Mathematical Biosciences and Engineering

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

MBE, 16(5): 4433–4455.
DOI: 10.3934/mbe.2019221
Received: 09 January 2019
Accepted: 25 April 2019
Published: 20 May 2019

Research article

Ramp secret image sharing

Xuehu Yan[1,*], Longlong Li[1], Lintao Liu[1], Yuliang Lu[1] and Xianhua Song[2]

[1] National University of Defense Technology, Hefei 230037, China
[2] Harbin University of Science and Technology, Harbin 150080, China

* **Correspondence:** Email: publictiger@126.com; Tel: 86-551-88602862; Fax: 86-551-88602862-881.

Abstract: Secret image sharing (SIS) belongs to but differs from secret sharing. In general, conventional (k, n) threshold SIS has the shortcoming of "all-or-nothing". In this article, first we introduce ramp SIS definition. Then we propose a (k_1, k_2, n) ramp SIS based on the Chinese remainder theorem (CRT). In the proposed scheme, on the one hand, when we collect any k_1 or more and less than k_2 shadows, the secret image will be disclosed in a progressive way. On the other hand, when we collect any k_2 or more shadows, the secret image will be disclosed losslessly. Furthermore, the disclosing method is only modular arithmetic, which can be used in some real-time applications. We give theoretical analyses and experiments to show the effectiveness of the proposed scheme.

Keywords: secret image sharing; ramp secret image sharing; Chinese remainder theorem; progressiveness; lossless recovery

1. Introduction

Secret image sharing (SIS) belongs to but differs from secret sharing, and image is widely used and covers many privacies [1, 2], thus, SIS should be specially studied and designed. In a (k, n) threshold SIS scheme, it aims at splitting a secret image into n shadows, i.e., shares or shadow images, which are then assigned to n participants. The secret can be disclosed by any k or more shadows while less than k shadows gain nothing of the secret. SIS can be applied to many scenarios, such as key management, access control, information hiding, authentication, watermarking, transmitting passwords, and distributed storage and computing in cloud computing [3–8]. In the field of SIS research, there are mainly Shamir's polynomial-based scheme [9] and visual secret sharing (VSS) [10] also called visual cryptography scheme (VCS) [11].

Shamir's original polynomial-based SIS [9, 12] for (k, n) threshold splits a secret image into the constant coefficient of a random $(k-1)$-degree polynomial to generate n shadows, which are then

assigned to n participants. The secret image can be disclosed with high-resolution by means of Lagrange interpolation with any k or more shadows. Inspired by Shamir's original scheme, some researchers [13–18] proposed more polynomial-based schemes to possess more features. Although polynomial-based SIS only needs k shadows for disclosing the distortion-less secret image, it has high computational complexity because of Lagrange interpolation and "all-or-nothing".

In (k, n) threshold VSS [19–24], the outputted n shadows are printed onto transparencies and then assigned to n participants. The beauty of VSS is that the secret image is disclosed by superposing any k or more shadows with human native eyes and no cryptographic computation. Collecting less than k shadows will in general give no clue about the secret image even a watchdog owns infinite computation power. Unfortunately, original VSS suffers from codebook design, pixel expansion problem, low contrast and "all-or-nothing", which are taken into account by the following works [23, 25–32]. Furthermore, most of the existing VSS schemes have limitations of lossy recovery and "all-or-nothing" [29, 33, 34].

In contrast to "all-or-nothing", progressive secret image sharing (PSIS) [33, 35–38] achieves the characteristic that the more shadows the better disclosed secret image quality. PSIS is useful in many multimedia applications, such as art work image vending, Pay-TV/Music, multi-level representation and degraded encryption, where we need to intentionally disclose the multimedia with a degraded but recognizable quality so as to protect the details in addition to multimedia content. Unfortunately, conventional PSIS may be lossy recovery. Progressiveness can be divided into global progressiveness and regional progressiveness. Global progressive PSIS mainly protects the detail of the secret image progressively, while regional progressive PSIS mainly protects the secret image region by region. Since the paper intends to protect the detail of the secret image, we focus on global progressiveness in this article. However, PSIS is mainly for (k, n) threshold, where lossless recovery is seldom achieved.

Based on above analyses, conventional SIS has the drawback of "all-or-nothing" and conventional PSIS has the limitation of lossy recovery. Thus, we intend to propose ramp SIS which achieves both progressive and lossless recovery by a unique disclosing method.

In this article, first we introduce ramp SIS definition according to image features and ramp secret sharing [39–41]. Then we propose (k_1, k_2, n) ramp SIS based on the Chinese remainder theorem (CRT) [42–44]. In the proposed ramp, i.e., (k_1, k_2, n) threshold, CRT-based SIS, when we collect any k_1 or more and less than k_2 shadows, the secret image will be disclosed in a progressive way [45]. On the other hand, when we collect any k_2 or more shadows, the secret image will be disclosed losslessly. Furthermore, the disclosing method is only modular arithmetic resulting in ability in real-time application. We give theoretical analyses and experiments to display the effectiveness of our method.

Our method allows the purchaser to review the secret with a degraded quality by collecting less shadows prior to buying them. Then the purchaser can obtain the lossless version by collecting more shadows after he decides to buy it. Image generally differs from data, thus the progressive feature with poor quality of image makes sense to some applicable scenarios. The progressive feature achieves that the quality of the image can be partially degraded. Such perceptibility makes it possible for the potential purchasers to view low-quality copies of the image prior to buying them.

A detailed scenario is given as follows. In the process of displaying and selling an art image, since the details are very important for the art image, details should be protected. After sharing the art image once, the owner can disclose and present different image qualities to different people on different

occasions, instead of sharing again. For example, in an exhibition, first the owner can demonstrate a low quality of the art image with any k_1 or more shadows to prove the copyright of the art, then after reaching a purchase agreement he shows the lossless quality with any k_2 or more shadows.

The detailed advantages and contributions of the proposed approach are as follows.

1. A formal definition of ramp SIS is first introduced.
2. (k_1, k_2, n) ramp SIS based on CRT is proposed. We use CRT due to the following advantages comparing to polynomial-based SIS. On one hand, CRT-based SIS can achieve lossless recovery, while most of the polynomial-based SIS schemes are in general lossy. On the other hand, the disclosed operation of polynomial-based SIS is Lagrange's interpolation ($O(k \log^2 k)$), while that of CRT-based SIS is only modular operation ($O(k)$) [44], therefore, CRT-based SIS has lower computational cost than polynomial-based SIS to disclose the secret image.
3. The secret image is decoded by only modular operation. When we collect any k_2 or more shadows, the secret image will be disclosed losslessly, which outperforms polynomial-based SIS due to lossy recovery for secret pixel value larger than 250 if 251 is selected as the prime value in polynomial-based SIS.

The rest of the paper is organized as follows. Section 2 introduces ramp SIS definition and some basic requirements for the proposed method. In section 3, the proposed method and its analyses are presented in detail. Section 4 is devoted to experimental results. Finally, section 5 concludes this paper.

2. Preliminaries

In this section, we will give some preliminaries. In conventional (k, n) threshold SIS, an original secret image S is encrypted into n shadows $SC_1, SC_2, \cdots SC_n$, and the decrypted secret image S' is disclosed from any t ($k \le t \le n, t \in \mathrm{Z}^+$) shadows.

2.1. Chinese remainder theorem (CRT)

CRT was first exploited in the Western han dynasty of China as well as formally introduced in the southern and northern dynasties. It intends to solve a set of linear congruence equations.

When we choose a set of integers $m_i (i = 1, 2, \cdots, k)$ satisfying $\gcd\left(m_i, m_j\right) = 1, i \neq j$, then there is a unique solution
$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) (\mathrm{mod}\ M)$, $y \in [0, M-1]$) to Eq. (2.1).

$$\begin{aligned} y &\equiv a_1 \,(\mathrm{mod}\ m_1) \\ y &\equiv a_2 \,(\mathrm{mod}\ m_2) \\ &\cdots \\ y &\equiv a_{k-1} \,(\mathrm{mod}\ m_{k-1}) \\ y &\equiv a_k \,(\mathrm{mod}\ m_k) \end{aligned} \tag{2.1}$$

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

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

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

$$a_i M_i M_i^{-1} \equiv a_i \left(\mathrm{mod}\ m_i\right), i \neq j \tag{2.2}$$

$$a_i M_i M_i^{-1} \equiv a_i \left(\mathrm{mod}\ m_j\right), \tag{2.3}$$

According to Eqs. (2.2) and (2.3),
$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \left(\mathrm{mod}\ M\right)$, $y \in [0, M-1]$ subject to Eq. (2.1).

Thus, on one hand, y is one solution to Eq. (2.1).

On the other hand, if both y_1 and y_2 are solutions to Eq. (2.1), we have $y_1 - y_2 \equiv 0 \left(\mathrm{mod}\ m_i\right)$. Since $\gcd\left(m_i, m_j\right) = 1, i \neq j$, M is exactly divided by $y_1 - y_2$. In addition, y is one solution to Eq. (2.1), thus, the set of solutions to Eq. (2.1) is $\{zM + y \,|z \in \mathbf{Z}\}$.

Therefore, there is a unique solution
$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \left(\mathrm{mod}\ M\right)$, $y \in [0, M-1]$) to Eq. (2.1).

□

CRT will be utilized in the proposed scheme to possess (k_x, n) threshold, where $2 \leq k_1 \leq k_x \leq k_2 \leq n$. Both Polynomial-based SIS and CRT-based SIS are well studied. We use CRT in our scheme due to the following advantages and differences.

- The shadow size of polynomial-based SIS is easier to be reduced.
- CRT-based SIS easily achieves lossless reconstruction, while most polynomial-based SIS schemes are not lossless.
- The disclosing operation is Lagranges interpolation ($O(klog^2k)$ in polynomial-based SIS, while that is modular operation ($O(k)$ [46]) in CRT-based SIS, thus CRT-based SIS has lower computational complexity than polynomial-based SIS to disclose the secret image.
- The principle of CRT-based SIS is complex and hard to be understood.
- The number of owners is in general not limited in polynomial-based SIS, while that in CRT-based SIS is small like n 6, because as n increases the available value of mi decreases, which will affect the distribution of the values of the shadow pixels and therefore further may lead to secure issue.

2.2. The characteristic analyses of image

Digital image differs from pure electronic data, where the differences mainly have:

- An image includes many pixels, which have correlations between adjacent ones, such as structure, texture, edge and other related information. The correlations are important to security and hence need to be considered in SIS algorithm design.Thus, SIS should encrypt not only the pixel values but also the correlations between adjacent pixels.
- There are lots of pixels in an image so that computational complexity of SIS should be considered.
- An image owns special file storage structure. Using grayscale image as an example, its pixel value is in the range of $[0, 255]$, which should be satisfied in SIS design, e.g., the output value, the input value, and other relative parameters, should lie in the range. For example, the secret pixel

value range and the shadow pixel value range should not exceed the range. In addition, we have $m_i \leq 256$ when applying to CRT.

- An image is a specific form of the data, where each grayscale (binary) pixel is represented as one byte (bit), so SIS is easily to be applied to secret sharing.
- In general, secret data is available only if it is losslessly recovered. Whereas, an image may be useful when recovered with some errors because of human eyes' low pass filter feature, thus, progressiveness makes sense to SIS.

The above differences lead to that in general traditional secret sharing cannot be directly applied to SIS. In particular, CRT-based ramp secret sharing cannot be directly applied to CRT-based ramp SIS.

2.3. Ramp SIS Definition

Definition 1. *A SIS splits a secret image, denoted as S, into n shadow images, denoted as $SC_1, SC_2, \cdots SC_n$. We say the SIS is a (k_1, k_2, n) ramp SIS subject to:*

- ***security condition.*** *The secret image cannot be reconstructed with any less than k_1 shares.*
- ***ramp recovery condition***. *The secret image will be reconstructed progressively with any k_1 or more and less than k_2 shares. The reconstructed image quality increases with the number of shares from k_1 to k_2.*
- ***decodable condition.*** *The secret image is decoded with any k_2 or more shares.*

If $k_1 = k_2 = k$, (k_1, k_2, n) ramp SIS will reduce to (k, n)-threshold SIS. The ramp SIS is called linear ramp SIS if the reconstructed image quality increases linearly with the number of shares from k_1 to k_2.

2.4. Quality evaluation metrics of the reconstructed secret image

In VSS, contrast is generally used, which is also adopted in this paper to evaluate the quality in VSS. In polynomial-based SIS, in general due to lossless recovery the metrics are seldom considered. In the research field of image processing, there are many metrics to evaluate image quality, where some typical metrics will be directly adopted in this paper.

The visual quality in VSS, which can decide how well human eyes can recognize the disclosed image, of the disclosed secret image S' corresponding to secret image S can be overall evaluated by contrast as follows [28].

Definition 2.

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S'[AS0] = 0) - P(S'[AS1] = 0)}{1 + P(S'[AS1] = 0)} \tag{2.4}$$

Where α is contrast, P_0 (resp., P_1) means the probability of white pixels in the disclosed image S' for the corresponding white (resp., black) area in secret image S, that is, P_0 denotes correctly decrypted probability corresponding to white area in secret image S, and P_1 denotes wrongly decrypted probability corresponding to black area in secret image S.

Since lossless disclose or nothing, i.e., "all-or-nothing", conventional SIS for grayscale image omits to discuss quality evaluation of disclosed secret image. Progressiveness differs from "all-or-nothing", therefore, we should discuss the quality evaluation of the disclosed gray secret image. The following typical objective metrics will be adopted to evaluate the image quality between S' and S.

1. Peak signal-to-noise-ratio (*PSNR*): *PSNR*, in Eq. (2.5), between the primary image I with size of $M \times N$ and modified image I' is adopted to measure the image similarity, where *MSE* as Eq. (2.6) denotes the mean square error.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB} \tag{2.5}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[I'(i,j) - I(i,j)]^2 \tag{2.6}$$

2. Structural similarity index measure (SSIM) [47] is to assess the visual impact of three characteristics in an image, i.e., luminance, contrast and structure, which gains a multiplicative combination of the above three terms, as Eq. (2.7). The value of SSIM is in -1 and 1. The larger SSIM results in higher image similarity.

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \tag{2.7}$$

where
$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}$
$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}$
$s(x,y) = \frac{2\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}$

$\mu_x, \mu_y, \sigma_x, \sigma_y, and\ \sigma_{xy}$ are the local means, standard deviations, and cross-covariance for images x, y. In this paper, we set $C_3 = \frac{C_2}{2}, \alpha = \beta = \gamma = 1$.

3. NC is to evaluate the quality between the original secret image and the disclosed secret image, as Eq. (2.8).

$$NC(I, I') = \frac{1}{\sum_{i=1}^{M}\sum_{j=1}^{N} I^2(i,j)}\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,j) \times I'(i,j) \tag{2.8}$$

4. The universal quality index (UQI) [48] can reflect the distortion of the disclosed secret image with its original secret image, whose value is between -1 and 1. The larger UQI means better quality. The block size of UQI is 8 in this paper. For details please refer to [48].

In addition, contrast can decide how well human eyes recognize the disclosed binary secret, so that it is expected to be as great as possible to obtain better visual quality. About how the contrast values map to the quality of the disclosed image, please refer to [49]. Herein, in order to show some intuitions about the expected performance, we have the followings.

1. When $\alpha \in$ [0,0.03], one cannot recognize the secret image.
2. When $\alpha \in$ (0.03,0.14], one can see a little information of the secret image.
3. When $\alpha \in$ (0.14,0.21], the secret image is recognized with acceptable quality.
4. When $\alpha \in$ (0.21,1], the secret image is fast recognized with good quality.

About how the PSNR values map to the image quality [50], we may refer to the followings.

1. When PSNR ∈ [28.5,+∞], the image quality is very good.
2. When PSNR ∈ [23.0,28.5), the image quality is good.
3. When PSNR ∈ [19.5,23.0), the image quality is medium.
4. When PSNR ∈ [17.0,19.5), the image quality is poor.
5. When PSNR ∈ [0,17.0), the image quality is bad.

3. The proposed (k_1, k_2, n) ramp SIS

3.1. Our method

Algorithm 1. The proposed (k_1, k_2, n) ramp SIS

Input: A secret image S with size of $H \times W$ and threshold parameters (k_1, k_2, n), where $2 \le k_1 \le k_2 \le n$.
Output: n shadows $SC_1, SC_2, \cdots SC_n$ and corresponding private integers $m_1, m_2, \cdots m_n$.

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

1. $\gcd\left(m_i, m_j\right) = 1, i \ne j$.
2. $\gcd(m_i, p) = 1$ for $i = 1, 2, \cdots, n$.
3. $M_{k_x} > pN_{k_x}$ for any $2 \le k_1 \le k_x \le k_2$.

where $M_{k_x} = \prod_{i=1}^{k_x} m_i$, $N_{k_x} = \prod_{i=1}^{k_x - 1} m_{n-i+1}$ and p is public.

Step 2: Calculate $T_{k_x} = \left\lfloor \frac{\left\lfloor \frac{M_{k_x}}{p} - 1 \right\rfloor - \left\lceil \frac{N_{k_x}}{p} \right\rceil}{2} + \left\lceil \frac{N_{k_x}}{p} \right\rceil \right\rfloor$ for $k_x = k_1, k_1 + 1, \cdots k_2$ and T_{k_x} is public as well among all the participants. For each coordinate $(h, w) \in \{(h, w) | 1 \le h \le H, 1 \le w \le W\}$, repeat Steps 3-5 .
Step 3: For now processing pixel value $s = S(h, w)$, we select randomly a threshold $k_x{}^*$ in $[k_1, k_2]$.
Step 4: If $0 \le x < p$, randomly pick up an integer A in $\left[T_{k_x{}^*} + 1, \left\lfloor \frac{M_{k_x{}^*}}{p} - 1 \right\rfloor\right]$ and compute $y = s + Ap$. Else randomly pick up an integer A in $\left[\left\lceil \frac{N_{k_x{}^*}}{p} \right\rceil, T_{k_x{}^*}\right)$ and $y = s - p + Ap$.
Step 5: Calculate $a_i \equiv y \pmod{m_i}$ and compute $SC_i(h, w) = a_i$ for $i = 1, 2, \cdots, n$.
Step 6: Output n shadows $SC_1, SC_2, \cdots SC_n$ and their private corresponding integers $m_1, m_2, \cdots m_n$.

We give the proposed (k_1, k_2, n) ramp SIS based on CRT in **Algorithm 1** with an original secret image S leading to n output shadows $SC_1, SC_2, \cdots SC_n$ and private corresponding integers $m_1, m_2, \cdots m_n$. The recovery Steps are described in Algorithm 2.

In Algorithm 1 and Algorithm 2, we find that.

1. In Step 1 of the proposed Algorithm 1, $\{128 \le p < m_1 < m_2 \cdots < m_n \le 256\}$ is given due to image pixel value range and $pN_{k_x} < M_{k_x}$. We suggest here that p is as small as possible for security and m_i is as large as possible, thus, the pixel values of shadow will be randomly distributed in large range.
2. $\gcd\left(m_i, m_j\right) = 1$ and $\gcd(m_i, p) = 1$ intend to satisfy CRT conditions, where m_i may be preserved as the private key for participant i or may be public. $\gcd(m_i, p) = 1$ is on account of not only applicable CRT but also containing all possible pixel values in range $[0, m_i)$ for shadow SC_i. We note that, our method can accommodate only a constant number of participants because in Step 1 of Algorithm 1 one has to choose $n + 1$ integers between 128 and 256, which must be pairwise relatively prime and whose available numbers are more than 23 but less than 128. However, these numbers can satisfy general applications.

Algorithm 2. Recovery for the proposed scheme.

Input: t shadows $SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}$, their corresponding private integers $m_{i_1}, m_{i_2}, \cdots m_{i_t}$, p and T_{k_x} for $k_x = k_1, k_1 + 1, \cdots k_2$, where $k_1 \leq t$.

Output: A $H \times W$ disclosed secret image S'.

Step 1: For each coordinate $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2-5.

Step 2: Calculate $a_{i_j} = SC_{i_j}(h, w)$ for $j = 1, 2, \cdots, t$. Let's solve the following linear equations according to CRT.

$$\begin{aligned} y &\equiv a_{i_1} \,(\mathrm{mod}\ m_{i_1}) \\ y &\equiv a_{i_2} \,(\mathrm{mod}\ m_{i_2}) \\ &\cdots \\ y &\equiv a_{i_{t-1}} \,(\mathrm{mod}\ m_{i_{t-1}}) \\ y &\equiv a_{i_t} \,(\mathrm{mod}\ m_{i_t}) \end{aligned} \tag{3.1}$$

Step 3: Calculate $T^* = \left\lfloor \frac{y}{p} \right\rfloor$.

Step 4: For $k_x = k_1, k_1+1, \cdots k_2$, if $T^* \geq T_{k_x}$, let $s_{k_x} \equiv y \,(\mathrm{mod}\ p)$; otherwise let $s_{k_x} = y \,(\mathrm{mod}\ p) + p$.

Step 5: ${k_x}^* = \underset{k_x \in [k_1, k_2]}{\arg\min} \{k_x | \, s_{k_x} = s_{k_x+1} = \cdots = s_{min(t,k_2)}\}$. Set $S'(h, w) = s_{{k_x}^*}$.

Step 6: Output the disclosed secret image S'.

3. In Step 2 of Algorithm 1, T_{k_x} divides interval $\left[\left\lceil \frac{N_{k_x}}{p} \right\rceil, \left\lfloor \frac{M_{k_x}}{p} - 1 \right\rfloor\right]$ into two parts with a view to classify $0 \leq x < p$ or $p \leq x \leq 255$ according to Step 4 of Algorithm 2. As a result, s can be losslessly disclosed for arbitrary $x \in [0, 255]$.
4. In Step 4 of our Algorithm 1, we know A is randomly picked up from $\left[\left\lceil \frac{N_{k_x}}{p} \right\rceil, \left\lfloor \frac{M_{k_x}}{p} - 1 \right\rfloor\right]$, thus, $N_{k_x} \leq y < M_{k_x}$ in order to obtain (k_x, n) threshold for y as explained in Section 2.1.
5. In Step 4 of Algorithm 1, A is randomly selected for every secret pixel s, hence $y = s + Ap$ can enlarge s value in order to scramble both the correlations between adjacent pixels and the secret pixel value without auxiliary encryption.

6. In Step 4 of Algorithm 1, $y = s + Ap$ and $s < p$ will determine a unique s according to $s \equiv y \,(\mathrm{mod}\ p)$.
7. In the recovery phase, for the current processing location (h, w), we do not know its threshold, thus, in Steps 4–5 of Algorithm 2 we search for the minimum threshold satisfying losslessly recovering the original secret pixel s, denoted as ${k_x}^*$.
8. Our (k_1, k_2, n) threshold extension method may be also suitable for other SIS, such as polynomial-based SIS.

Moreover, we explain the differences between Algorithm 1 and the classical ones as follows.

1. Ramp SIS has not been formally introduced before our work.
2. CRT is first applied to Algorithm 1 to achieve ramp SIS.
3. Steps 1–4 of Algorithm 1 are different from the classical CRT-based SIS schemes since Steps 1–4 will achieve ramp SIS proved in Section 3.2.

3.2. Security and progressiveness analyses

We will show performances of the proposed method by theoretically analyzing the security, visual recognition and valid ramp threshold construction. In Theorem 1, we will prove that the proposed scheme is a valid (k_1, k_2, n) ramp SIS construction. Prior to the proof of Theorem 1, some Lemmas are given.

Without loss of generality, in the following analyses, we assume that ${k_x}^* = k_0$ threshold is selected in Step 3 of Algorithm 1 for now processing pixel value $s = S(h, w)$.

Lemma 1. *Each shadow generated by our method gives no clue about the secret image.*

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

If A is fixed, since s represents the pixel value of secret image, we assume s and $s - p$ is random in range $[0, 255]$. Due to $a_i \equiv (s + Ap) \pmod{m_i}$, we have a_i is random in range $[0, m_i)$.

On the other hand, if s is fixed, $\gcd(m_i, p) = 1$, thus, $Ap \pmod{m_i}$ will cover all possible values in range $[0, m_i)$. We have $s + Ap \pmod{m_i}$ will cover all possible values in range $[0, m_i)$ as well. As a result, we have a_i is random in range $[0, m_i)$.

Thus, the Lemma is proved to be met. □

Lemma 2. *In the proposed scheme, any k_0 or more shadow pixels can disclose the secret pixel losslessly.*

Proof. Since s represents the pixel value of secret image, we will prove any k_0 or more shadows can disclose s losslessly.

In order to disclose s, we only need to find y due to $s \equiv y \pmod{p}$ or $s \equiv y \pmod{p} + p$.

When $a_{i_1}, a_{i_2}, \cdots a_{i_{k_0}}$ are given, according to CRT, there exists only solution y modulo $N_1 = \prod_{j=1}^{k_0} m_{i_j}$ since $N_1 \geq M_{k_0}$. Finally we can uniquely determine y and thus, s based on Steps 4-5 of our Algorithm 2. □

Lemma 3. *In the proposed scheme, any $k_0 - 1$ or less shadows give no clue about secret.*

Proof. When $k_0 - 1$ shadow pixels $a_{i_1}, a_{i_2}, \cdots a_{i_{k_0-1}}$ are given, according to CRT then all we have is y_0 modulo $N_2 = \prod_{j=1}^{k_0-1} m_{i_j}$, where $y_0 \in [0, N_2 - 1]$. On one hand, the true $y \in [N_{k_0}, M_{k_0} - 1]$, which is absolutely different from y_0. On the other hand, since $N_{k_0} \geq N_2$, $N_{k_0} \leq y < M_{k_0}$ and $\gcd(N_2, p) = 1$, in $[N_2, M_{k_0} - 1]$, $y_0 + b \prod_{j=1}^{k_0-1} m_{i_j}$ for $b = 1, 2, \cdots, m_{i_{k_0}} - 1$ are also the solutions for the collected $k_0 - 1$ equations in Eq. (3.1). Thus, there are another $m_{i_{k_0}} - 1$ solutions in $[N_2, M_{k_0} - 1]$, other than only one. Thus $k_0 - 1$ or less shadows give no clue about secret. □

Theorem 1. *Our method is a valid (k_1, k_2, n) ramp SIS construction.*

Proof. Based on the above Lemmas, we know for now processing pixel value $s = S(h, w)$ (k_0, n) threshold is achieved by our method.

Since $sc_1, sc_2, \cdots sc_n$ are generated according to the secret pixel s with (k_0, n) threshold, we can disclose the secret s when we collect any k_0 or more shadow pixels.

Since in Step 3 of Algorithm 1, for every processing pixel value $s = S(h, w)$, a threshold k_x in $[k_1, k_2]$ is selected randomly, when we collect more than k_1 shadows, more secret pixels will be disclosed losslessly so that the progressive quality of disclosed secret image will be gained. On the

other hand, when we collect any k_2 or more shadows, every pixel of the secret image is disclosed losslessly, thus, the secret image is disclosed losslessly. As a result, our method is a valid (k_1, k_2, n) ramp SIS construction. □

4. Experimental results and analyses

In this section, experiments and analyses are taken into account to evaluate the effectiveness of the proposed scheme.

4.1. Image illustration

Figure 1 is one experimental result of our proposed (k_1, k_2, n) ramp CRT-based SIS, where $p = 128, m_1 = 245, m_2 = 247, m_3 = 249, m_4 = 251, m_5 = 253$, $k_1 = 2, k_2 = 4, n = 5$ and its employed grayscale secret image is in Figure 1(a). Figures 1(b–f) are the generated 5 shadows, which are noise-like. Figures 1(g–j) display the disclosed grayscale secret image with any $t\,(2 \le t \le 5)$ shadows by our recovery method, where $S'_{1,2,\cdots,t}$ is the disclosed secret image S' from $SC_1, SC_2, \cdots, SC_t$ and for saving pages we only give the disclosed results with the first tth shadows. When more shadows are used, better disclosed secret image is obtained in $[k_1, k_2]$, thus, the proposed (k_1, k_2, n) ramp SIS is progressive in $[k_1, k_2]$. The disclosed secret images with any k_2 or more shadows, as Figures $1(i) - (j)$, are the same as the original secret image in Figure $1(a)$, since $\sum_{h=1}^{H}\sum_{w=1}^{W} |S(h, w) - S'(h, w)| = 0$.

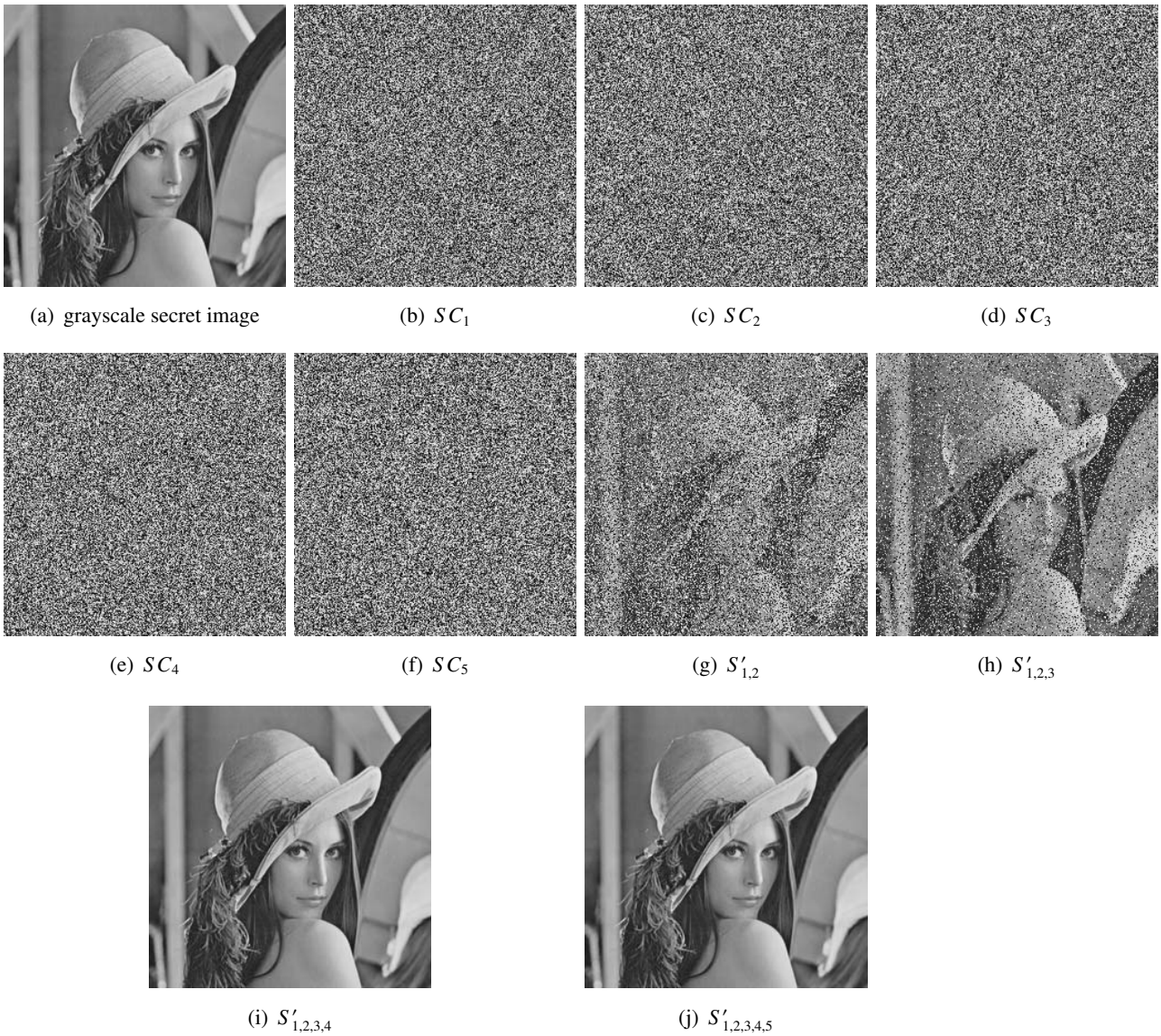
Furthermore, progressive rate can be adopted to evaluate the progressive effect of the disclosed secret image [51]. In Figure 1, taking PSNR as an example, the progressive rate at $t = 2$ is 3.0746 and the progressive rate at $t = 3$ is $+\infty$.

In addition, Figure 2 shows shadows histogram analyses of proposed (k_1, k_2, n) ramp SIS corresponding to Figure 1. For each shadow, the pixel values are approximately uniformly distributed in range $[0, m_i - 1]$, which tells that each shadow gives no clue about the secret image. In the following experiments, we will omit the shadows histogram analyses for saving pages.

Figure 3 is the further experimental result of our proposed (k_1, k_2, n) ramp CRT-based SIS, where $p = 128, m_1 = 245, m_2 = 247, m_3 = 249, m_4 = 251, m_5 = 253$, $k_1 = 3, k_2 = 5, n = 5$ and its employed grayscale secret image is in Figure 3(a). Figures 3(b–f) are the generated 5 shadows, which are noise-like. Figures 3(g–j) display the disclosed grayscale secret image with any $t\,(2 \le t \le 5)$ shadows by our recovery method. When less than k_1 shadows are inspected, nothing of the secret image can be obtained. When k_1 or more shadows are collected, the secret image can be disclosed in a degree. When more shadows are used, better disclosed secret image is obtained as well in $[k_1, k_2]$, thus, the proposed (k_1, k_2, n) ramp SIS is progressive in $[k_1, k_2]$ as well. The disclosed secret images with any k_2 shadows as Figure 3(j) is the same as the original secret image Figure 3(a) as well.

Based on the above results we conclude that:

1. The shadows are noise-like, thus, every single shadow is secure.
2. When any $t < k_1$ shadows are inspected, there is no information on the secret image is leaked except for image size, which shows security of our method.
3. When any $t(k_1 \le t \le k_2)$ shadows are collected, the secret image will be disclosed by our recovery method in a progressive way.

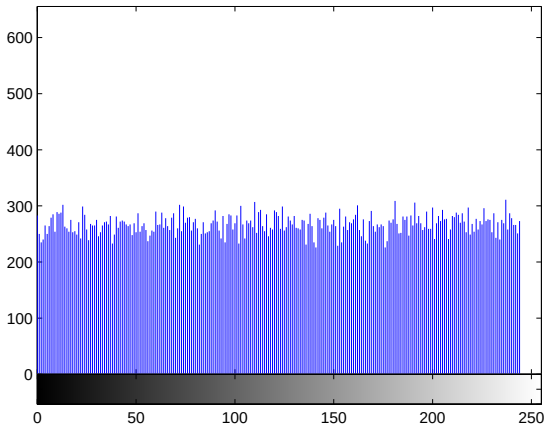


(a) grayscale secret image (b) SC_1 (c) SC_2 (d) SC_3

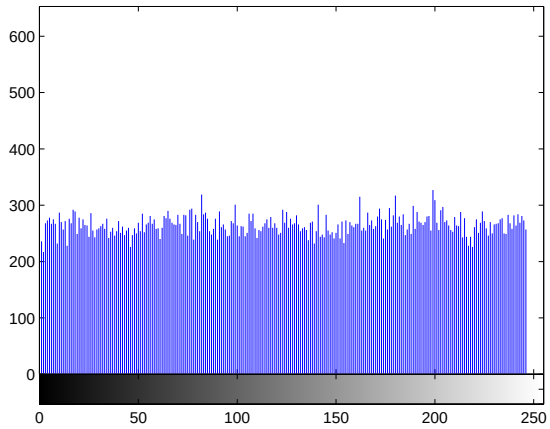
(e) SC_4 (f) SC_5 (g) $S'_{1,2}$ (h) $S'_{1,2,3}$

(i) $S'_{1,2,3,4}$ (j) $S'_{1,2,3,4,5}$

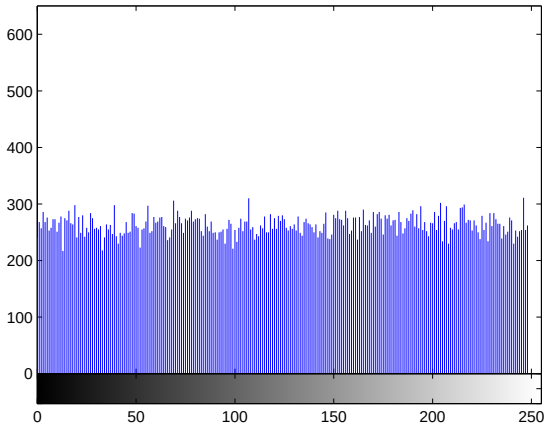
Figure 1. Simulation results of the proposed (k_1, k_2, n) ramp CRT-based PSIS, where $k_1 = 2, k_2 = 4, n = 5$. (a) The grayscale secret image; (b) – (f) five shadows SC_1, SC_2, SC_3, SC_4 and SC_5; (g) – (j) disclosed results by any t shadows, where $t = 2, 3, 4$ and 5, respectively.



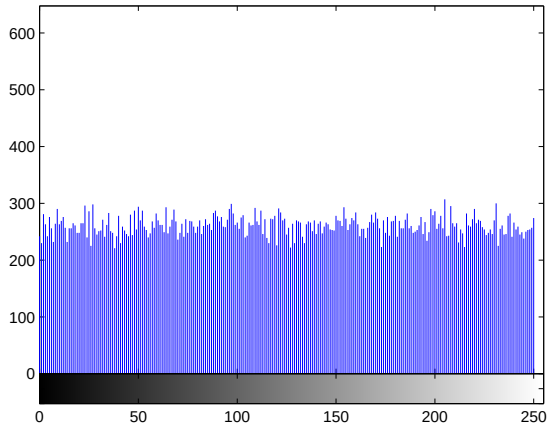
(a) Histogram of SC_1



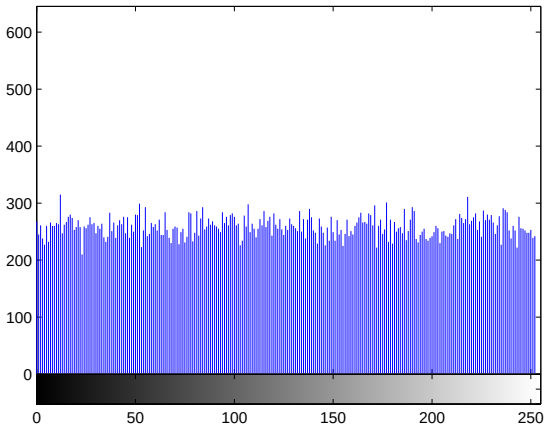
(b) Histogram of SC_2



(c) Histogram of SC_3

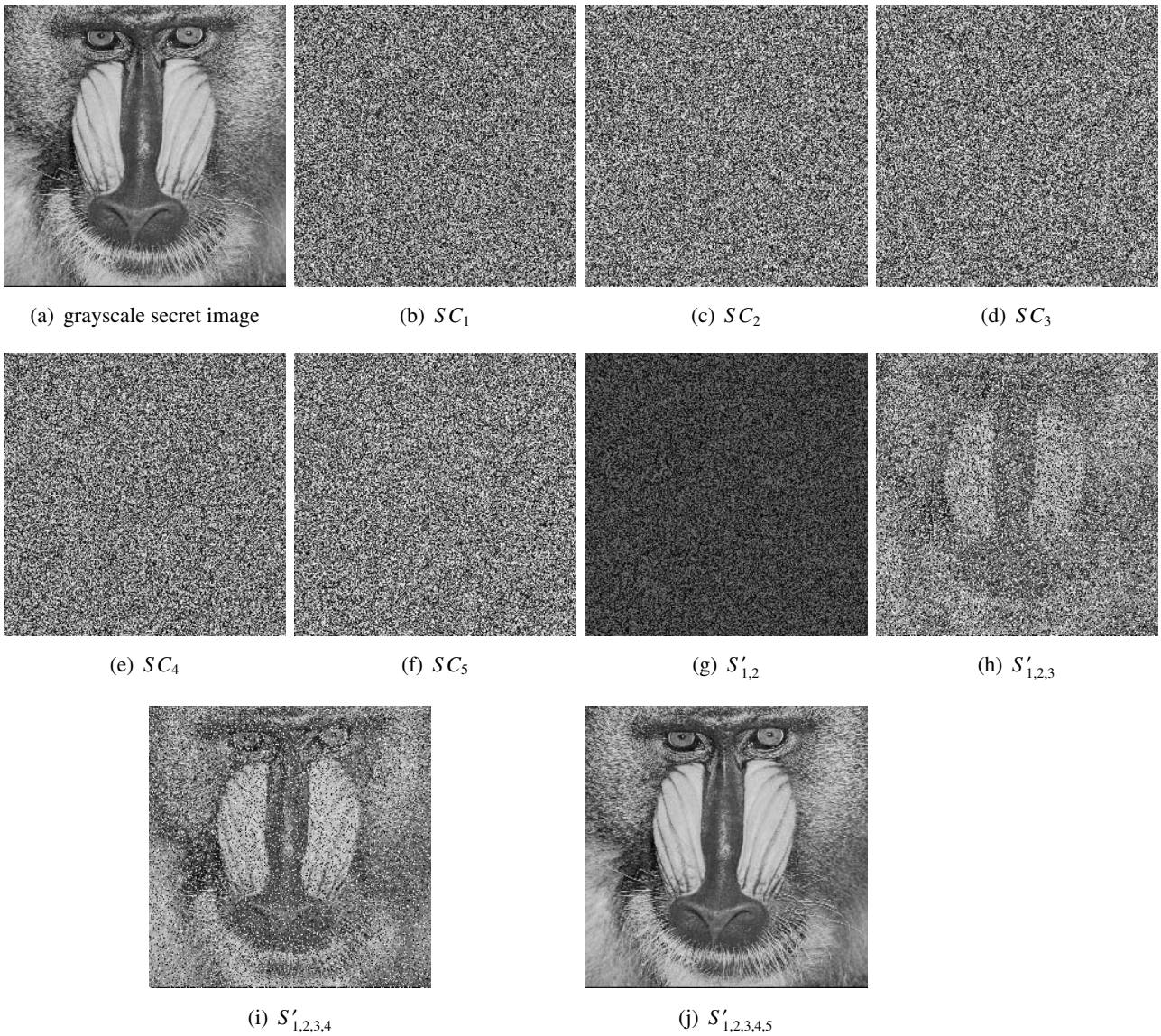


(d) Histogram of SC_4



(e) Histogram of SC_5

Figure 2. Histogram analyses of shadows in Figure 1.



(a) grayscale secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) SC_5 (g) $S'_{1,2}$ (h) $S'_{1,2,3}$

(i) $S'_{1,2,3,4}$ (j) $S'_{1,2,3,4,5}$

Figure 3. Simulation results of the proposed (k_1, k_2, n) ramp CRT-based PSIS, where $k_1 = 3, k_2 = 5, n = 5$. (a) The grayscale secret image; (b) − (f) five shadows SC_1, SC_2, SC_3, SC_4 and SC_5; (g) − (j) disclosed results by t shadows, where $t = 2, 3, 4$ and 5, respectively.

4. When we collect any k_2 or more shadows, the secret image is disclosed losslessly by our recovery method.
5. (k_1, k_2, n) ramp SIS is achieved.

4.2. Available parameters

Some available parameters of $p, m_1, m_2 \cdots, m_n$ for different participant numbers are suggested in Table 1, some of which are applied to our experiments as well. The user can also search other parameters according to specific applications.

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

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

4.3. Comparisons with related works

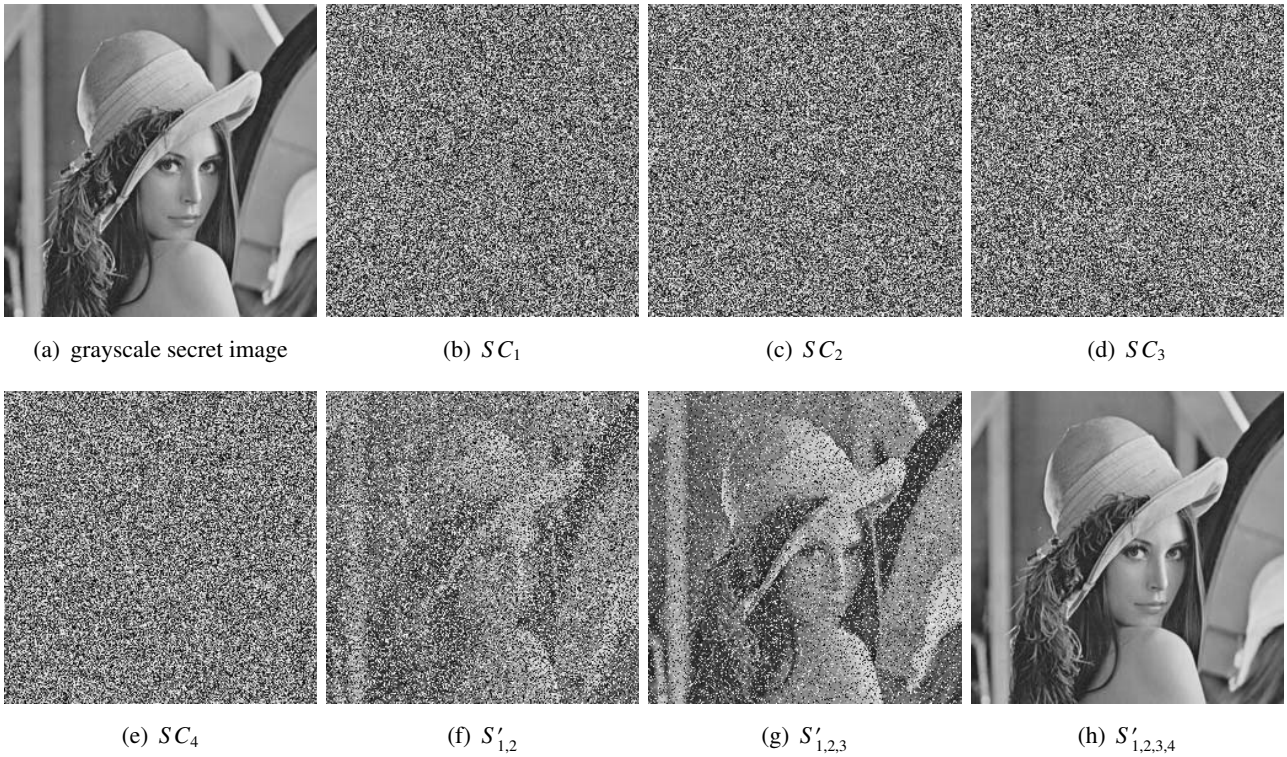
Herein, we compare the proposed scheme with other related schemes especially VSS [28] and polynomial-based scheme [12], since they are typical SIS schemes. Furthermore, VSS in [28] is progressive without codebook design and pixel expansion based on stacking recovery. Polynomial-based scheme in [12] is fully lossless.

We note that, as stated in section 2.2, in general secret sharing is hard to be directly applied to SIS, thus, we omit the comparisons to ramp secret sharing.

Figure 4 is one experimental result of our proposed (k_1, k_2, n) ramp CRT-based SIS, where $p = 131, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, k_1 = 2, k_2 = 4, n = 4$ and its employed grayscale secret image is in Figure 4(a). Figures 4(b–e) are the generated 4 shadows, which are noise-like. Figures 4(f–h) display the disclosed grayscale secret image with any $t\,(2 \le t \le 4)$ shadows by our recovery method. When more shadows are used, better disclosed secret image is obtained as well in $[k_1, k_2]$, thus, the proposed (k_1, k_2, n) ramp SIS is progressive in $[k_1, k_2]$. The disclosed secret image with k_2 shadows as Figure 4(h) is the same as the original secret image Figure 4(a), since $\sum_{h=1}^{H}\sum_{w=1}^{W} |S(h,w) - S'(h,w)| = 0$ as well.

Figure 5 is further experimental result of our proposed (k_1, k_2, n) ramp CRT-based SIS, where $p = 131, m_1 = 251, m_2 = 253, m_3 = 254, m_4 = 255, k_1 = 2, k_2 = 2, n = 4$ and its employed grayscale secret image is in Figure 5(a). Figures 5(b–e) are the generated 4 shadows, which are noise-like. Figures 5(f–h) display the disclosed grayscale secret image with any $t\,(2 \le t \le 4)$ shadows by our

recovery method. When two or more shadows are used, the secret image is losslessly disclosed so that our proposed (k_1, k_2, n) ramp SIS reduces to (k, n) ramp SIS if $k_1 = k_2$.



(a) grayscale secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $S'_{1,2}$ (g) $S'_{1,2,3}$ (h) $S'_{1,2,3,4}$

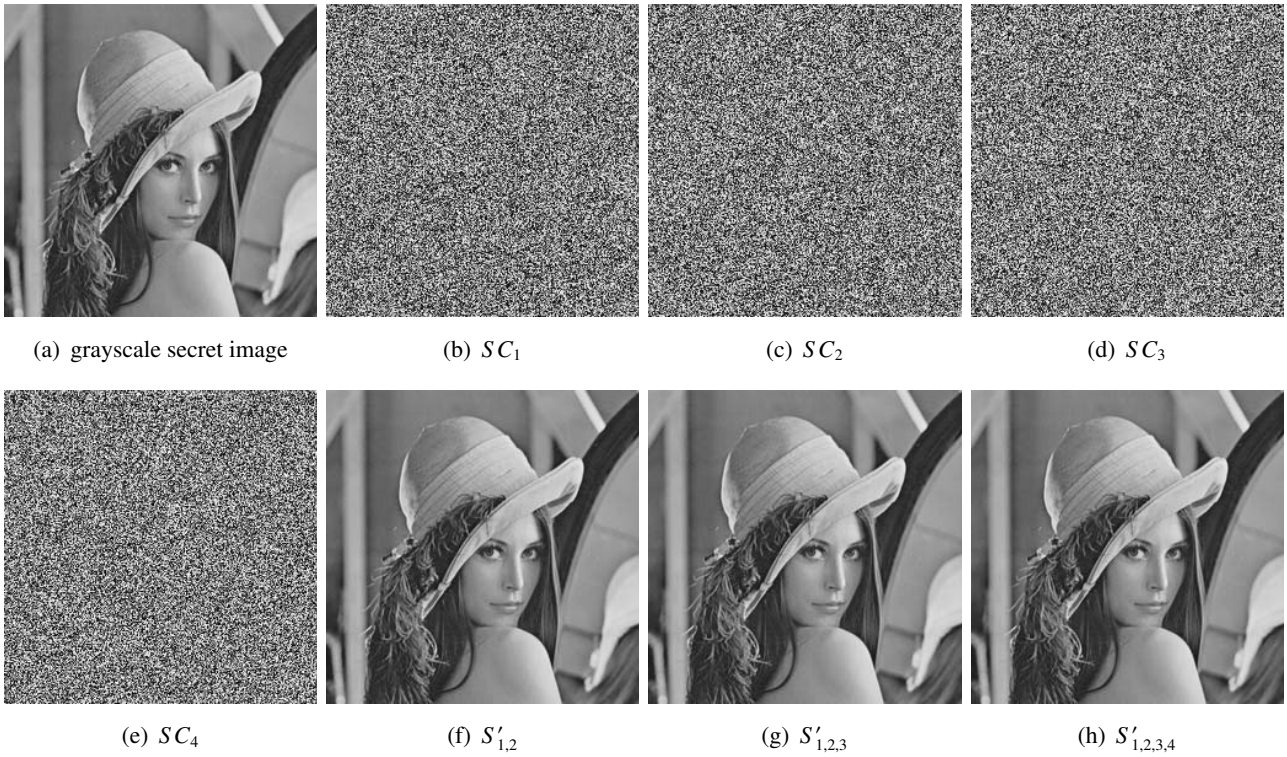
Figure 4. Simulation results of the proposed (k_1, k_2, n) ramp CRT-based PSIS, where $k_1 = 2, k_2 = 4, n = 4$. (a) The grayscale secret image; (b) – (e) four shadows SC_1, SC_2, SC_3 and SC_4; (f) – (h) disclosed results by t shadows, where $t = 2, 3$ and 4, respectively.

Then Figure 6 illustrates one experimental result of VSS for (k, n) threshold in [28], where $k = 2, n = 4$ and its employed binary secret image is in Figure 6(a). Figures 6(b–e) are the generated 4 shadows, which are noise-like as well. Figures 6(f–h) display the disclosed grayscale secret image with any $t\,(2 \le t \le 4)$ shadows by stacking recovery. When 2 or more shadows are used, better disclosed secret image is obtained as well in $[k, n]$, thus, VSS for (k, n) threshold in [28] is progressive in $[k, n]$.

According to Figure 4, Figure 5 and Figure 6, comparisons between VSS and our method are given as follows.

1. Our method is for (k_1, k_2, n) ramp threshold due to random threshold selection in Step 3 of our method while VSS is only for (k, n) threshold, where (k, n) threshold is one special case of our method.
2. Our disclosing method is modular arithmetic since CRT while VSS is stacking, thus, our disclosing method needs more computation than VSS.
3. The secret image is disclosed in a progressive way by our method when $t(k_1 \le t \le k_2)$ shadows are collected due to random threshold selection in Step 3 of our method, while VSS is progressive in $[k, n]$.

4. Our method discloses the secret image losslessly when we collect any k_2 or more shadows since Steps 4–5 of our method, while VSS is lossy.
5. Our method is suitable for grayscale secret image as well as possible color secret image due to image characteristic analyses and CRT parameters design, while VSS is for binary secret image.



(a) grayscale secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $S'_{1,2}$ (g) $S'_{1,2,3}$ (h) $S'_{1,2,3,4}$

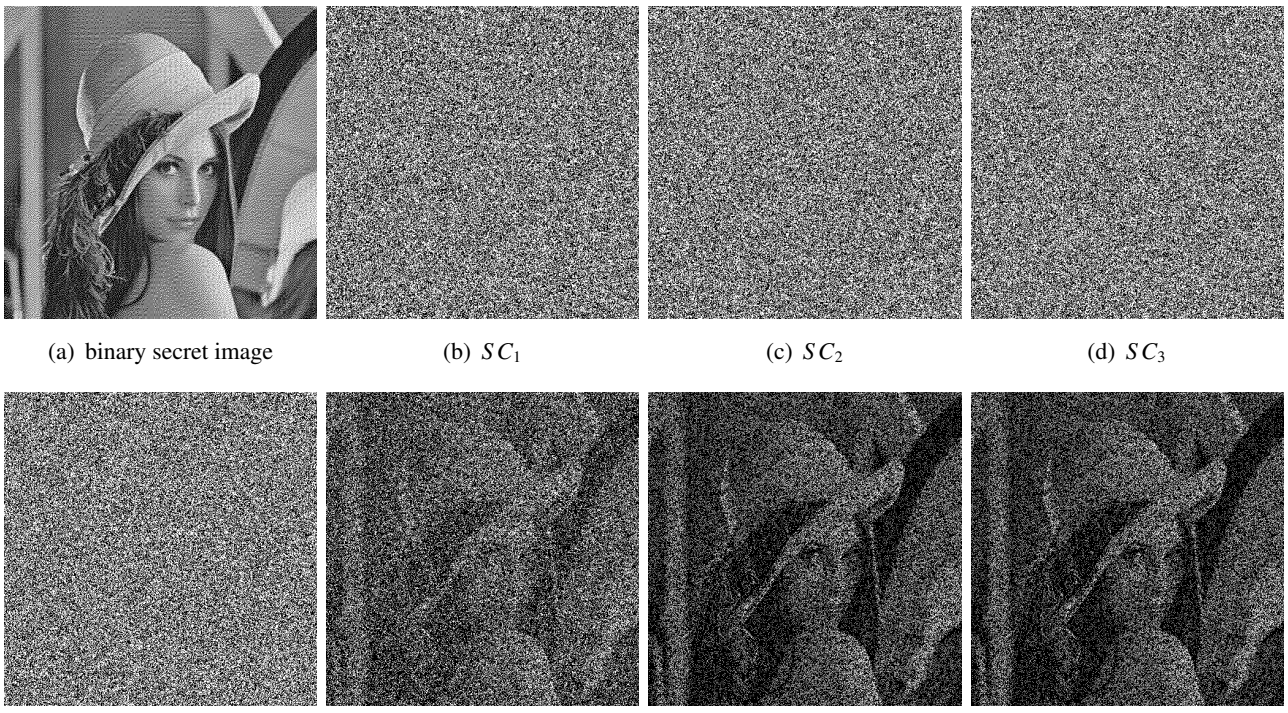
Figure 5. Simulation results of the proposed (k_1, k_2, n) ramp CRT-based PSIS, where $k_1 = 2, k_2 = 2, n = 4$. (a) The grayscale secret image; (b) − (e) four shadows SC_1, SC_2, SC_3 and SC_4; (f) − (h) disclosed results by t shadows, where $t = 2, 3$ and 4, respectively.

Figure 7 is one experimental result of (k, n) threshold polynomial-based SIS [12], where $k = 2, n = 4$ and its employed grayscale secret image is in Figure 7(a). Figures 7(b–e) are the generated 4 shadows, which are noise-like. Figures 7(f–h) display the same disclosed grayscale secret images with high-resolution with any $k = 2$ or more shadows by Lagrange interpolation.

According to Figure 4, Figure 5 and Figure 7, comparisons between our method and polynomial-based SIS are given as follows.

1. Our method is for (k_1, k_2, n) ramp threshold due to random threshold selection in Step 3 of our method while polynomial-based SIS is only for (k, n) threshold, where (k, n) threshold is one special case of our method.
2. Our disclosing method is modular arithmetic ($O(k)$ operations [44]) since CRT while polynomial-based SIS is Lagrange interpolation ($O(k \log^2 k)$ operations [44]), thus, our disclosing method needs less computation than polynomial-based SIS.

3. The secret image is disclosed in a progressive way by our method when any $t(k_1 \leq t \leq k_2)$ shadows are gained due to random threshold selection in Step 3 of our method, while polynomial-based SIS is "all-or-nothing".
4. In some polynomial-based SIS schemes, it is generally lossy recovery since secret image is decoded by modular 251 which is less than max grayscale value 255. The recovering image will be lossy if the pixel value of the secret image exceeds 251 and some polynomial-based SIS schemes have a little bit of loss. By contrast, our method is lossless because of CRT. We further analyze this issue as follows. In polynomial-based SIS, the primes near 255 are 257 and 251. In most polynomial-based SIS, 251 is used. If 257 is used, we cannot store the i-th shadow pixel for the value of 256; otherwise 251 is used, we cannot disclose the value of the secret pixel greater than 250. Although some methods are given to solve the 251 problem, such as selecting the prime 257 [52], primitive polynomial for $GF(2^8)$, splitting the secret pixel greater than 250 into two pixels and so on, they are achieved at some other costs. Taking [53] as one example, Huffman coding and image differencing process are employed to reduce the size of each shadow and to avoid auxiliary encryption. Primitive polynomial for $GF(2^8)$ is adopted to avoid quality degradation. However, primitive polynomial for $GF(2^8)$ has larger computational complexity.



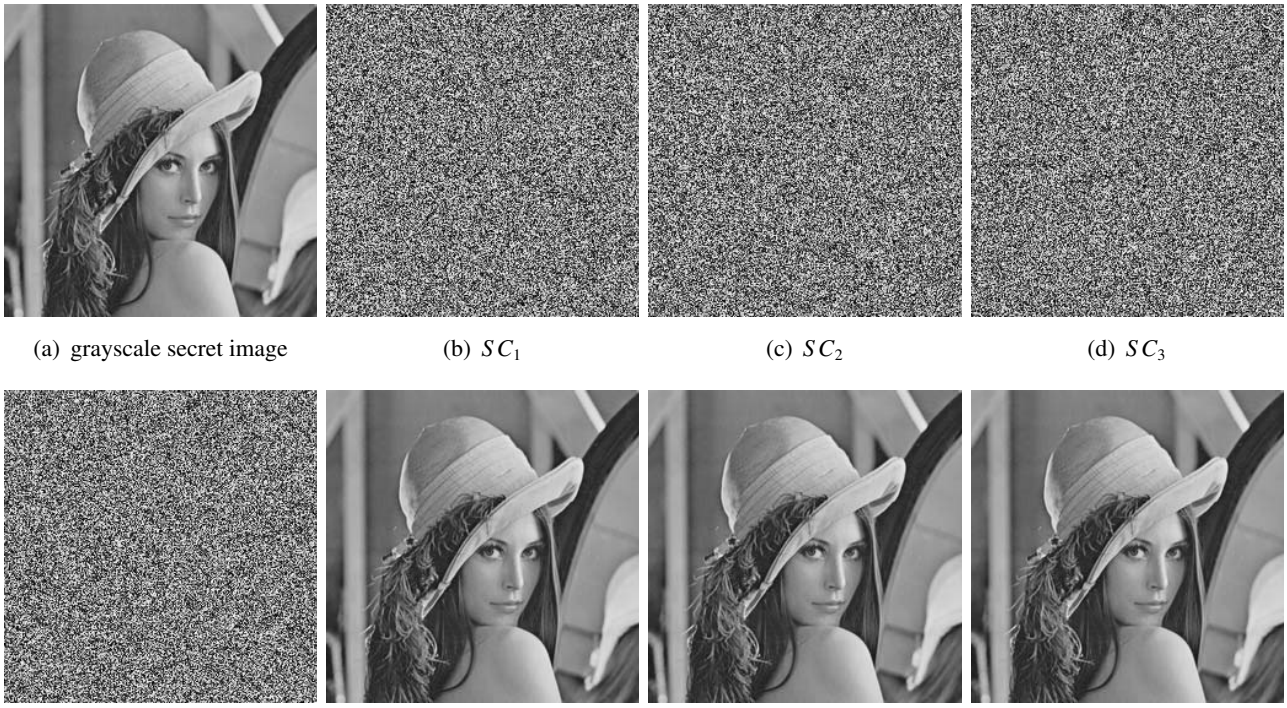
(a) binary secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $S'_{1,2}$ (g) $S'_{1,2,3}$ (h) $S'_{1,2,3,4}$

Figure 6. Simulation results of VSS for (k, n) threshold [28], where $k = 2, n = 4$. (a) The binary secret image; (b) − (e) four shadows SC_1, SC_2, SC_3 and SC_4; (f) − (h) disclosed results by t shadows, where $t = 2, 3$ and 4, respectively.

In addition, actually, when $k_1 = k_2 = k$, the (k_1, k_2, n) ramp SIS will be a (k, n)-SIS. Progressiveness is studied in some degree in VSS while that is seldom discussed in polynomial-based SIS. However, VSS is only suitable for binary image rather than grayscale image.

In a word, based on image characteristics and CRT, the proposed (k_1, k_2, n) ramp SIS has the features of (k_1, k_2, n) threshold with only modular arithmetic recovery method and no auxiliary encryption, which outperforms conventional (k, n) threshold SIS.



(a) grayscale secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $S'_{1,2}$ (g) $S'_{1,2,3}$ (h) $S'_{1,2,3,4}$

Figure 7. Simulation results of (k, n) threshold polynomial-based SIS [12], where $k = 2, n = 4$. (a) The grayscale secret image; (b) − (e) four shadows SC_1, SC_2, SC_3 and SC_4; (f) − (h) disclosed results by t shadows, where $t = 2, 3$ and 4, respectively.

4.4. Quality of disclosed secret image

For the above experiments, the quality evaluation metrics of the disclosed secret image are given in Table 2. According to Table 2, the proposed method achieves progressive characteristic in general (k_1, k_2, n) threshold when more shadows are collected, which outperforms conventional SIS as well.

Table 2. The quality evaluation of disclosed secret image.

Schemes	Metrics	$t = 2$	$t = 3$	$t = 4$	$t = 5$
Our $(2, 4, 5)$ ramp SIS in Figure 1	PSNR	10.4435	13.5181	$+\infty$	$+\infty$
Our $(2, 4, 5)$ ramp SIS in Figure 1	SSIM	0.0545	0.1500	1	1
Our $(2, 4, 5)$ ramp SIS in Figure 1	UQI	0.0566	0.1609	1	1
Our $(2, 4, 5)$ ramp SIS in Figure 1	NC	0.9351	0.9679	1	1
Our $(3, 5, 5)$ ramp SIS in Figure 3	PSNR	-	10.2597	13.2965	$+\infty$
Our $(3, 5, 5)$ ramp SIS in Figure 3	SSIM	-	0.1224	0.3198	1
Our $(3, 5, 5)$ ramp SIS in Figure 1	UQI	-	0.1204	0.3234	1
Our $(3, 5, 5)$ ramp SIS in Figure 1	NC	-	0.9133	0.9577	1
Our $(2, 4, 4)$ ramp SIS in Figure 4	PSNR	10.2811	13.2348	$+\infty$	-
Our $(2, 4, 4)$ ramp SIS in Figure 4	SSIM	0.0528	0.1403	1	-
Our $(2, 4, 4)$ ramp SIS in Figure 1	UQI	0.0544	0.1511	1	-
Our $(2, 4, 4)$ ramp SIS in Figure 1	NC	0.9482	0.9745	1	-
Our $(2, 2, 4)$ ramp SIS in Figure 5	PSNR	$+\infty$	$+\infty$	$+\infty$	
Our $(2, 2, 4)$ ramp SIS in Figure 5	SSIM	1	1	1	-
Our $(2, 2, 4)$ ramp SIS in Figure 1	UQI	1	1	1	-
Our $(2, 2, 4)$ ramp SIS in Figure 1	NC	1	1	1	-
$(2, 4)$ threshold RGVSS in Figure 6	α	0.2886	0.5018	0.5018	-
Polynomial-based $(2, 4)$ threshold SIS in Figure 7	PSNR	$+\infty$	$+\infty$	$+\infty$	-
Polynomial-based $(2, 4)$ threshold SIS in Figure 7	SSIM	1	1	1	-
Polynomial-based $(2, 4)$ threshold SIS in Figure 7	UQI	1	1	1	-
Polynomial-based $(2, 4)$ threshold SIS in Figure 7	NC	1	1	1	-

5. Conclusion

In this paper, based on the study of image characteristics, the Chinese remainder theorem (CRT) and secret image sharing (SIS), we proposed (k_1, k_2, n) ramp SIS. Our method realizes (k_1, k_2, n) threshold and lossless recovery for grayscale image without auxiliary encryption. When we collect any k_1 or more shadows, the secret image will be disclosed in a progressive way. On the other hand, when we collect any k_2 or more shadows, the secret image will be disclosed losslessly. Furthermore, the disclosing method is only modular arithmetic resulting in ability in real-time application. Theoretical analyses and experiments are performed to display the effectiveness of our method. Applying our method to other SIS schemes like polynomial-based SIS and comparing to related ramp secret sharing will be our future work.

Acknowledgments (All sources of funding of the study must be disclosed)

The authors would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Numbers: 61602491, 61501148) and the Key Program of the National University of Defense Technology (Grant Number: ZK-17-02-07).

Conflict of interest

We have no conflicts of interest to declare.

References

1. Z. Qian, H. Xu, X. Luo, et al., New framework of reversible data hiding in encrypted jpeg bitstreams, *IEEE Trans. Circuit Syst. Video Tech.*, **29** (2019), 351–362.
2. Y. Zhang, C. Qin, W. Zhang, et al., On the fault-tolerant performance for a class of robust image steganography, *Signal Process.*, **146** (2018), 99–111,
3. A. Belazi and A. A. A. El-Latif, A simple yet efficient s-box method based on chaotic sine map, *Optik-Int. J. Light Electron Opt.*, **130** (2017), 1438–1444.
4. Y. Cheng, Z. Fu and B. Yu, Improved visual secret sharing scheme for qr code applications, *IEEE Trans. Inf. Forensics Security.*, **13** (2018), 2393–2403.
5. C. Kim, D. Shin, L. Leng, et al., Separable reversible data hiding in encrypted halftone image, *Displays*, **55** (2018), 71–79.
6. Y. Ma, X. Luo, X. Li, et al., Selection of rich model steganalysis features based on decision rough set α -positive region reduction, *IEEE Trans. Circuit Syst. Video Tech.*, **29** (2019), 336–350.
7. G. Wang, F. Liu and W. Q. Yan, Basic visual cryptography using braille, *Int. J. Digital Crime Forensics (IJDCF)*, **8** (2016), 85–93.
8. X. Yan, S. Wang, X. Niu, et al., Generalized random grids-based threshold visual cryptography with meaningful shares, *Signal Process.*, **109** (2015), 317–333.
9. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.
10. 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*, (A DeSantis), Springer, 1995, 1–12.
11. L. Liu, Y. Lu, X. Yan, et al., A progressive threshold secret image sharing with meaningful shares for gray-scale image, in *Mobile Ad-Hoc and Sensor Networks (MSN), 2016 12th International Conference on*, IEEE, 2016, 380–385.
12. W. Ding, K. Liu, X. Yan, et al., Polynomial-based secret image sharing scheme with fully lossless recovery, *Int. J. Digital Crime Forensics (IJDCF)*, **10** (2018), 120–136.
13. L. Bao, S. Yi and Y. Zhou, Combination of sharing matrix and image encryption for lossless (k, n) -secret image sharing, *IEEE Trans. Image Process.*, **26** (2017), 5618–5631.

14. W. Ding, K. Liu, X. Yan, et al., A general (k,n) threshold secret image sharing construction based on matrix theory, *Data Science: Third International Conference of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2017, Proceedings, Part I*, (2017), 331–340.
15. P. Li, Z. Liu and C. N. Yang, A construction method of (t,k,n)-essential secret image sharing scheme, *Signal Process. Image Commun.*, **65** (2018), 210–220.
16. Y. Liu and C. Yang, Scalable secret image sharing scheme with essential shadows, *Signal Process. Image Commun.*, **58** (2017), 49–55.
17. Y. Liu, C. Yang, Y. Wang, et al., Cheating identifiable secret sharing scheme using symmetric bivariate polynomial, *Inf. Sci.*, **453** (2018), 21–29.
18. X. Wu, C. N. Yang, Y. T. Zhuang, et al., Improving recovered image quality in secret image sharing by simple modular arithmetic, *Signal Process. Image Commun.*, **66** (2018), 42–49.
19. H. Chao and T. Fan, Generating random grid-based visual secret sharing with multi-level encoding, *Signal Process. Image Commun.*, **57** (2017), 60–67.
20. T. Guo and L. Zhou, Constructing visual cryptography scheme by hypergraph decomposition, *Procedia Comput. Sci.*, **131** (2018), 336–343,
21. Y. Ren, F. Liu, T. Guo, et al., Cheating prevention visual cryptography scheme using latin square, *IET Inf. Secur.*, **11** (2017), 211–219.
22. M. Sasaki and Y. Watanabe, Visual secret sharing schemes encrypting multiple images, *IEEE Trans. Inf. Forensics Security*, **13** (2018), 356–365.
23. Z. Wang, G. R. Arce and G. Di Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Security*, **4** (2009), 383–396.
24. J. Weir and W. Yan, A comprehensive study of visual cryptography, in *Transactions on DHMS V, LNCS 6010, Springer-Verlag*, Springer, Berlin, Heidelberg, 2010, 70–105.
25. Z. X. Fu and B. Yu, Visual cryptography and random grids schemes, in *Digital-Forensics and Watermarking*, Springer, Auckland, New Zealand, 2014, 109–122.
26. F. Liu and C. Wu, Embedded extended visual cryptography schemes, *IEEE Trans. Inf. Forensics Security*, **6** (2011), 307–322.
27. X. Wu and W. Sun, Visual secret sharing for general access structures by random grids, *IET Inf. Secur.*, **6** (2012), 299–309.
28. X. Yan, X. Liu and C. N. Yang, An enhanced threshold visual secret sharing based on random grids, *J. Real-Time Image Proc.*, **14** (2018), 61–73.
29. X. Yan and Y. Lu, Progressive visual secret sharing for general access structure with multiple decryptions, *Multimed. Tools Appl.*, **77** (2018), 2653–2672.
30. X. Yan, Y. Lu and L. Liu, General meaningful shadow construction in secret image sharing, *IEEE Access*, **6** (2018), 45246–45255.
31. X. Yan, S. Wang and X. Niu, Threshold construction from specific cases in visual cryptography without the pixel expansion, *Signal Process.*, **105** (2014), 389–398.
32. C. N. Yang, C. C. Wu, et al., A discussion on the relationship between probabilistic visual cryptography and random grid, *Inf. Sci.*, **278** (2014), 141–173.

33. Y. C. Hou, Z. Y. Quan, C. F. Tsai, et al., Block-based progressive visual secret sharing, *Inf. Sci.*, **233** (2013), 290–304.
34. X. Yan and Y. Lu, Generalized general access structure in secret image sharing, *J. Vis. Commun. Image Represent.*, **58** (2019), 89–101,
35. S. K. Chen, Friendly progressive visual secret sharing using generalized random grids, *Optical Engineer.*, **48** (2009), 117001–117001–7.
36. W. P. Fang, Friendly progressive visual secret sharing, *Pattern Recognit.*, **41** (2008), 1410–1414.
37. C. P. Huang, C. H. Hsieh and P. S. Huang, Progressive sharing for a secret image, *J. Syst. Softw.*, **83** (2010), 517–527.
38. C. H. Lin, Y. S. Lee and T. H. Chen, Friendly progressive random-grid-based visual secret sharing with adaptive contrast, *J. Vis. Commun. Image Represent.*, **33** (2015), 31–41,
39. G. R. Blakley and C. Meadows, Security of ramp schemes, *Proc. Crypto*, **196** (1984), 242–268.
40. Q. Chen, D. Pei, C. Tang, et al., A note on ramp secret sharing schemes from error-correcting codes, *Math. Com. Model.*, **57** (2013), 2695–2702.
41. X. Gong, P. Hu, K. W. Shum, et al., A zigzag-decodable ramp secret sharing scheme, *IEEE Trans. Inf. Forensics Security.*, **13** (2018), 1906–1916.
42. X. Jia, D. Wang, D. Nie, et al., A new threshold changeable secret sharing scheme based on the chinese remainder theorem, *Inf. Sci.*, **473** (2019), 13–30,
43. X. Yan, Y. Lu, L. Liu, et al., Chinese remainder theorem-based secret image sharing for (k, n) threshold, *Cloud Computing and Security: Third International Conference, ICCCS 2017,Revised Selected Papers, Part II, (2017)*, 433–440,
44. C. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. Inf. Theory*, **29** (1983), 208–210.
45. X. Yan, Y. Lu and L. Liu, A general progressive secret image sharing construction method, *Signal Process., Image Commun.*, **71** (2019), 66–75,
46. C. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. Inf. Theory*, **30** (1983), 208–210.
47. Z. Wang, A. C. Bovik, H. R. Sheikh, et al., Image quality assessment: from error visibility to structural similarity, *IEEE Trans. Image Process.*, **13** (2004), 600–612.
48. Z. Wang and A. C. Bovik, A universal image quality index, *IEEE Signal Process. Lett.*, **9** (2002), 81–84.
49. X. Yan, Y. Lu, H. Huang, et al., Clarity corresponding to contrast in visual cryptography, *Social Computing: Second International Conference of Young Computer Scientists, Engineers and Educators, ICYCSEE 2016, Proceedings, Part I, (2016)*, 249–257.
50. J. Huang, C. Wang and Y. Wang, A snr method of evaluating image quality based on the hvs model, *J. HEBEI Uni. Sci. Tech.*, **23** (2002), 80–85.
51. X. Yan, Y. Lu, L. Liu, et al., Random grids-based threshold visual secret sharing with improved visual quality, *Digital Forensics and Watermarking: 15th International Workshop, IWDW 2016, Revised Selected Papers*, (2016), 209–222,

52. X. Zhou, Y. Lu, X. Yan, et al., Lossless and efficient polynomial-based secret image sharing with reduced shadow size, *Symmetry*, **10** (2018), 249.

53. R. Z. Wang and C. H. Su, Secret image sharing with smaller shadow images, *Pattern Recognit. Lett.*, **27** (2006), 551–555.

AIMS Press