A Compact Secret Image Sharing Scheme Based on Flexible Secret Matrix Sharing Scheme

Lingfu Wang, Jing Wang*, Mingwu Zhang, and Weijia Huang

School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China
wjing@guet.edu.cn

Abstract. In social networks, Secret Image Sharing (SIS) provides an effective way to protect secret images. However, most existing SIS schemes only support limited access policies, which are not flexible enough for lots of scenarios. In this work, we propose an SIS scheme to solve this defect. The core contributions of our scheme can be summarized as follows. Firstly, we propose a Secret Matrix Sharing Scheme (SMSS), which is extended from the traditional Linear Secret Sharing Scheme (LSSS). Different from LSSS, SMSS shares a secret matrix instead of a single secret value. Secondly, based on our SMSS, we propose an SIS scheme named LM-SIS, which supports *monotonous access policies*. Compared with other SIS schemes, our scheme has advantages in flexibility and efficiency. Furthermore, the LM-SIS scheme is *compact*, which is reflected in its shadow size ratio is approximately $1/k$, where k denotes the root threshold of the access tree. Finally, our scheme provides lossless or approximately lossless recovery, and experimental results show that the PSNR of the recovered images is always greater than 30dB and the SSIM usually exceeds 0.99. By sacrificing a little storage cost, our LM-SIS scheme can achieve *lossless recovery*.

Keywords: Secret image sharing · Linear secret sharing scheme · Access policy · Cauchy matrix · Lossless recovery.

1 Introduction

Nowadays, with the popularization of photo devices and the development of social networks, information (particularly image information) sharing on the internet plays an important role in our daily lives. However, some images, such as sensitive personal images, and confidential military maps, need to be shared securely. Secret Image Sharing (SIS) [1] gives a secure sharing pattern of secrets among a set of participants. Take the threshold (i.e. k-out-of-n) SIS for example. A secret image is encoded into n shadows, and the secret image can be recovered iff we get k or more shadows. In some scenarios, participants may have different statuses and be assigned different privileges. Thus, Essential SIS (ESIS) [2] and Weighted SIS (WSIS) [3] are proposed with limited access policies. In an ESIS scheme, there are two kinds of shadows: essential shadows and non-essential shadows. The secret image can be recovered iff the number of shadows

and the number of essential shadows are equal to or greater than the thresholds respectively. Furthermore, WSIS introduces weights for shadows to present diverse privileges of different participants. The secret image can be recovered iff the total weight of the collected shadows reaches the threshold.

However, ESIS and WSIS only implement a relatively limited access policy, which will severely restrict the flexibility of SIS in some situations. For example, in a company with many departments, each department may have subordinate relationships, the implementation of secret sharing in the company requires complex access policies. In this paper, we propose an SIS scheme that supports monotonous access policies. At the same time, considering computational efficiency and storage redundancy, the access policy should be presented in a compact form. Linear Secret Sharing Scheme (LSSS) [4] provides a smart way to share secrets through linear matrices. On the one hand, LSSS can present arbitrary monotonous access policies. On the other hand, LSSS has advantages in computational efficiency, since it can be processed by linear functions. However, LSSS can not be directly introduced into SIS, because LSSS only supports sharing a single secret value. Thus, it requires a multi-secret sharing scheme to support a flexible, efficient and secure SIS. Additionally, considering that the recovered image quality is very important in some cases. So the proposed SIS scheme should provide lossless or approximately lossless recovered images.

In this paper, we propose a Secret Matrix Sharing Scheme (SMSS) extended from LSSS. Different from LSSS, the proposed SMSS can securely share a matrix instead of a single value. The SMSS has advantages in both flexibility and efficiency. An SMSS-based SIS named LM-SIS is also proposed to achieve flexible image sharing. In the LM-SIS, an SMSS generating matrix is generated by a monotonous access policy, which is more flexible than the traditional threshold policy. Then shadows are generated by the SMSS generating matrix and the secret image matrix. Significantly, the generation process is very efficient, because it only invokes some linear transformations. During the recovery procedure, like LSSS, only the authorized participant sets can recover the secret image. Furthermore, the recovered images of LM-SIS are lossless or approximately lossless, which implies that the proposed scheme can support the secure sharing of high-quality images. In brief, the contributions can be summarized as follows:

1. We propose an SMSS, which can share a secret matrix with monotonous access policies. In detail, SMSS is an improved version of traditional LSSS.
2. We propose an SIS scheme based on the SMSS, which shares a secret image as a matrix with monotonous access policies.
3. Sufficient experimental results are given to evaluate the performance of our SIS scheme, and the results imply that our scheme is flexible, efficient and lossless.

The rest of the paper is organized as follows. Section 2 introduces the related work of the SIS scheme. Section 3 introduces the background of the proposed scheme like access policy and LSSS. The SMSS is proposed in Section 4. Section 5 proposes our LM-SIS scheme in detail. The experiments and analyses are shown in Section 6. Finally, conclusions and future work are drawn in Section 7.

2 Related Work

Secret Sharing Secret sharing [5] refers to a cryptographic method that securely shares secrets, which has a wide range of applications, such as secure multiparty computation [6], SIS [7–9], and electronic voting [10]. There are many ways to realize secret sharing. In addition to the polynomial-based technique, the Chinese Remainder Theorem (CRT) [11] and LSSS can also implement secret sharing. LSSS can be regarded as a general promotion of Shamir's secret sharing scheme [5] and its formal definition was first proposed by Beimel [12]. LSSS can describe any secret sharing scheme by a LSSS matrix as long as the scheme is linear. However, Beimel did not provide a method to implement an access policy through LSSS. Thus, Lewko and Waters [4] proposed a scheme to convert any monotonous Boolean Formulas to the LSSS matrices. However, when the algorithm is applied to the Access Tree, a large LSSS matrix will be generated. To address this problem, Liu et al. [13] proposed a new algorithm, which can directly support threshold gates and obtain a smaller LSSS matrix. Nevertheless, the scalability is still ignored. Therefore, Wang et al. [14] proposed a block LSSS with strong scalability. When the access policy is updated, the LSSS matrix only needs to be partially modified.

Secret Image Sharing SIS is an extension of secret sharing applied to images, so many methods in secret sharing can be introduced to SIS. Thien and Lin [15] embedded the secret image pixel value in the constant term of a $(k-1)$-degree polynomial over $\mathbb{Z}_{251}$ to achieve a (k, n) threshold SIS. Due to the truncation of pixel values, the recovered image will be distorted. To address this deficiency, Zhou et al. [16] regarded two adjacent pixels in the secret image as a secret value, and selected 65537 as the prime in the sharing polynomial to achieve lossless recovery. Meanwhile, the CRT-based SIS schemes have also been studied to achieve lossless recovery [1, 17]. Another weakness of [15] is that part of the secret can be revealed from $k-1$ shadows, which will compromise the threshold property. To this end, Zhou et al. [18] applied the pixel encryption method. Although the shadow size is increased, the security of SIS is improved.

Extended Secret Image Sharing All the schemes discussed above only implement a threshold access policy, in which each participant plays the same role. But in some cases, participants will be assigned different privileges based on their status. To meet this scenario, ESIS and WSIS have been proposed. Li et al. [19] firstly proposed a (t, s, k, n) ESIS, all n shadows are classified into s essential shadows and $n-s$ non-essential shadows. When recovering, k shadows included at least t essential shadows are required. However, in this scheme, the size of the essential shadows is not equal to the size of non-essential shadows, which may lead to security vulnerabilities. To solve this problem, Li et al. [20, 21] proposed ESIS schemes to generate shadows with the same size and reduce the shadow size to 1/k times of the secret image respectively. However, the concatenation operation of sub-shadows will increase computational complexity. Wu et al. [22] proposed an ESIS scheme using derivative polynomials to solve this defect. To

increase the flexibility of the scheme, Hu et al. [2] proposed a scalable (t, s, k, n) ESIS based on the Lagrange interpolation. Even if there is no essential shadow, k non-essential shadows can obtain the outline of the secret image. In a WSIS scheme, all shadows are assigned different weights and the secret image can be recovered iff the total weight of the collected shadows reaches the threshold. Tan et al. [23] proposed a WSIS based on the CRT which has progressive characteristics. That is, as the number of collected shadows increases, the quality of the recovered image also improves. Additionally, WSIS schemes based on other techniques have also been proposed, such as polynomial-based WSIS [3], and random grid-based WSIS [24].

However, even the access policies supported by WSIS and ESIS are relatively limited. In this paper, we propose a flexible and compact SIS scheme. Compared with the existing schemes, our scheme has the advantage of supporting monotonous access policies. Meanwhile, the quality of the recovered image is also high, so our scheme can be used for secret sharing of high-quality images.

3 Preliminaries

3.1 Access Policy

Access policy is also known as access structure, which is a core notion of secret sharing scheme. The formal definition of access policy is given as follows.

Definition 1 (Access Policy [13]). *Let $\mathcal{P} = \{P_0, P_1, ..., P_{N-1}\}$ be a set of participants. $\forall \mathbb{A} \subset 2^{\{P_0, P_1, ..., P_{N-1}\}}$ can be called an access policy of P. Furthermore, the access policy $\mathbb{A}$ is monotone if:*

$$\forall\ B, C \subset P : B \in \mathbb{A} \wedge B \subset C \rightarrow C \in \mathbb{A}.$$

Additionally, $\forall A \in \mathbb{A}$ is the authorized set of the access policy, otherwise, A is the unauthorized set. Furthermore, access policy can be presented in different forms, such as Access Tree, and Boolean Formula. For example, Fig. 1 shows an Access Tree, where non-leaf nodes represent threshold gates [14], and leaf nodes represent participants. Suppose the secret is denoted as $\mathbf{S}$ and the shadow set is

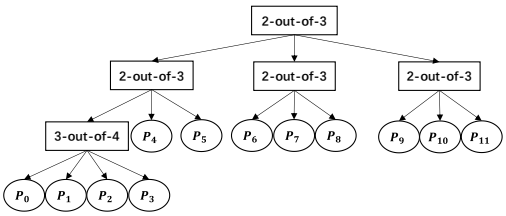


Fig. 1. Access tree

denoted as $\bar{\mathbf{S}}$. Each $P_i \in \mathcal{P}$ gets a $\bar{\mathbf{S}}_i \in \bar{\mathbf{S}}$. The $\mathbf{S}$ can be outputted iff the recovery set $\mathbf{S}^{'}$ is authorized. The existing SIS schemes cannot support the Access Tree, so this paper proposes an SIS scheme which can support monotonous access policies.

3.2 Linear Secret Sharing Schemes (LSSS)

As a commonly used form of access policy, LSSS is defined as follows:

Definition 2 (Linear Secret Sharing Schemes (LSSS) [13]). *Let Π be a secret sharing scheme over a set of participants $\mathcal{P}$, Π is linear (over $\mathbb{Z}_p$), if:*

1. *The shadows for each participant are presented as a vector over $\mathbb{Z}_p$.*
2. *There is a generating matrix $\mathbf{M}$, in which each row vector $\mathbf{M}_i$ corresponds to a participant $P_i \in \mathcal{P}$. Furthermore, there is a vector $\boldsymbol{v} = (s, r_1, ..., r_{d-1})^T$, where $s \in \mathbb{Z}_p$ is the secret, $r_1, ..., r_{d-1} \in \mathbb{Z}_p$ are random numbers and d denotes the column number of $\mathbf{M}$. Finally, the shadow of P_i is calculated as $\lambda_i = (\mathbf{M}\boldsymbol{v})_i$.*

Suppose Π is a LSSS of access policy $\mathbb{A}$, S be an authorized set and $I = \{i : P_i \in S\}$. We can find a set of constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ in polynomial time such that $\sum_{i \in I} \omega_i \mathbf{M}_i = (1, 0, ..., 0)$. Furthermore, we can get $\sum_{i \in I} \omega_i \lambda_i = s$.

3.3 Image Quality Evaluation Indicator

The Peak to Signal Noise Ratio(PSNR) [25] and Structural Similarity(SSIM) [26] are two common indicators to measure the distortion of images. Let x and y be the original image and the recovered image, respectively. The first indicator PSNR is calculated as follows:

$$PSNR = 20 \cdot log_{10}(\frac{MAX_I}{\sqrt{MSE}}), \tag{1}$$

where MAX_I represents the maximum value of the image pixels, MSE is the mean square error of images x and y. The higher $PSNR$ implies y is more similar to x. The second indicator SSIM is given as the following equation:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{2}$$

where μ_x is the average of x, μ_y is the average of y, σ_x is the variance of x, σ_y is the variance of y, σ_{xy} is the covariance of x and y, c_1 and c_2 are constants, $SSIM \in [-1, 1]$. The higher $SSIM$ implies the higher similarity between x and y.

4 Secret Matrix Sharing Scheme

SMSS can be viewed as an extended version of LSSS, which is used to share a secret matrix instead of a single secret value.

Definition 3 (Secret Matrix Sharing Scheme (SMSS)). *Let Π be a secret sharing scheme over a set of participants $\mathcal{P}$, Π is called SMSS (over $\mathbb{Z}_p$), if:*

1. *The shadows for each participant are represented by a vector $S_i \in \mathbb{Z}_p^{1 \times t}$.*

2. *There is a matrix* $\mathbf{M}$ *called the share-generating matrix with the access policy* $\mathbb{T}$*, and each row vector* $\mathbf{M}_i$ *corresponds to a participant* $P_i \in \mathcal{P}$*. Let matrix* $\bar{\mathbf{S}} = [\mathbf{S}, \mathbf{R}]^T$*, where* $\mathbf{S} \in \mathbb{Z}_p^{t\times t}$ *denotes the secret matrix and* $\mathbf{R} \in \mathbb{Z}_p^{t\times(n-t)}$ *denotes a non-zero random matrix.* $\hat{\mathbf{S}} = \mathbf{M}\bar{\mathbf{S}}$ *is calculated as shadow matrix, and each row vector* $\hat{\mathbf{S}}_i = \mathbf{M}_i\bar{\mathbf{S}}$ *denotes the shadow of* P_i*.*

Similar to LSSS, SMSS gets linear reconstruction property. Suppose Π is an SMSS of access policy $\mathbb{T}$, which is presented as generating matrix $\mathbf{M}$. Suppose S be a subset of $\mathcal{P}$ according with sub generating matrix $\mathbf{M}^{'}$ and shadow matrix $\mathbf{S}^{'}$, where $\mathbf{M}^{'}$ is composed of the row vector $\mathbf{M}_i, P_i \in S$ and $\mathbf{S}'$ is composed of according shadows $\hat{\mathbf{S}}_i, P_i \in S$. Iff S is an authorized set of $\mathbb{T}$, it can find matrix $\tilde{\mathbf{M}}$ in polynomial time to satisfy $\tilde{\mathbf{M}}\mathbf{M}^{'} = [\mathbf{I}_t, \mathbf{O}]$, where $\mathbf{I}_t$ denotes an identity matrix with order t and $\mathbf{O}$ denotes a zero matrix. Thus, we can get the secret matrix as $\mathbf{S}^* = \tilde{\mathbf{M}}\mathbf{S}^{'} = \mathbf{S}$. Two or more LSSS policies can be combined into one by the theorem proposed in [27]. Additionally, we introduce the theorem into SMSS to get a generating matrix with monotonous access policies.

Theorem 1. *Let* $\mathbb{T}_1$ *and* $\mathbb{T}_2$ *be the monotone access policies defined on the set of participants* $\mathcal{P}_1$ *and* $\mathcal{P}_2$ *respectively, and let* $P_z \in \mathcal{P}_1$*. Additionally,* $\mathbb{T}_1$ *and* $\mathbb{T}_2$ *are described by matrices* $\mathbf{M}$ *and* $\bar{\mathbf{M}}$ *respectively, where* $\mathbf{M} = (m_{i,j})_{n\times k}$ *and* $\bar{\mathbf{M}} = (\bar{m}_{i,j})_{x\times y}$*. The combined policy* $\mathbb{T}_1(P_z \to \mathbb{T}_2)$ *denotes the insertion of* $\mathbb{T}_2$ *at participant* P_z *in* $\mathbb{T}_1$*, which can be described by the following matrix:*

$$\mathbf{M}_{\mathbb{T}_1(P_z\to\mathbb{T}_2)} = \begin{bmatrix} m_{0,0} & \cdots & m_{0,k-1} & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & 0 & 0 & 0 \\ m_{z,0}\bar{m}_{0,0} & \cdots & m_{z,k-1}\bar{m}_{0,0} & \bar{m}_{0,1} & \cdots & \bar{m}_{0,y-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{z,0}\bar{m}_{x-1,0} & \cdots & m_{z,k-1}\bar{m}_{x-1,0} & \bar{m}_{x-1,1} & \cdots & \bar{m}_{x-1,y-1} \\ \vdots & \ddots & \vdots & 0 & 0 & 0 \\ m_{n-1,0} & \cdots & m_{n-1,k-1} & 0 & 0 & 0 \end{bmatrix}. \quad (3)$$

In reference [13], Liu et al. proposed a method to generate a Vandermonde matrix based LSSS matrix by Theorem 1. However, Cauchy matrix not only gets the same linear property as Vandermonde matrix, but also has advantages in efficiency. It implies that the time complexity of Cauchy matrix solving is only $O(n^2)$ while the time complexity of Vandermonde matrix is $O(n^3)$ [28]. Thus, we adopt the Cauchy matrix based SMSS to describe the access policy of SIS in this work. The definition of Cauchy matrix is given as follows.

Definition 4 (Cauchy matrix over $\mathbb{Z}_p$). *Let* $X = \{x_0, ..., x_{m-1}\}$ *and* $Y = \{y_0, ..., y_{n-1}\}$ *are two disjoint sets of elements over* $\mathbb{Z}_p$*, where* p *is a prime number. Cauchy matrix* $\mathbf{C} = (c_{i,j})_{m\times n}$*, where* $c_{i,j} = 1/(x_i + y_j)$ *and* $x_i + y_j \not\equiv 0 \ mod\ p$ $(0 \le i \le m-1,\ 0 \le j \le n-1)$.

In brief, a (k, n) threshold of SMSS can be described by a Cauchy matrix $\mathbf{C}_{n\times k}$. To improve computational efficiency, we provide a function *Divide*() to process the Cauchy matrix. Given a Cauchy matrix $\mathbf{C} = (c_{i,j})_{m\times n}$. The function

$Divide(\mathbf{C}) = (c_{i,j})_{m\times(n-1)}$, where $c_{i,j} = (x_i+y_0)/(x_i+y_{j+1})$ $(0 \le i \le m-1,\ 0 \le j \le n-2)$.

Following [13], we propose Algorithm 1 as the SMSS generating matrix generation algorithm. Let $\mathbb{T}$ be an access policy, which is presented as an access tree. Algorithm 1 takes the access policy $\mathbb{T}$ as input, performs the depth-first traversal of $\mathbb{T}$ to get threshold sequence $TG(\mathbb{T}) = \{TG_0, ..., TG_{m-1}\}$ and generates a Cauchy matrix $\mathbf{C}_i$ $(0 \le i \le m-1)$ for each gate. Then, such Cauchy matrices are combined by Theorem 1 to describe the policy $\mathbb{T}$. Finally, the SMSS generating matrix $\mathbf{M}$ is outputted.

Algorithm 1 SMSSMatrix($\mathbb{T}$)

Input: Access policy $\mathbb{T}$
Output: The SMSS generating matrix $\mathbf{M}$

1: Perform the depth-first traversal of $\mathbb{T}$ to get $TG(\mathbb{T}) = \{TG_0, ..., TG_{m-1}\}$ and denote each TG_i as policy $\mathbb{T}_i$
2: Generate the Cauchy matrix $\mathbf{C}_i$ for each threshold-gate TG_i
3: $\mathbf{M} \leftarrow \mathbf{C}_0$
4: **for** i from 1 to $m-1$ **do**
5: $\quad \mathbf{C}_i \leftarrow Divide(\mathbf{C}_i)$
6: $\quad$ Get the row index k of TG_i
7: $\quad \mathbf{M} \leftarrow \mathbf{M}_{\mathbb{T}_{i-1}(P_k \to \mathbb{T}_i)}$
8: $\quad$ Update the row index of nodes $TG_i \in TG(\mathbb{T})$
9: **end for**
10: **return** $\mathbf{M}$

It is important that the flexibility of SMSS is stronger than the access policies of other SIS schemes. For example, Fig. 2 shows a complex access tree which can be easily described by an SMSS. However, traditional ESIS and WSIS schemes can not support such complex access policies.

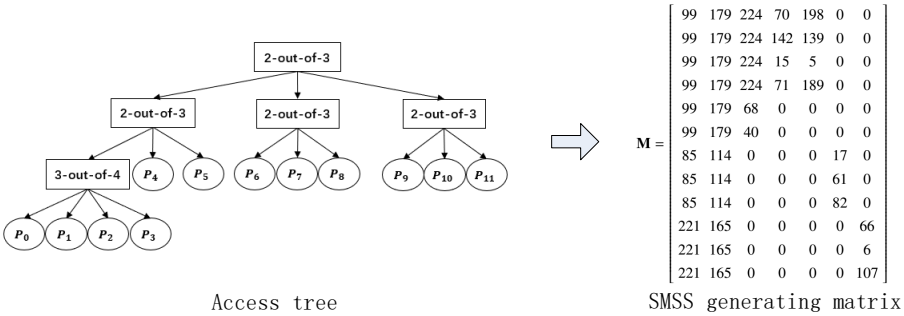


Fig. 2. Access policy to SMSS generating matrix

Furthermore, the security and correctness of SMSS are intuitive, since it is an All-or-Nothing Transformation (AONT) [29] scheme. AONT means that authorized set can get all (i.e. the original secret matrix can be reconstruct correctly), and unauthorized set can get nothing (i.e. the original secret matrix cannot be reconstruct correctly). "All" corresponds to the correctness of the scheme, and "Nothing" corresponds to the security of the scheme.

Theorem 2. *The SMSS is an AONT scheme.*

Proof. The theorem can be easily proved according to the theories of monotone span programs [27] and LSSS [13]. □

5 Linear Matrix based Secret Image Sharing Scheme

Based on the SMSS, we propose the Linear Matrix based Secret Image Sharing (LM-SIS) scheme which supports arbitrary monotonous access policies. The LM-SIS scheme includes three procedures: secret image preprocessing, shadow generation and recovery.

5.1 Secret Image Preprocessing

Considering the property of digital images that each pixel can be viewed as an element of $GF(2^8)$, the computation of LM-SIS is performed in $\mathbb{Z}_p$, where p is a prime number close to 256 (i.e. 2^8). The LM-SIS can be divided into two cases: 251-LM-SIS and 257-LM-SIS, that is, the prime number is picked as 251 or 257. The LM-SIS secret image preprocessing procedure is shown in Fig. 3.

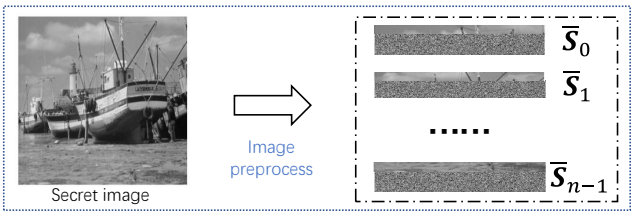


Fig. 3. Secret image preprocess

Algorithm 2 Preprocess the secret image matrix

Input: Secret image matrix $\mathbf{S}_{M\times L}$; Parameter k and T; Prime number p
Output: The set of secret matrices $\bar{\mathbf{S}} = \{\bar{\mathbf{S}}_j | \ 0 \le j \le n-1\}$

1: **if** $p \le 256$ **then**
2: Truncate all pixel value larger than $p-1$ to $p-1$
3: **end if**
4: Divide each k rows of the $\mathbf{S}$ into a unit, obtained $\bar{\mathbf{S}} = \{\bar{\mathbf{S}}_j | \ 0 \le j \le n-1\}$
5: **for** each $\bar{\mathbf{S}}_j$ **do**
6: Generate a non-zero random matrix $\mathbf{R}^*_{L\times(T-k)}$
7: $\bar{\mathbf{S}}_j \leftarrow (\bar{\mathbf{S}}_j^T, \ \mathbf{R}^*)^T$
8: **end for**
9: **return** $\bar{\mathbf{S}}$

We propose Algorithm 2 to transform image $\mathbf{S}$ into secret matrix set $\bar{\mathbf{S}}$. Suppose the size of the secret image is $M \times L$. Algorithm 2 first maps all pixels of $\mathbf{S}$ into $\mathbb{Z}_p$, where p is a prime number. Then the matrix over $\mathbb{Z}_p$ is divided

into a set of secret matrices. $\bar{\mathbf{S}} = \{\bar{\mathbf{S}}_j | \ 0 \leq j \leq n-1\}$, where the size of each $\bar{\mathbf{S}}_j \in \bar{\mathbf{S}}$ is $T \times L$, $n = \lceil M/k \rceil$, k denotes the root threshold of access policy and T denotes the column number of the SMSS generating matrix $\mathbf{M}$.

5.2 Shadow Generation

Fig. 4 shows the shadow generation procedure of LM-SIS. The shadow generation requires two matrices: the SMSS generating matrix $\mathbf{M}$ and the random full rank matrix $\mathbf{R}$. We call Algorithm 1 to generate matrix $\mathbf{M}$ with access policy $\mathbb{T}$. The matrix $\mathbf{R}$ is composed of two non-zero blocks $\mathbf{R}^{'}$ and $\mathbf{R}^{*}$. Furthermore, $\mathbf{R}^{'}$ is a $k \times k$ matrix and $\mathbf{R}^{*}$ is a $(T-k) \times (T-k)$ matrix, where k denotes the root threshold of $\mathbb{T}$ and T denotes the column number of the SMSS generating matrix. For simplicity, it can take the identity matrix $\mathbf{I}_{(T-k)}$ as $\mathbf{R}^{*}$.

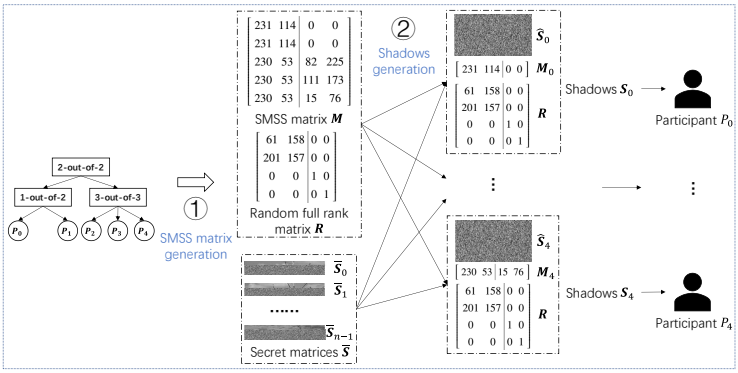


Fig. 4. Shadow generation

Algorithm 3 Generate the shadow matrices

Input: Access policy $\mathbb{T}$; Random matrix $\mathbf{R}$; The set of secret matrices $\bar{\mathbf{S}}$
Output: The set of shadow matrices $\hat{\mathbf{S}} = \{\hat{\mathbf{S}}_i | \ 0 \leq i \leq N-1\}$

$\mathbf{M}$ = SMSSMatrix($\mathbb{T}$) // Call Algorithm 1
for each $\mathbf{M}_i$ **do**
  $\mathbf{M}_i^{(0)} \leftarrow \mathbf{M}_i$
  $\hat{\mathbf{S}}_{i,0} \leftarrow \mathbf{M}_i^{(0)} \bar{\mathbf{S}}_0 \ mod \ p$
  for j from 1 to $n-1$ **do**
    $\mathbf{M}_i^{(j)} \leftarrow \mathbf{M}_i^{(j-1)} \mathbf{R} \ mod \ p$
    $\hat{\mathbf{S}}_{i,j} \leftarrow \mathbf{M}_i^{(j)} \bar{\mathbf{S}}_j \ mod \ p$
  end for
  $\hat{\mathbf{S}}_i \leftarrow (\hat{\mathbf{S}}_{i,0}, ..., \hat{\mathbf{S}}_{i,n-1})^T$
  if $p > 256$ **then**
    Each value in $\hat{\mathbf{S}}_i$ is represented by 9 or more bits, and every 8 bits of $\hat{\mathbf{S}}_i$ is saved as a pixel of shadow images $\hat{\mathbf{S}}$
  end if
end for
return $\hat{\mathbf{S}}$

Algorithm 3 shows the shadow generation algorithm. Each shadow matrix $\hat{\mathbf{S}}_i$ is composed of a set of shadow vectors $\hat{\mathbf{S}}_{i,j}$ $(0 \leq j \leq n-1)$. The computation of the shadow vector $\hat{\mathbf{S}}_{i,j}$ is similar to the Output Feedback (OFB) mode [30] which is usually used in block ciphers. As shown in Fig. 5, the core idea of OFB mode is getting each shadow vector $\hat{\mathbf{S}}_{i,j}$ by the vector $\mathbf{M}_i^{(j)}$, where $\mathbf{M}_i^{(j)}$ is generated by the row $\mathbf{M}_i$ of matrix $\mathbf{M}$ and the matrix $\mathbf{R}$. Finally, the matrix $\hat{\mathbf{S}}_i$, row vector $\mathbf{M}_i$ and the random matrix $\mathbf{R}$ are sent to participant P_i as the shadow.

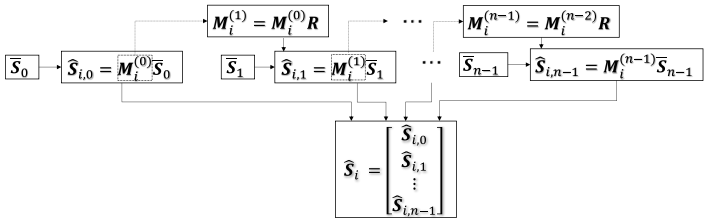


Fig. 5. Shadow generation of LM-SIS

5.3 Recovery

The recovery procedure of LM-SIS is shown in Fig. 6. Assume that $I^{'}$ is an

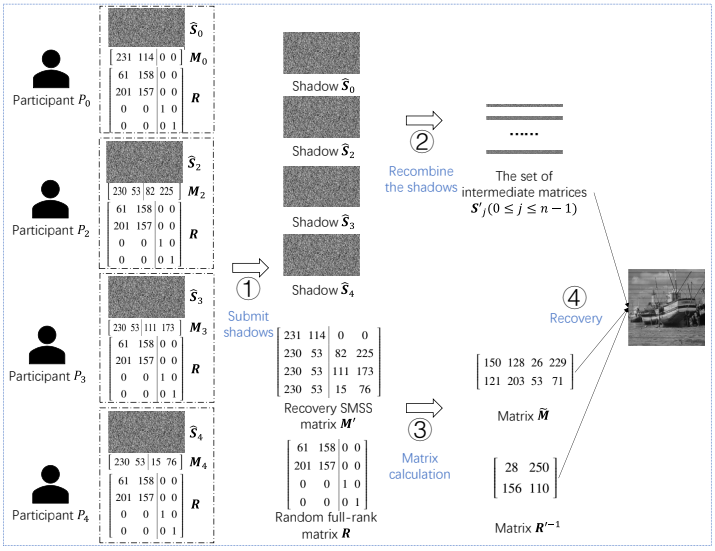


Fig. 6. Recovery

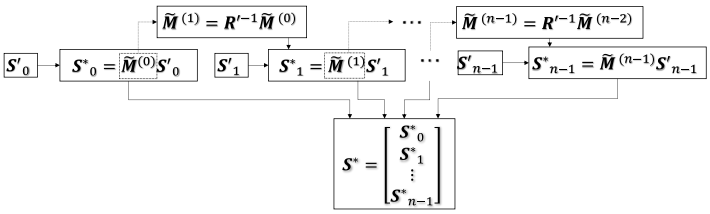


Fig. 7. Image recovery of LM-SIS

authorized set of access policy $\mathbb{T}$ and the number of participants in the authorized set $|I^{'}| = N^{'}$. The secret image $\mathbf{S}$ can be recovered after all participants $P_i \in I^{'}$ submit their shadows. Then, it gets the intermediate matrices $\mathbf{S}_j^{'} = [\hat{\mathbf{S}}_{0,j}, ..., \hat{\mathbf{S}}_{N'-1,j}](0 \leq j \leq n-1)$, where $\hat{\mathbf{S}}_{i'} = [\hat{\mathbf{S}}_{i',0}, ..., \hat{\mathbf{S}}_{i',n-1}]$ denotes the shadow of P_i and $i' \in I'$. The recovery SMSS matrix $\mathbf{M}^{'}$ is composed of the row vector $\mathbf{M}_{i'}$, $i^{'} \in I^{'}$. Following the definition of SMSS, it can find a matrix $\tilde{\mathbf{M}}$ such that $\tilde{\mathbf{M}}\mathbf{M}^{'} = [\mathbf{I}_t,\ \mathbf{O}]$. Furthermore, we calculate the inverse matrix $\mathbf{R}^{'-1}$ of the sub-matrix $\mathbf{R}^{'}$ of the random matrix $\mathbf{R}$. Algorithm 4 takes $\mathbf{R}^{'-1}$, $\tilde{\mathbf{M}}$, $\mathbf{S}^{'}$ as input and outputs the recovered image $\mathbf{S}^*$, where $\mathbf{S}^* = [\mathbf{S}_0^*, ..., \mathbf{S}_{n-1}^*]^T$. The $\mathbf{S}^*$ is combined by the components $\mathbf{S}_j^*$ $(0 \leq j \leq n-1\})$, and the calculation of secret image recovery is shown in Fig. 7.

Algorithm 4 Recovery

Input: Inverse matrix $\mathbf{R}^{'-1}$; Matrix $\tilde{\mathbf{M}}$; The set of intermediate matrices $\mathbf{S}^{'} = \{\mathbf{S}_j^{'}| 0 \leq j \leq n-1\}$

Output: Recovered image matrix $\mathbf{S}^*$

1: **if** $p > 256$ **then**
2: $\quad$ $\mathbf{S}^{'}$ is represented by a set of 8-bit pixel, and every 9 bits is saved as a pixel
3: **end if**
4: $\tilde{\mathbf{M}}^{(0)} = \tilde{\mathbf{M}}$
5: $\mathbf{S}_0^* = \tilde{\mathbf{M}}^{(0)}\mathbf{S}_0^{'}\ mod\ p$
6: **for** j from 1 to $n-1$ **do**
7: $\quad$ $\tilde{\mathbf{M}}^{(j)} = \mathbf{R}^{'-1}\ \tilde{\mathbf{M}}^{(j-1)}\ mod\ p$
8: $\quad$ $\mathbf{S}_j^* = \tilde{\mathbf{M}}^{(j)}\mathbf{S}_j^{'}\ mod\ p$
9: **end for**
10: $\mathbf{S}^* = (\mathbf{S}_0^*, ..., \mathbf{S}_{n-1}^*)^T$
11: **return** $\mathbf{S}^*$

Note that the proposed LM-SIS can be used to share both grayscale and color images. For color images, it can share the three components of RGB through the proposed scheme respectively, and finally merge the three components to realize the sharing of color secret images.

6 Performance Analysis and Evaluation

The comparison between the proposed LM-SIS scheme and other SIS schemes is shown in Table 1. Significantly, LM-SIS is divided into 251-LM-SIS and 257-

Table 1. Comparison of the proposed scheme with others

	Yan et al.'s [9]	Wu et al.'s [22]	Tan et al.'s [23]	our LM-SIS scheme	
				$p = 251$	$p = 257$
Method	Random grid	Derivative polynomial	Chinese remainder theorem	SMSS	
Shadow size ratio	1	$1/k$	1	$1/k$	$9/8k$
Access structure	(k, n)	(t, s, k, n)	Weighted (k, n)	Monotonous access policy	
Recovery quality	Lossy	Lossless	Lossless	Approximate lossless	Lossless

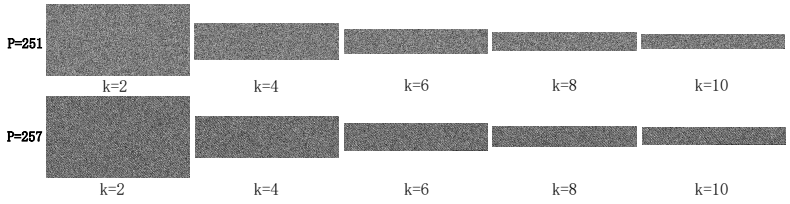
LM-SIS. In the first case, p is picked as 251, the LM-SIS brings slight quality loss of recovered images while it gets the more compact shadow size. In the other case (i.e. $p = 257$), each value of the LM-SIS matrix should be performed as a 9-bit unit instead of an 8-bit unit. It implies that the LM-SIS scheme over $\mathbb{Z}_{257}$ can keep the secret image quality but also brings some storage redundancy. Compared with other schemes, the advantage of our scheme is the flexibility of the access policy. As shown in Table 1, lots of methods are proposed to construct SIS schemes, such as random grid [9], derivative polynomial [22] and Chinese remainder theorem [23]. However, these schemes only support limited access policies. For example, Yan et al. [9] implemented a tranditional (k, n)-SIS, Wu et al. [22] implemented an ESIS and Tan et al. [23] proposed a WSIS. Our LM-SIS is more flexible than others, because SMSS provides a monotonous access policy. Meanwhile, LM-SIS also has advantages in storage costs and recovered quality. On the one hand, it gets smaller shadow size than most SIS schemes. On the other hand, it can provide lossless or approximate lossless recovered images.

We first take the images in Fig. 8 as examples to evaluate the performance of LM-SIS. The simulation runs on the PYCHARM [1] platform, and the computer used in the experiments is Intel(R) Core(TM) i5-9300H CPU 2.40GHz, RAM 8.00 GB. As shown in Fig. 8, there are two grayscale images and two color images with size 512×512.

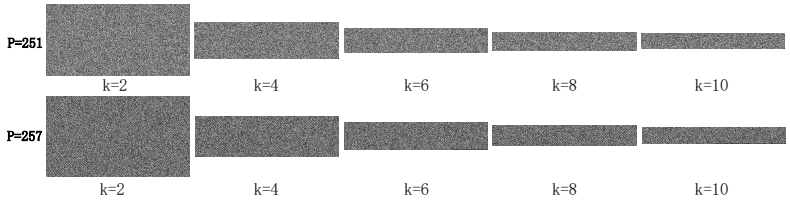
(a) Boat (b) Bridge (c) Baboon (d) Lena

Fig. 8. The secret images

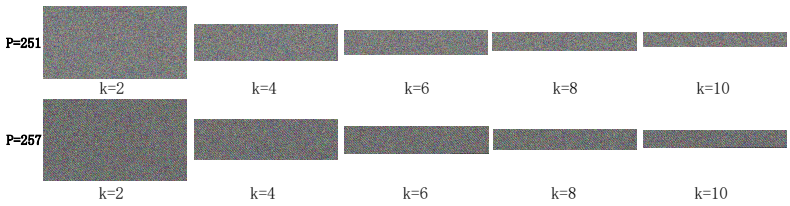
[1] PyCharm is a Python Integrated Development Environment



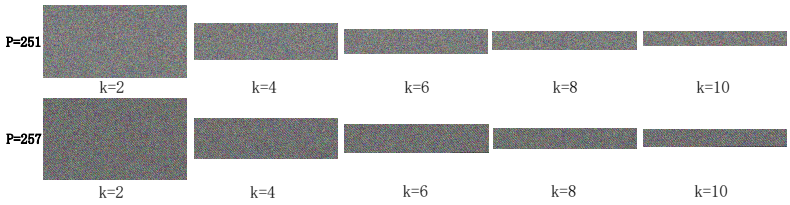
(a) Boat



(b) Bridge



(c) Baboon

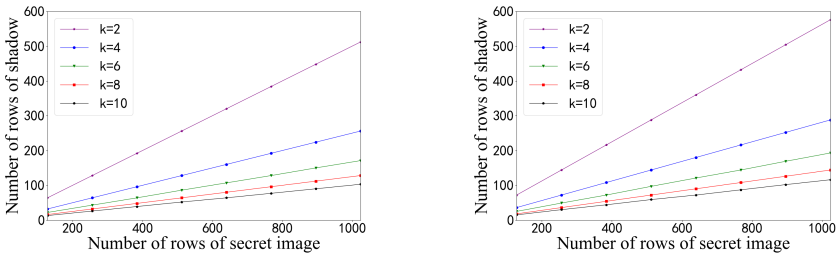


(d) Lena

Fig. 9. The shadows

Fig. 9 shows the shadows of different images generated by LM-SIS. Although the secret images are different, the shadows they generate are meaningless. It implies that our scheme reduces the probability of information leakage when the shadow is obtained by attackers. Meanwhile, it can also be seen from Fig. 9, the shadow size of LM-SIS is related to the parameter k, where k denotes the root threshold of access policy. It is clear that the size ratio of the shadow is approximately $1/k$ or $9/8k$ while the prime number is p equal to 251 or 257. This is because in the shadow generation procedure, one row of the shadow is generated by k rows of secret image. The shadow size in [9] and [23] is equal to secret iamge and the shadow size in [22] is $1/k$ of the secret image, which proves the advantages of our scheme in storage. Furthermore, Fig. 10 presents

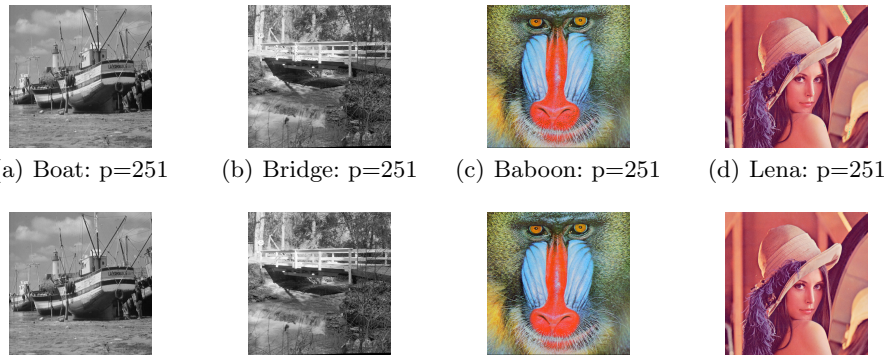
the influence of k on the shadow size. It can be seen that the number of rows of the shadow increases linearly with the number of rows of the secret image and the slope is equal to the size ratio of the shadow.



(a) $p = 251$ (b) $p = 257$

Fig. 10. The size of the shadows

To evaluate the recovered image quality, Fig. 11 shows the recovered images in various cases, the first line are the recovered images over $\mathbb{Z}_{251}$, and the second

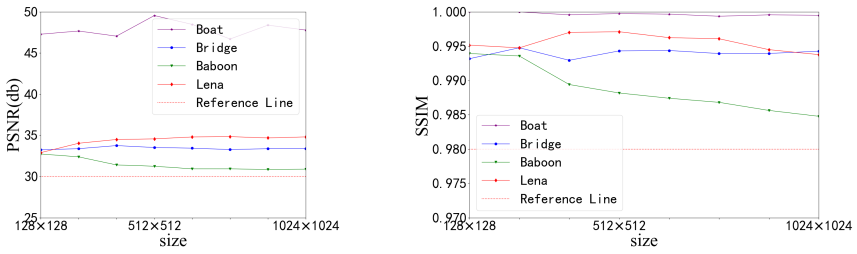


(a) Boat: p=251 (b) Bridge: p=251 (c) Baboon: p=251 (d) Lena: p=251

(e) Boat: p=257 (f) Bridge: p=257 (g) Baboon: p=257 (h) Lena: p=257

Fig. 11. The recovered images

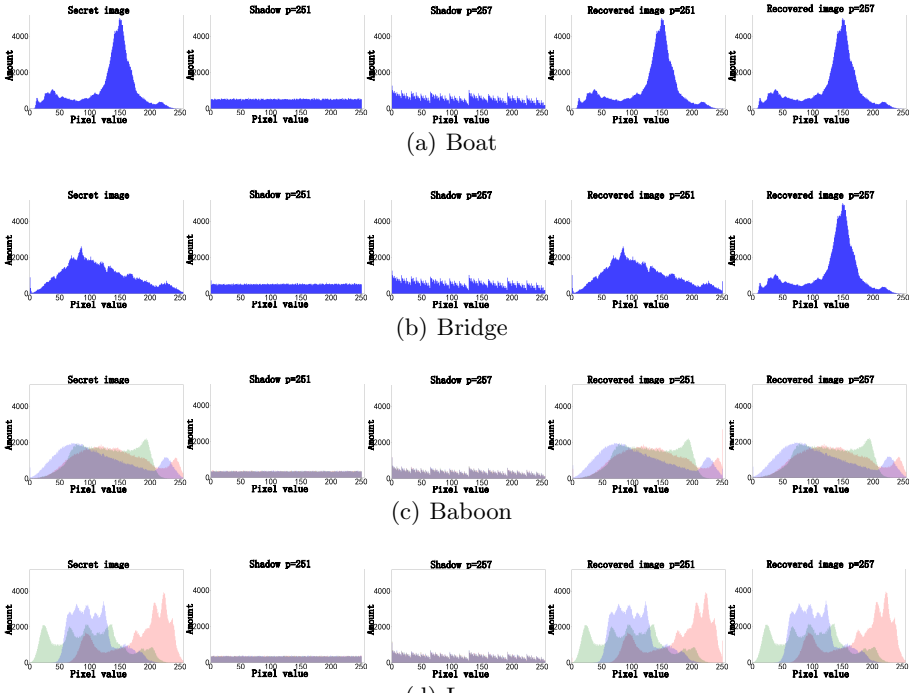
line are the recovered images over $\mathbb{Z}_{257}$. It can be seen that the recovered images over $\mathbb{Z}_{251}$ are approximately lossless, because only a few pixels larger than 250 are truncated. Meanwhile, the recovered images over $\mathbb{Z}_{257}$ are lossless. In the 251-LM-SIS and 257-LM-SIS schemes, the difference between the recovered images of different schemes is always negligible. In brief, the recovered image loss of 251-LM-SIS is too slight to be perceived visually. Furthermore, for the case $p = 251$, the PSNR and SSIM of such recovered images are given in Fig. 12. Generally speaking, PSNR of 30-40dB or SSIM over 0.98 indicates that the image quality



(a) PSNR (b) SSIM

Fig. 12. The PSNR and SSIM of the recovered images

is good. It can be seen that the PSNR and SSIM of our recovered images are always exceed the reference line(i.e. good visual effect), the PSNR is always greater than 30dB and the SSIM usually exceeds 0.99. In general, our LM-SIS scheme has high and stable recovered image quality.



(a) Boat

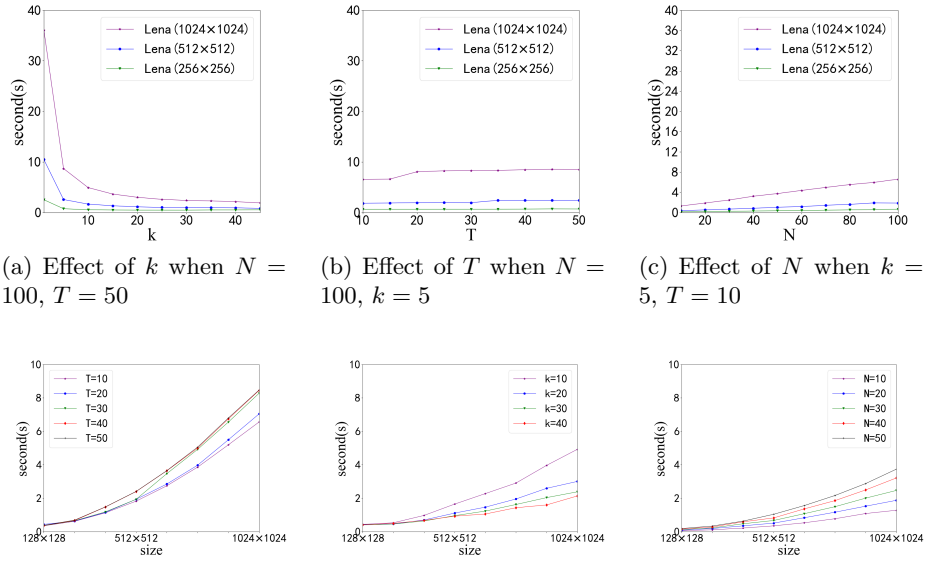
(b) Bridge

(c) Baboon

(d) Lena

Fig. 13. The histogram

For presenting the pixel probability distribution of the images, Fig. 13 shows the histogram of the original image, 251-LM-SIS shadow, 257-LM-SIS shadow, 251-LM-SIS recovered image and 257-LM-SIS recovered image, respectively. Furthermore, for color images, Fig. 13(c) and Fig. 13(d) present R, G, B pixel distributions by red, green, and blue histogram respectively. In summary, in each case, the shadow histogram is uniform. It implies that the shadow can reveal nothing about the secret image information. In the third column, the histogram of 257-LM-SIS shadow is jagged. This is because we use nine bits to represent a pixel value and save every eight bits as a shadow pixel value. Meanwhile, the difference of histogram between the original image and 251-LM-SIS recovered image is negligible. Thus, the image quality loss of 251-LM-SIS is too slight to influence the visual effect.



(a) Effect of k when $N = 100$, $T = 50$

(b) Effect of T when $N = 100$, $k = 5$

(c) Effect of N when $k = 5$, $T = 10$

(d) Effect of size when $N = 100$, $k = 5$

(e) Effect of size when $N = 100$, $T = 50$

(f) Effect of size when $k = 5$, $T = 10$

Fig. 14. Shadow generation time

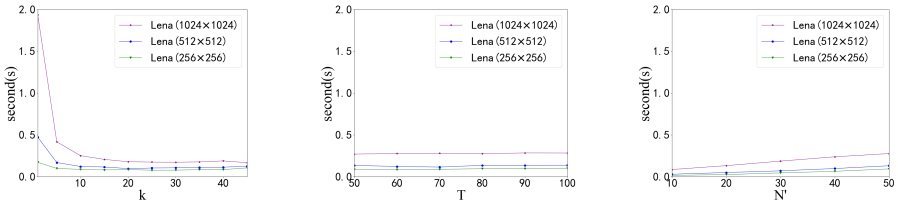
To evaluate the efficiency of the proposed LM-SIS, we simulate the scheme in various cases to get simulation relevant data. The simulation aims to evaluate the influence of the root threshold k, the SMSS generating matrix column number T, and the participant number N on LM-SIS runtime. The test cases of running time are grayscale image Lena, unless specified otherwise. For reliability, the simulation of each case is run 20 times and we take the average runtime as the result shown in Fig. 14. It shows the following conclusions:

1. The shadow generation time is decreasing as k increases.

2. The shadow generation time increases slightly, while T is increasing.
3. The shadow generation time approximately linearly increases with N.
4. The size of the secret image seriously affects shadow generation time. The larger-sized secret image will have a longer shadow generation time with the same size access policy.

A larger k brings a less number of secret matrix units, that is, a secret matrix with more rows can be processed in one operation, so the shadow generation time will be reduced. The increase of T will slightly increase the shadow generation time, this is because the random matrix $\mathbf{R}^*$ has $T-k$ rows, and the preprocessing time of the secret image will increase. N represents the number of participants and the generation time of each shadow is approximately the same, so N has a linear relationship with the shadow generation time. At the same time, the size of the secret image will also affect the shadow generation time. The larger the secret matrix corresponding to the secret image, the more calculations are required.

Additionally, the impact of parameters k, T, $N^{'}$ on recovery time is also shown in Fig. 15, where k denotes the root threshold of access policy, T denotes the column number of the SMSS matrix and N' denotes the number of shadows used for recovery. As shown in Fig. 15(a), the recovered time will decrease while k is increasing. Fig. 15(b) implies that the recovery time should slightly increase with T. At the same time, Fig. 15(c) shows that the recovering runtime linear increases with $N^{'}$. The change of recovery time with parameters is the same as the change of shadow generation time with parameters, we won't explain it in detail here.



(a) Effect of k when $N' = 50$, $T = 50$

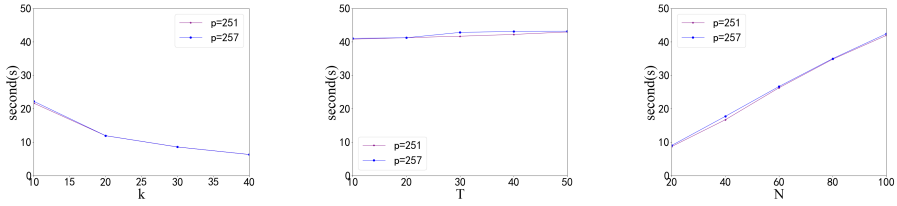
(b) Effect of T when $N' = 50$, $k = 10$

(c) Effect of N' when $k = 10$, $T = 50$

Fig. 15. Recovery time

Finally, Fig. 16 shows the shadow generation time in 251-LM-SIS and 257-LM-SIS affected by parameters k, T, N, where k denotes the root threshold of access policy, T denotes the column number of the SMSS generating matrix and N denotes the row number of SMSS generating matrix. We use the color image Lena as an example to simulate the scheme. The runtime decreases with k and increases with T and N. It can be seen that the shadow generation time is significantly longer than that in Fig. 14. This is because our LM-SIS scheme

needs to process the RGB three components of the color image respectively. Furthermore, we can see from Fig. 16 that the runtime difference between 251-LM-SIS and 257-LM-SIS is too slight to be detected. Because converting the eight-bit pixel value of the secret image to nine-bit does not cost a lot of computational overhead, the shadow generation time is mainly concentrated in matrix multiplication.



(a) Effect of k when $N = 100$, $T = 50$

(b) Effect of T when $N = 100$, $k = 2$

(c) Effect of N when $k = 5$, $T = 10$

Fig. 16. Shadow generation time of 251-LM-SIS and 257-LM-SIS

7 Conclusions and Future Work

In this paper, we extend the traditional LSSS into the secret matrix and propose an SMSS which is used to share a secret matrix. Furthermore, we present an SMSS based SIS scheme named LM-SIS. Compared with WSIS and ESIS, our scheme provides a more flexible access policy. Thus it can be implemented in more complex scenarios. Meanwhile, the proposed LM-SIS also has advantages in efficiency, storage cost and image quality. The superiority of our scheme can be summarized as follows. Firstly, SMSS can provide a monotonous access policy for LM-SIS and Cauchy matrix improves the efficiency of LM-SIS. Secondly, the shadow size of LM-SIS is smaller than most existing SIS schemes. Finally, both 251-LM-SIS and 257-LM-SIS support high image quality, since the recovered images of such LM-SIS schemes are lossless or approximately lossless. In conclusion, the proposed LM-SIS scheme is flexible, low-load and lossless of image quality. How to design an SIS scheme in which the shadows are meaningful images is our future work.

Acknowledgment

This work was supported by the National Science Foundation of China (No. 61802083, 61862011), the Natural Science Foundation of Guangxi (2018GXNSFB A281164, 2018GXNSFAA138116).

References

1. Longlong Li, Yuliang Lu, Xuehu Yan, Lintao Liu, and Longdan Tan. Lossless (k, n) -threshold image secret sharing based on the chinese remainder theorem without auxiliary encryption. *IEEE Access*, 7:75113–75121, 2019.
2. Yan-Xiang Hu and Yi-Ning Liu. A progressively essential secret image sharing scheme using hierarchy shadow. *J. Inf. Secur. Appl.*, 47:371–376, 2019.
3. Yongjie Wang, Jia Chen, Qinghong Gong, Xuehu Yan, and Yuyuan Sun. Weighted polynomial-based secret image sharing scheme with lossless recovery. *Secur. Commun. Networks*, 2021:1–11, 2021.
4. Allison B. Lewko and Brent Waters. Decentralizing attribute-based encryption. *IACR Cryptol. ePrint Arch.*, 2010:351, 2010.
5. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
6. Marcel von Maltitz and Georg Carle. A performance and resource consumption assessment of secret sharing based secure multiparty computation. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, volume 11025, pages 357–372, 2018.
7. Ching-Nung Yang and Yi-Yun Yang. On the analysis and design of visual cryptography with error correcting capability. *IEEE Trans. Circuits Syst. Video Technol.*, 31(6):2465–2479, 2021.
8. Xuehu Yan, Yuliang Lu, Ching-Nung Yang, Xinpeng Zhang, and Shudong Wang. A common method of share authentication in image secret sharing. *IEEE Trans. Circuits Syst. Video Technol.*, 31(7):2896–2908, 2021.
9. Xuehu Yan, Xin Liu, and Ching-Nung Yang. An enhanced threshold visual secret sharing based on random grids. *J. Real Time Image Process.*, 14(1):61–73, 2018.
10. Jing Li, Xianmin Wang, Zhengan Huang, Licheng Wang, and Yang Xiang. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *J. Parallel Distributed Comput.*, 130:91–97, 2019.
11. Xingxing Jia, Daoshun Wang, Daxin Nie, Xiangyang Luo, and Jonathan Zheng Sun. A new threshold changeable secret sharing scheme based on the chinese remainder theorem. *Inf. Sci.*, 473:13–30, 2019.
12. Beimel and Amos. Secure schemes for secret sharing and key distribution. *Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel*, 1996.
13. Zhen Liu, Zhenfu Cao, and Duncan S Wong. Efficient generation of linear secret sharing scheme matrices from threshold access trees. *IACR Cryptol. ePrint Arch.*, 2010:374, 2010.
14. Jing Wang, Chuanhe Huang, Neal N. Xiong, and Jinhai Wang. Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system. *Inf. Sci.*, 424:1–26, 2018.
15. Chih-Ching Thien and Ja-Chen Lin. Secret image sharing. *Comput. Graph.*, 26(5):765–770, 2002.
16. Xuan Zhou, Yuliang Lu, Xuehu Yan, Yongjie Wang, and Lintao Liu. Lossless and efficient polynomial-based secret image sharing with reduced shadow size. *Symmetry*, 10(7):249, 2018.
17. Xuehu Yan, Yuliang Lu, Lintao Liu, Song Wan, Wanmeng Ding, and Hanlin Liu. Chinese remainder theorem-based secret image sharing for (k, n) threshold. In *Third International Conference Cloud Computing and Security*, volume 10603, pages 433–440, 2017.
18. Zhili Zhou, Ching-Nung Yang, Yi Cao, and Xingming Sun. Secret image sharing based on encrypted pixels. *IEEE Access*, 6:15021–15025, 2018.

19. Peng Li, Ching-Nung Yang, Chih-Cheng Wu, Qian Kong, and Yanpeng Ma. Essential secret image sharing scheme with different importance of shadows. *J. Vis. Commun. Image Represent.*, 24(7):1106–1114, 2013.
20. Peng Li, Ching-Nung Yang, and Zhili Zhou. Essential secret image sharing scheme with the same size of shadows. *Digit. Signal Process.*, 50:51–60, 2016.
21. Peng Li and Zuquan Liu. An improved essential secret image sharing scheme with smaller shadow size. *Int. J. Digit. Crime Forensics*, 10(3):78–94, 2018.
22. Zhen Wu, Yi-Ning Liu, Dong Wang, and Ching-Nung Yang. An efficient essential secret image sharing scheme using derivative polynomial. *Symmetry*, 11(1):69, 2019.
23. Longdan Tan, Yuliang Lu, Xuehu Yan, Lintao Liu, and Longlong Li. Weighted secret image sharing for a (k, n) threshold based on the chinese remainder theorem. *IEEE Access*, 7:59278–59286, 2019.
24. Zuquan Liu, Guopu Zhu, Feng Ding, and Sam Kwong. Weighted visual secret sharing for general access structures based on random grids. *Signal Process. Image Commun.*, 92:116129, 2021.
25. M. Yadav and R. Singh. Essential secret image sharing approach with same size of meaningful shares. *Multimed. Tools. Appl.*, pages 1–18, 2021.
26. Sonal Kukreja, Geeta Kasana, and Singara Singh Kasana. Copyright protection scheme for color images using extended visual cryptography. *Comput. Electr. Eng.*, 91:106931, 2021.
27. Ventzislav Nikov and Svetla Nikova. New monotone span programs from old. *IACR Cryptol. ePrint Arch.*, 2004:282, 2004.
28. Zlatko Drmac, Igor Mezic, and Ryan Mohr. Data driven koopman spectral analysis in vandermonde-cauchy form via the DFT: numerical method and theoretical insights. *SIAM J. Sci. Comput.*, 41(5):A3118–A3151, 2019.
29. Navid Nasr Esfahani and Douglas R. Stinson. On security properties of all-or-nothing transforms. *IACR Cryptol. ePrint Arch.*, page 314, 2021.
30. Arthur Silitonga, Zhou Jiang, Nadir Khan, and Jürgen Becker. Reconfigurable module of multi-mode AES cryptographic algorithms for AP socs. In *IEEE Nordic Circuits and Systems Conference*, pages 1–7, 2019.