{i1}) = C_i(w,h)$ for $i = 1, 2, \cdots n$ in Step 5. In this manner, $C_i$ can be losslessly recovered by binarization processing.

Regarding Algorithm 2, we note the following.

1) To recover cover image $C_{i_j}$ for $j = 1, 2, \cdots, t$, we can directly perform binarization on share $SC_{i_j}$ with threshold $(m_{i_j}/2)$ due to Step 5 in Algorithm 1.
2) Steps 3-4 can losslessly reconstruct $S(w,h) = x$ by collecting any $k$ or more shared pixels. Because $T$ divides the interval $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ into two parts corresponding to $0 \le x < p$ or $p \le x \le 255$ in Step 4 of Algorithm 1, $x$ is losslessly reconstructed for arbitrary $x \in [0, 255]$.

## IV. Security Analysis and Performance Proof

Here, we present the security analysis and performance proof of the designed RISS by theoretically analyzing the security and other conditions in Definition 1.

In the following analyses, we consider that both the secret image and cover images are natural images and that they all are independent of each other; i.e., there is no correlation among them.

Without loss of generality, in the recovery phase, the collected $t$ grayscale pixels are denoted by $sc_{i_1}, sc_{i_2}, \cdots sc_{i_t}$, corresponding to $SC_{i_1}(w,h), SC_{i_2}(w,h), \cdots SC_{i_t}(w,h)$.

*Lemma 1:* The secret image $S$ cannot be reconstructed with $k-1$ or fewer shares.

*Proof:* We assume that $y$ is generated in Step 4 of Algorithm 1, where $y \in [N, M-1]$. When $k-1$ share pixels $a_{i_1} = sc_{i_1}, a_{i_2} = sc_{i_2}, \cdots a_{i_{k-1}} = sc_{i_{k-1}}$ are collected, according to CRT we can only obtain the solution $y_0$ modulo $N_2 = \prod_{j=1}^{k-1} m_{i_j}$, where $y_0 \in [0, N_2 - 1]$. The true $y$ value range is different from the above $y_0$. In addition, $N \ge N_2$, $N \le y < M$ and $\gcd(N_2, p) = 1$; hence, in $[N_2, M-1]$, $y_0 + b\prod_{j=1}^{k-1} m_{i_j}$ are also solutions to the collected $k-1$ equations in Eq. (8) for $b = 1, 2, \cdots, m_{i_k} - 1$. Therefore, we have $m_{i_k}$ solutions in $[0, M-1]$ rather than only one. ■

*Lemma 2:* The secret image $S$ can be losslessly reconstructed with $k$ or more shares.

*Proof:* Since $x = S(w,h)$ in Step 4 of Algorithm 1, we will prove that any $k$ or more share pixels enable the lossless reconstruction of $x$. To reconstruct $x$, we have to obtain $y$, since $x \equiv y \pmod{p}$ or $x \equiv y \pmod{p} + p$. When we collect $a_{i_1}, a_{i_2}, \cdots a_{i_k}$, based on CRT, we have a unique solution $y$ modulo $N_1 = \prod_{j=1}^{k} m_{i_j}$ due to $N_1 \ge M$. Finally, we have a unique $y$ and hence $x$ in Step 4 of Algorithm 2. ■

*Lemma 3:* $SC_i$ looks similar to $C_i$ for $i = 1, 2, \cdots n$.

*Proof:* The white (black) pixel of $C_i$ corresponds to the grayscale value 255 (0) of $C_i$ for $i = 1, 2, \cdots n$. According to Step 4 of Algorithm 1, we know $255 - SC_i(w,h) \le TH_{i1}$ when $C_i(w,h)$ is white; $SC_i(w,h) - 0 < TH_{i0}$ when $C_i(w,h)$ is black. Therefore, $SC_i$ looks similar to $C_i$ for $i = 1, 2, \cdots n$. ■

*Lemma 4:* $C'_i = C_i$ for $i = 1, 2, \cdots n$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

*Proof:* In Step 1 of Algorithm 2, the binarization threshold $m_i/2$ for $i = 1, 2, \cdots, n$ is known. Since $TH_{i0} \leq (m_i/2)$ and $TH_{i1} \geq (m_i/2)$, based on Step 5 of Algorithm 1, we know that $C_i' = C_i$ for $i = 1, 2, \cdots n$, where $C_i'$ is obtained from $SC_i'$ by the binarization processing operation with threshold $m_i/2$. ■

**Theorem 1:** The proposed scheme is a valid fully RISS approach.

*Proof:* Based on the above Lemmas 1-4, according to Definition 1, the mentioned conditions are satisfied. ■

**Proposition 1** In the proposed Algorithm 1, $N_A = T \times \prod_{i=1}^{n} \left( \frac{1}{2} \times \frac{TH_{i0}}{m_i} + \frac{1}{2} \times \frac{m_i - TH_{i1}}{m_i} \right)$, and $N_A \geq 8$ for better performance.

*Proof:* In general, $A$ has $T$ possible values in Step 4 of Algorithm 1. To satisfy $Q\left(SC_i\left(w,h\right), TH_{i0}, TH_{i1}\right) = C_i\left(w,h\right)$ for $i = 1, 2, \cdots n$, $N_A$ will decrease to $T \times \prod_{i=1}^{n} \left( \frac{1}{2} \times \frac{TH_{i0}}{m_i} + \frac{1}{2} \times \frac{m_i - TH_{i1}}{m_i} \right)$.

A larger $N_A$ leads to enhanced security because the number of brute-force attacks is $T^{N_A}$. We require $N_A \geq 2$ for the lowest security since if $N_A = 1$, we have only one integer $A$ repeatedly used in Step 4 of Algorithm 1, which is not secure. $N_A \geq 8$ is suggested to achieve an acceptable time for searching available values of $A$ in fully RISS, which is given in the experiments and further analyzed in section V-B. ■

**Proposition 2** The embedding capacity of the proposed Algorithm 1 is $\frac{8+n}{8n}$.

*Proof:* Since in this paper, $w_S = 1$, $w_C = 1$, $n_C = n, L_S = 8, L_C = 1$, and we have no pixel expansion, the result is obtained. ■

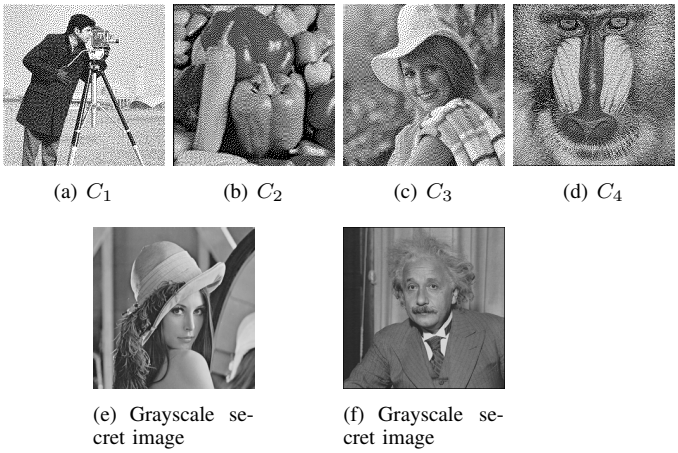
## V. Experimental results and discussions

In this section, experiments are presented to prove the effectiveness of our RISS. Then, some discussions regarding our parameters are given. Finally, comparisons with related methods will be demonstrated in terms of illustrations and features to indicate the advantages of our scheme.

### A. Image illustration

In the following experiments, we set $TH_{i0} = (m_i/2 - TH)$ and $TH_{i1} = (m_i/2 + TH)$ for the $i$-th cover image, $i = 1, 2, \cdots n$. The experimental binary cover images and grayscale secret images with a size of $256 \times 256$ used in this paper are illustrated in Fig. 2, which are scaled to the proper size in some experiments.

Fig. 3 shows the results of the proposed $(k, n)$ threshold RISS, where $k = 3, n = 4, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, p = 131, TH = 64$ and the input grayscale secret image is presented in Fig. 3 (a). Figs. 3 (b-e) illustrate the output of 4 comprehensible shares $SC_1, SC_2, SC_3$ and $SC_4$, which appear similar to the cover images, as well as their PSNRs. Figs. 3 (f-p) show the secret images reconstructed with any 2 or more shares based on CRT, where $S'_{i_1 i_2 \cdots i_t}$ denotes the secret image $S'$ reconstructed from $SC_{i_1}, SC_{i_2}, \cdots, SC_{i_t}$. From Figs. 3 (f-p), the secret image reconstructed with any 3 or more shares is recognized, while nothing of the secret image reconstructed with 2 or fewer shares is recognized. The secret image is losslessly reconstructed with any 3 or more shares, i.e., Fig. 3 (l) is the same as the original secret image in Fig. 3 (a) as $PSNR = +\infty$. The recovered binary cover images are demonstrated in Figs. 3 (q-t), which are all lossless and have the same size as the secret image.



(a) $C_1$ (b) $C_2$ (c) $C_3$ (d) $C_4$

(e) Grayscale secret image (f) Grayscale secret image

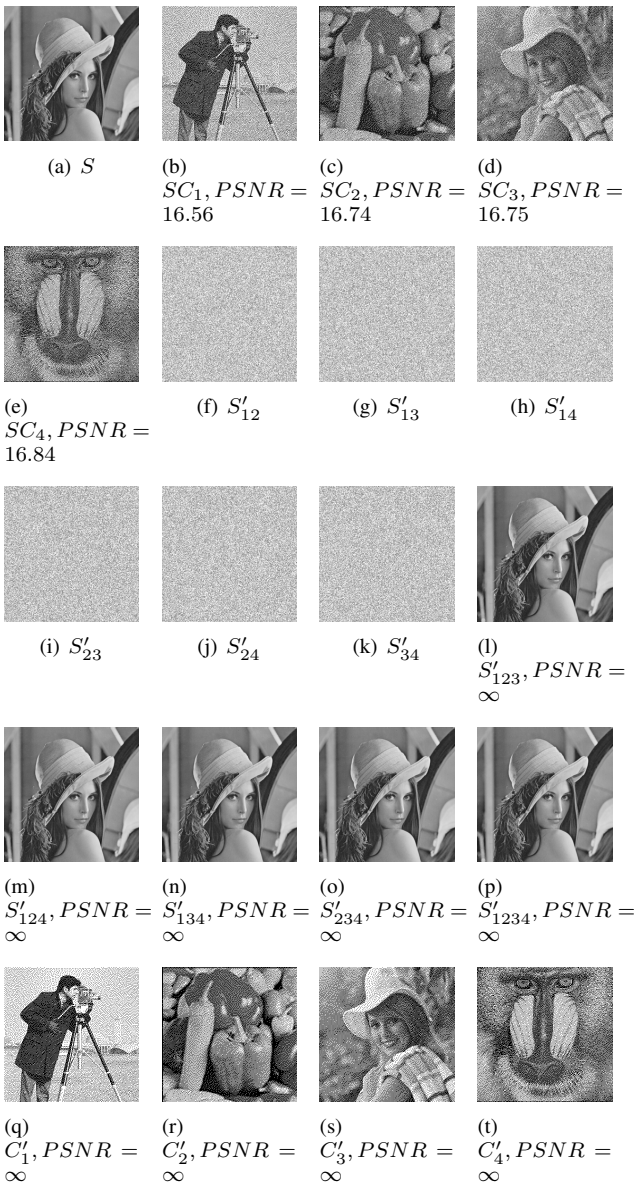
Figure 2. Experimental images. (a) − (d) four input binary cover images $C_1, C_2, C_3$ and $C_4$. (e) − (f) different input grayscale secret images.

Fig. 4 shows the results of the proposed $(k, n)$ threshold RISS, where $k = 2, n = 3, m_1 = 251, m_2 = 253, m_3 = 255, p = 128, TH = 24$ and the input grayscale secret image is presented in Fig. 4 (a). Figs. 4 (b-d) illustrate the output of 3 comprehensible shares $SC_1, SC_2$ and $SC_3$, which look similar to the cover images, as well as their PSNRs. Fig. 4 (e) shows the secret image reconstructed with the first 2 shares based on CRT, where only the first $t-th$ shadows are utilized to save pages. From Fig. 4 (e), the secret image reconstructed with any 2 or more shares is recognized, while nothing of the secret image reconstructed with any one share is recognized. The secret image is losslessly reconstructed with any 2 or more shares, i.e., Fig. 4 (e) is the same as the original secret image in Fig. 4 (a) as $PSNR = +\infty$. The recovered binary cover images are demonstrated in Figs. 4 (f-h), which are all lossless and have the same size as the secret image.

According to the above illustrations, we can conclude the following:

1) The shares with no pixel expansion are comprehensible and have no cross-interference for the natural secret image.
2) With fewer than $k$ shares, no secret information is leaked, which indicates the security of our RISS.
3) With any $k$ or more shares, the secret image is losslessly reconstructed.
4) The original $n$ different cover images are losslessly recovered by only the binarization processing operation.
5) An RISS algorithm for a general $(k, n)$-threshold is achieved, where $n \geq k \geq 2$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security



(a) $S$ (b) $SC_1, PSNR = 16.56$ (c) $SC_2, PSNR = 16.74$ (d) $SC_3, PSNR = 16.75$

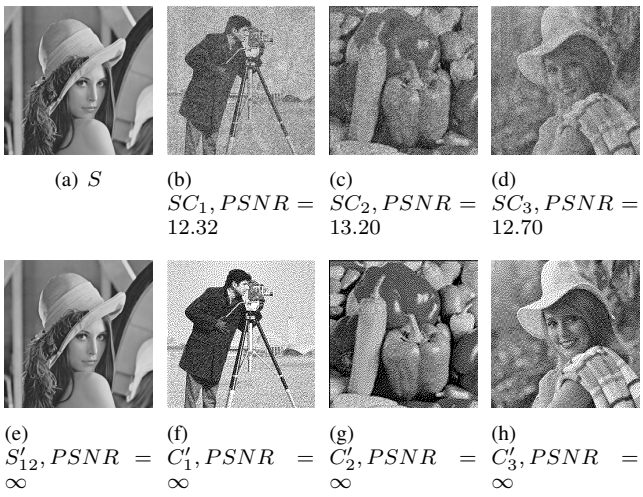
(e) $SC_4, PSNR = 16.84$ (f) $S'_{12}$ (g) $S'_{13}$ (h) $S'_{14}$

(i) $S'_{23}$ (j) $S'_{24}$ (k) $S'_{34}$ (l) $S'_{123}, PSNR = \infty$

(m) $S'_{124}, PSNR = \infty$ (n) $S'_{134}, PSNR = \infty$ (o) $S'_{234}, PSNR = \infty$ (p) $S'_{1234}, PSNR = \infty$

(q) $C'_1, PSNR = \infty$ (r) $C'_2, PSNR = \infty$ (s) $C'_3, PSNR = \infty$ (t) $C'_4, PSNR = \infty$

Figure 3. Experimental results of the introduced $(k, n)$ threshold RISS, where $k = 3, n = 4, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, p = 131$ and $TH = 64$. (a) The grayscale secret image; (b) $-$ (e) four grayscale comprehensible shares $SC_1, SC_2, SC_3$ and $SC_4$; (f) $-$ (p) reconstructed grayscale secret images; (q) $-$ (t) recovered binary cover images.



(a) $S$ (b) $SC_1, PSNR = 12.32$ (c) $SC_2, PSNR = 13.20$ (d) $SC_3, PSNR = 12.70$

(e) $S'_{12}, PSNR = \infty$ (f) $C'_1, PSNR = \infty$ (g) $C'_2, PSNR = \infty$ (h) $C'_3, PSNR = \infty$

Figure 4. Experimental results of the introduced $(k, n)$ threshold RISS, where $k = 2, n = 3, m_1 = 251, m_2 = 253, m_3 = 255, p = 128$ and $TH = 24$. (a) The grayscale secret image; (b) $-$ (d) three grayscale comprehensible shares $SC_1, SC_2$ and $SC_3$; (e) grayscale secret image reconstructed with the first two shares; (f) $-$ (h) recovered binary cover images.

### *B. Available parameters and quality analyses*

*1) Available parameters:* In step 1 of Algorithm 1, a set of integers $\{128 \leq p < m_1 < m_2 \cdots < m_n \leq 256\}$ is selected to satisfy some conditions, where the conditions intend to achieve the $(k, n)$-threshold CRT-based ISS. $\{128 \leq p < m_1 < m_2 \cdots < m_n \leq 256\}$ is required due to the image pixel value range and $pN < M$.

We suggest that $m_i$ should be as large as possible to ensure that the pixel values of shares can randomly lie within a large range to improve the security and that $p$ should be as small as possible for security reasons, under the condition that $p$ can divide the secret pixel values into two intervals to losslessly recover the secret. When the image pixel value range is $[0, 255]$, we can set $p = 128$. In addition, a prime generally has significance in cryptography; thus, we can set $p = 131$, the smallest prime greater than 128.

Ultimately, we provide some available values of parameters $p, m_1, m_2 \cdots, m_n$ for different values of $n$ in Table I, some of which are used in our experiments. The user can search for other suitable parameters according to the specific applications in addition to the above available parameters.

Table I
AVAILABLE PARAMETERS FOR $p, m_1, m_2 \cdots, m_n$

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

*2) Image quality analyses:* In our experiments, we set $TH_{i0} = (m_i/2 - TH)$ and $TH_{i1} = (m_i/2 + TH)$ for the $i$-th cover image for $i = 1, 2, \cdots n$. Thus, $TH$ plays an important role in the quality of both the secret image and the share. Herein, we intend to study the quality and some other curves as $TH$ changes. The binary cover images and grayscale secret image with a size of $128 \times 128$ in Fig. 2 and Fig. 3 (a) are employed in our experiments, where $k = 3, n = 3, m_1 = 251, m_2 = 253, m_3 = 255, p = 128$, $TH \in [8, 120]$, and $PSNR/WPSNR = 100$ indicates lossless recovery for better figure presentation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

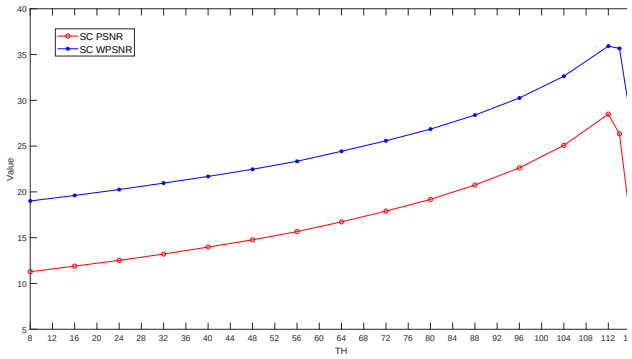



Figure 5. PSNR and WPSNR curves of shadow images

Fig. 5 shows the average of the shares' quality evaluation metric curves for $TH$, from which we can deduce the following:

1) When $0 \leq TH \leq 112$, the PSNR and WPSNR are both monotonically increasing functions of $TH$.
2) When $TH \geq 112$, the PSNR and WPSNR are both monotonically dramatically decreasing functions of $TH$.
3) $TH = 112$ is an extreme point for the share quality.

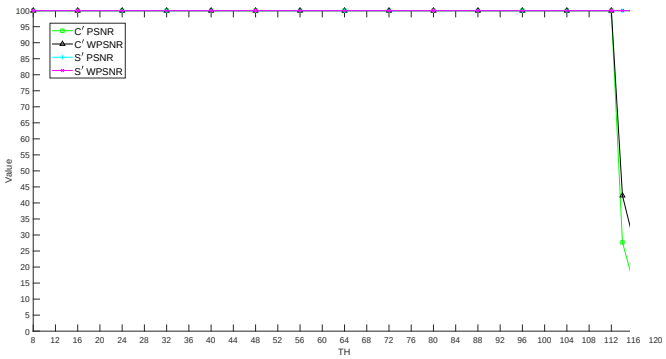



Figure 6. PSNR and WPSNR curves of recovered cover images and the reconstructed secret image

Fig. 6 depicts the mean of the quality evaluation metric curves of the recovered cover images and reconstructed secret image for $TH$, from which we can deduce the following:

1) When $0 \leq TH \leq 112$, the PSNR and WPSNR are both 100, i.e., both the recovered cover images and reconstructed secret image are lossless.
2) When $TH \geq 112$, the PSNR and WPSNR are both monotonically dramatically decreasing functions of $TH$.
3) $TH = 112$ is an extreme point for the quality of the recovered cover images and the reconstructed secret image.

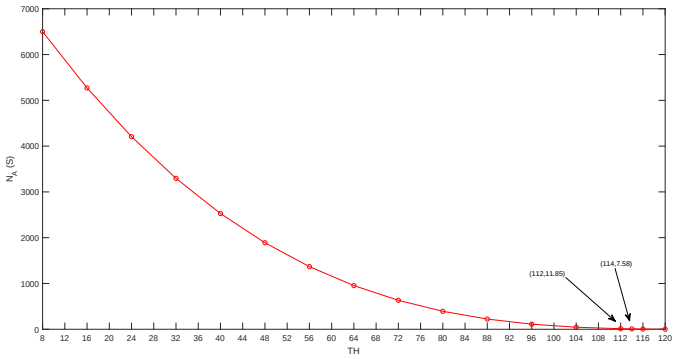



Figure 7. $N_A$ curve

Fig. 7 shows the number of available values of $A$ satisfying $Q\left(SC_i\left(w,h\right),TH_{i0},TH_{i1}\right) = C_i\left(w,h\right)$ for $i = 1,2,\cdots n$ in Step 5 of Algorithm 1, i.e., the $N_A$–$TH$ curve, from which we can deduce the following:

1) $N_A$ is a monotonically decreasing function of $TH$.
2) When $TH = 112$, $N_A = 11.85 \geq 8$; when $TH = 114$, $N_A = 7.58 < 8$.

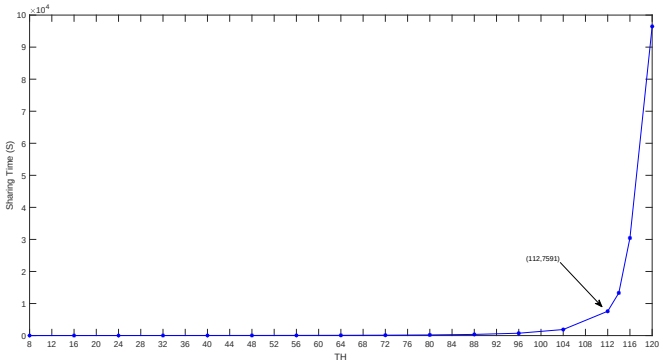



Figure 8. Sharing time curve

Fig. 8 shows the sharing time–$TH$ curve, from which we can deduce the following:

1) When $0 \leq TH \leq 112$, the sharing time is a monotonically increasing function of $TH$.
2) When $TH \geq 112$, the sharing time is a monotonically dramatically increasing function of $TH$.
3) When $TH = 112$, the sharing time is 7591 (s), which is an acceptable time for sharing.

We further analyze the above curves as follows.

1) $TH = 112$ ($N_A = 8$) is the extreme point. When $TH \geq 112$ ($N_A < 8$), we cannot find $A$ subject to $Q\left(SC_i\left(w,h\right),TH_{i0},TH_{i1}\right) = C_i\left(w,h\right)$ for $i = 1,2,\cdots n$, which leads to lossy recovered cover images

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

and a lossy reconstructed secret image. When $TH \geq 112$ ($N_A < 8$), the sharing time dramatically increases, which leads to a low sharing efficiency.

2) Hence, in our algorithm, $N_A \geq 8$ is suggested to result in an acceptable time for searching available values of $A$ in fully RISS. $N_A$ may be slightly different in some other environments.

### C. Comparisons with relative schemes

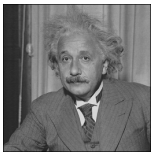
We will compare our RISS with the method of Ulutas *et al*. [38] by means of illustrations and features, in which the same secret image as in Fig. 9 (a) and a $(3, 3)$ threshold are used. The method of Ulutas *et al*. [38] is selected for comparison because their ISS method is reversible for a binary cover image.

*1) Illustration comparison:* Ulutas *et al.* [38] proposed an RISS approach for a dithered binary cover image based on the exploiting modification direction method, which transforms the secret image pixel values to base 17 and embeds them into the first $(k-2)$-th coefficients of the constructed polynomial. We use the same parameters as those of Ulutas *et al*. to realize their results, as shown in Fig. 9, where $k = 3, n = 3$ and the grayscale secret image of size $256 \times 256$ is shown in Fig. 9 (a). Figs. 9 (c-e) are the 3 output shares of size $512 \times 512$, which are comprehensible and have the same content. Fig. 9 (b) displays the grayscale secret image of size $256 \times 256$ reconstructed with all three shares using Lagrange interpolation. The recovered binary cover image is demonstrated in Fig. 9 (f), which is a lossless image of size $512 \times 512$.

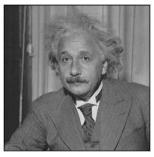
Fig. 10 shows the comparison example of our $(k, n)$ threshold RISS, where $k = 3, n = 3, m_1 = 253, m_2 = 254, m_3 = 255, p = 131, TH = 114$ and the input grayscale secret image is presented in Fig. 10 (a). Figs. 10 (b-d) illustrate the output of 3 comprehensible shares $SC_1, SC_2$ and $SC_3$ of size $256 \times 256$, which are similar to different cover images, as well as their PSNRs. Fig. 10 (e) shows the secret image of size $256 \times 256$ losslessly reconstructed with all 3 shares based on CRT. The three recovered binary cover images of size $256 \times 256$ are depicted in Figs. 10 (f-h), which are all lossless.

According to Figs. 9 and 10, comparisons between our method and that of Ulutas *et al*. [38] reveal the following.

1) Both methods can losslessly reconstruct the secret image with any $k$ or more shares. Our method is suitable for $k \geq 2$, while the method of Ulutas *et al*. [38] is only suitable for $k \geq 3$. More importantly, our method needs only $O(k)$ operations [15] to recover each secret pixel due to the modularity of CRT, while the method of Ulutas *et al*. [38] requires Lagrange interpolation. Thus, our method is more general, with a lower computational complexity for secret images.
2) The shares of both methods are comprehensible. Our method includes no pixel expansion, while that of Ulutas *et al*. [38] includes pixel expansion. More importantly, our method outputs $n$ different shares, while that of Ulutas *et al*. [38] outputs only the same single share. Thus, our method has higher share management efficiency.



(a) Grayscale secret image of size $256 \times 256$



(b) $S'_{123}$, reconstructed grayscale secret image of size $256 \times 256$, $PSNR = \infty$

(c) $SC_1$, grayscale share of size $512 \times 512$, $PSNR = 41.38$

(d) $SC_2$, grayscale share of size $512 \times 512$, $PSNR = 41.43$

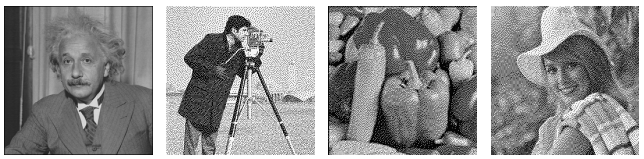
(e) $SC_3$, grayscale share of size $512 \times 512$, $PSNR = 41.39$

(f) $C'$, recovered binary cover image of size $512 \times 512$, $PSNR = \infty$

Figure 9. Experimental example by using the method of Ulutas *et al*. [38], where $k = 3, n = 3$. (a) The grayscale secret image; (b) grayscale secret image reconstructed with all three shares; (c) $-$ (e) three grayscale comprehensible shares $SC_1, SC_2$ and $SC_3$; (f) the same recovered binary cover image.

3) The original cover image is losslessly recovered in both methods. Our method losslessly recovers $n$ different cover images, while that of Ulutas *et al*. [38] recovers only one cover image. More importantly, our method needs only the binarization processing operation to recover the cover image, while Lagrange interpolation is needed in the method of Ulutas *et al*. [38]. Thus, our method has lower computational complexity when recovering the cover image.
4) The $EC$ of our method is $\frac{8+3}{8\times3} = 0.46$, while that of Ulutas *et al*. [38] is $\frac{8+4}{8\times3\times4} = 0.125$. Thus, our method has a higher embedding capacity.
5) Our method is only suitable for binary cover images, while the method of Ulutas *et al*. [38] is suitable for both grayscale and binary cover images. In addition, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security



(a) Grayscale secret image of size $256 \times 256$



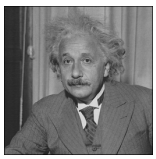
(b) $SC_1$, grayscale share of size $256 \times 256$, $PSNR = 29.46$



(c) $SC_2$, grayscale share of size $256 \times 256$, $PSNR = 30.14$



(d) $SC_3$, grayscale share of size $256 \times 256$, $PSNR = 30.31$



(e) $S'_{123}$, reconstructed grayscale secret image of size $256 \times 256$, $PSNR = \infty$

(f) $C'_1$, recovered binary cover image of size $256 \times 256$, $PSNR = \infty$

(g) $C'_2$, recovered binary cover image of size $256 \times 256$, $PSNR = \infty$

(h) $C'_3$, recovered binary cover image of size $256 \times 256$, $PSNR = \infty$

Figure 10. Experimental comparison example of our $(k, n)$ threshold RISS, where $k = 3, n = 3, m_1 = 253, m_2 = 254, m_3 = 255, p = 131$ and $TH = 114$. (a) The grayscale secret image; (b) − (d) three grayscale comprehensible shares $SC_1, SC_2$ and $SC_3$; (e) grayscale secret image reconstructed with the first two shares; (f) − (h) recovered binary cover images.

method of Ulutas *et al*. [38] has a higher share PSNR than our method. Our method only outputs an acceptable share quality.

*2) Feature comparison:* Our RISS is applicable for a general $(k, n)$ threshold with $n$ different input cover images, while conventional RISS schemes are applicable to a specific $(k, n)$ threshold with the same single input cover image; thus, we further compare our method with related schemes according to features rather than statistics.

Feature comparisons between our RISS and related methods are shown in Table II, from which our method is shown to have more features as follows.

1) Our method is applicable for a $(k, n)$-threshold with any $n \geq k \geq 2$ due to the use of $(k, n)$-threshold CRT-based ISS.
2) We input $n$ different cover images, resulting in $n$ different shares, which improves the share management efficiency.
3) Our shares have no pixel expansion, which can save storage space.
4) Both the original cover images and the secret image are losslessly reconstructed in our method.
5) Our secret recovery method includes modular arithmetic ($O(k)$ operations [15]), as implemented with CRT, and the cover recovery method only includes binarization, achieving a lower operation time than that with Lagrange interpolation.

In particular, compared with traditional methods, the proposed RISS for the $(k, n)$-threshold exhibits the features of $n$ cover images, no pixel expansion, low recovery operation and lossless recovery for both the secret image and cover image, with an acceptable share quality that outperforms conventional schemes.

### D. Discussion

Both polynomial-based ISS and CRT-based ISS are studied. They are compared as follows.

1) The reconstruction operation is Lagrange interpolation ($O(k \log^2 k)$) in polynomial-based ISS, while that in CRT-based ISS is modular operation ($O(k)$); thus, CRT-based ISS has a lower computational cost than that of polynomial-based ISS to reconstruct the secret image.
2) CRT-based ISS can achieve lossless reconstruction, while most polynomial-based ISS schemes are lossy.
3) The shadow size of polynomial-based ISS is easily reduced.
4) The principle of CRT-based ISS is complex and hard to be understood.
5) The number of owners is not limited in polynomial-based ISS, while that in CRT-based ISS is generally small, such as $n \leq 6$, since the available value of $m_i$ decreases as $n$ increases, which will affect the distribution of shadow pixel values and thus further lead to security issues. However, $n \leq 6$ is applicable in most situations.

We choose CRT in our scheme due to the advantages of lower computation cost and lossless reconstruction, where lower computation cost is significant in mobile applications and lossless reconstruction is important to image details.

Actually, Shamir's polynomial-based ISS schemes are widely studied, and they can be applied to our scheme as well. When applying Shamir's polynomial-based ISS to our scheme, Steps 1 and 2 can be removed; in Step 4, we can construct a $k-1$ degree polynomial as Eq.(9), with the constant coefficient equal to the secret pixel grayscale value and the other coefficients chosen randomly; Step 5 can be preserved. In such a way, we could use polynomial-based ISS.

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P \qquad (9)$$

where $a_0 = S(w, h)$ and $a_i$ is random, for $i = 1, 2, \cdots k-1$.

## VI. Conclusion

In this paper, we have introduced a formal definition of reversible image secret sharing (RISS). Based on this definition, our proposed RISS algorithm for a $(k, n)$-threshold implements the principle of Chinese remainder theorem-based ISS (CRTISS), exhibiting the features of $n$ cover images, no pixel expansion, low recovery operation, lossless recovery and share comprehensibility. The experiments have proven the effectiveness of the algorithm. Available parameters and quality analyses have been provided as well. We have performed experiments and feature comparisons with related schemes to indicate the advantages of our approach. We will focus on

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2020.3001735, IEEE Transactions on Information Forensics and Security

Table II
FEATURE COMPARISON WITH RELATED SCHEMES

| Scheme | $(k, n)$-threshold | Number of cover images | No pixel expansion | Lossless recovery of secret image | Lossless recovery of cover image | Secret image recovery method | Cover image recovery method |
|---|---|---|---|---|---|---|---|
| Lin *et al*. [36] | Yes | 1 | No | High quality | High quality | Interpolation | Interpolation |
| Lin and Chan [35] | Yes | 1 | No | High quality | High quality | Interpolation | Interpolation |
| Ulutas *et al*. [38] | $k \geq 3$ | 1 | No | Yes | Yes | Interpolation | Interpolation |
| Ours | Yes | $n$ | Yes | Yes | Yes | Modular | Binarization |

the following aspects in future work. First, we will test and theoretically analyze the optical image quality factors $TH_{i0}$, $TH_{i1}$ and $N_A$ to balance the sharing time, image quality and security. Second, we will extend the cover pattern to grayscale and color patterns. Third, we will apply other ISS mechanisms to our scheme, such as polynomial-based ISS. Fourth, we will apply other authentication techniques to our scheme to achieve participant authentication, such as the hash function.

## VII. ACKNOWLEDGMENTS

The authors would like to thank the associate editor and the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491), the Key Program of the National University of Defense Technology (Grant Number: ZK-17-02-07) and the Natural Science Foundation of Heilongjiang Province (Grant Number: QC2017075).

## REFERENCES

[1] Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for qr code applications," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2393–2403, 2018.

[2] H. Luo, Z. M. Lu, and J. S. Pan, "Multiple watermarking in visual cryptography," in *International Workshop on Digital Watermarking*, 2007, pp. 60–70.

[3] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, 2018.

[4] Y. Li and L. Guo, "Robust image fingerprinting via distortion-resistant sparse coding," *IEEE Signal Processing Letters*, vol. 25, no. 1, pp. 140–144, Jan 2018.

[5] P. V. Chavan, M. Atique, and L. Malik, "Signature based authentication using contrast enhanced hierarchical visual cryptography," in *Electrical, Electronics and Computer Science*, 2014, pp. 1–5.

[6] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and D. Takahashi, "A proposal of a secure p2p-type storage scheme by using the secret sharing and the blockchain," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, March 2017, pp. 803–810.

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

[8] W. Wang, F. Liu, T. Guo, and Y. Ren, "Temporal integration based visual cryptography scheme and its application," in *Digital Forensics and Watermarking: 16th International Workshop , IWDW 2017, Magdeburg, Germany, August 23-25*, 2017, pp. 406–419.

[9] S. Zou, Y. Liang, L. Lai, and S. Shamai, "An Information Theoretic Approach to Secret Sharing," *Arxiv preprint*, 2014. [Online]. Available: http://arxiv.org/abs/1404.6474

[10] I. Komargodski, M. Naor, and E. Yogev, "Secret-Sharing for NP," *Journal of Cryptology*, vol. 30, no. 2, pp. 444–469, 2017.

[11] D. R. Stinson, "An explication of secret sharing schemes," *Designs Codes & Cryptography*, vol. 2, no. 4, pp. 357–390, 1992.

[12] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology-EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques, May 9-12*, Springer. Perugia, Italy: Springer, 1995, pp. 1–12.

[13] G. Wang, F. Liu, and W. Q. Yan, "Basic visual cryptography using braille," *International Journal of Digital Crime & Forensics*, vol. 8, no. 3, pp. 85–93, 2016.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[16] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Chinese remainder theorem-based secret image sharing for (k, n) threshold," *Cloud Computing and Security: Third International Conference, ICCCS 2017, Nanjing, China, June 16-18, 2017, Revised Selected Papers, Part II*, pp. 433–440, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-68542-7_36

[17] J. Weir and W. Yan, "A comprehensive study of visual cryptography," in *In: Transactions on DHMS V, LNCS 6010, Springer-Verlag*. Berlin, Heidelberg: Springer, 2010, pp. 70–105.

[18] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security.*, vol. 4, no. 3, pp. 383–396, 2009.

[19] 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.

[20] T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids with improved contrast," *Journal of Systems and Software*, vol. 86, no. 8, pp. 2094–2109, 2013.

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

[22] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2653–2672, Jan 2018.

[23] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

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

[25] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences*, vol. 453, pp. 21 – 29, 2018.

[26] W. Yan, W. Ding, and Q. Dongxu, "Image sharing based on chinese remainder theorem," *J. NORTH CHINA UNIV. OF TECH*, vol. 12, no. 1, pp. 6–9, 2000.

[27] S. J. Shyu and Y. R. Chen, "Threshold secret image sharing by chinese remainder theorem," in *IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1332–1337.

[28] M. Ulutas, V. V. Nabiyev, and G. Ulutas, "A new secret image sharing technique based on asmuth bloom's scheme," in *Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on*, 2009, pp. 1–5.

[29] H. Chunqiang, L. Xiaofeng, and X. Di, "Secret image sharing based on chaotic map and chinese remainder theorem," *International Journal of Wavelets Multiresolution & Information Processing*, vol. 10, no. 3, p. 1250023 (2012) [18 pages], 2012.

[30] T. W. Chuang, C. C. Chen, and B. Chien, "Image sharing and recovering based on chinese remainder theorem," in *International Symposium on Computer, Consumer and Control*, 2016, pp. 817–820.

[31] C.-C. Chang, N.-T. Huynh, and H.-D. Le, "Lossless and unlimited multi-image sharing based on chinese remainder theorem and lagrange interpolation," *Signal Processing*, vol. 99, pp. 159 – 170, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0165168413005112

[32] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, March 2006.

[33] D. Hou, W. Zhang, J. Liu, S. Zhou, D. Chen, and N. Yu, "Emerging applications of reversible data hiding," in *International Conference on Image and Graphics Processing (ICIGP) 2019 ACM, February 2325, 2019, Singapore*, Feb 2019, pp. 105–109.

[34] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.

[35] P.-Y. Lin and C.-S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.

[36] P.-Y. Lin, J.-S. Lee, and C.-C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886 – 895, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320308004056

[37] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Security analysis of secret image sharing," *Data Science: Third International Conference of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2017, Changsha, China, September 22–24, 2017, Proceedings, Part I*, pp. 305–316, 2017. [Online]. Available: https://doi.org/10.1007/978-981-10-6385-5_26

[38] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Invertible secret image sharing for gray level and dithered cover images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 485 – 500, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121212002701

[39] M. Miyahara, K. Kotani, and V. R. Algazi, "Objective picture quality scale (pqs) for image coding," *IEEE Transactions on Communications*, vol. 46, no. 9, pp. 1215–1226, Sep. 1998.

[40] X. Yan, S. Wang, X. Niu, and C.-N. Yang, "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," *Digital Signal Processing*, vol. 38, no. 0, pp. 53 – 65, 2015.