symmetry

MDPI

Article

An Image Secret Sharing Method Based on Matrix Theory

Wanmeng Ding, Kesheng Liu, Xuehu Yan *, Huaixi Wang, Lintao Liu and Qinghong Gong

National University of Defense Technology, Hefei 230037, China; wanmeng502@sina.com (W.D.); liukeshenggolf@163.com (K.L.); permutation@163.com (H.W.); liuta1989@163.com (L.L.); first_hong@126.com (Q.G.)

* Correspondence: publictiger@126.com; Tel.: +86-551-8640-2861

Received: 4 September 2018; Accepted: 19 October 2018; Published: 22 October 2018

Abstract: Most of today's secret image sharing technologies are based on the polynomial-based secret sharing scheme proposed by shamir. At present, researchers mostly focus on the development of properties such as small shadow size and lossless recovery, instead of the principle of Shamir's polynomial-based SS scheme. In this paper, matrix theory is used to analyze Shamir's polynomial-based scheme, and a general (k, n) threshold secret image sharing scheme based on matrix theory is proposed. The effectiveness of the proposed scheme is proved by theoretical and experimental results. Moreover, it has been proved that the Shamir's polynomial-based SS scheme is a special case of our proposed scheme.

Keywords: threshold construction; Shamir's polynomial-based scheme; secret image sharing; matrix theory; Vandermonde matrix

1. Introduction

Since more and more data are being transmitted via the Internet, how to protect the privacy and security of the data such as military images becomes a focus. Although secret data can be protected by traditional encryption, it cannot be revealed exactly if the stego-media is lossy. With a property of loss-tolerance, secret sharing(SS) techniques have been proposed. SS, also called secret division, was invented independently by Adi Shamir [1] and George Blakley [2] in 1979. A (k, n) threshold SS scheme is a method of encrypting a secret into n shares such that any subset consisting of k shares can reveal the secret, while less than k shares cannot reconstruct the secret.

Based on the SS scheme, a secret image sharing (SIS) scheme was proposed. In the scheme, several shadow images (or shares) are generated by the secret image, and there will be no secret information leakage. In the recovery phase, a secret image can be recovered through partial shadow images, even if some of the shadow images are lost or damaged. Therefore, compared with other cryptographic techniques, the SIS scheme has the characteristic of loss tolerance. Because of its characteristic, there are lots of application scenarios for SIS, such as electronic voting, communications in unreliable public channels, distributed storage system and access control, etc.

At present, there are many kinds of SIS, and the two most important ones are polynomial-based SIS (PSIS) and visual cryptography scheme (VCS) [3–5].

In 2002, Shamir's polynomial-based scheme was adopted into SIS by Thien and Lin [6]. The scheme encrypts the secret into the coefficients of a random $(k-1)$-degree polynomial in a finite field. In the recovery phase, the secret can be reconstructed by Lagrange interpolation. VCS has a unique property that the secret information can be obtained by stacking the shadow images, and humans can easily recognize the secret information by eyes. However, since it is implemented based on OR operation, it has some disadvantages such as low visual quality of recovered images

and lossy recovery, etc. In comparison with VCS, PSIS is more suitable for digital images, which can achieve secret image recovery with high visual quality.

Since PSIS can recover the secret image with a high quality, more properties of Shamir's polynomial-based scheme were studied. Yang et al. in [7,8] made use of a polynomial-based scheme to achieve lossless recovery and obtained a two-in-one SIS scheme. In addition, Li et al. in [9] gained the lossless secret image and enhanced the contrast of the image meantime. When considering the case that some shadows with higher importance are essential, Ref. [10] proposed a new (t, s, k, n)-ESIS scheme based on Shamir's scheme, where essential shadows are more important than non-essential shadows. In addition, shadow images with diferent priorities [11–15].Thus, Shamir's polynomial-based scheme has been widely used in SIS [16–18].

As a classic SS scheme, the polynomial interpolation is used to recover secret information in Shamir's polynomial-based scheme. The secrets are encrypted into the constant coefficient of a random $(k-1)$-degree polynomial. In the recovery phase, the constant coefficient can be solved by Lagrange interpolation, and the coefficient is the value of the secret pixel.

In Shamir's polynomial-based method, to divide the secret number s, a random $k-1$ degree polynomial $f(x) = a_0 + a_1 x + ... + a_{k-1}x^{k-1}$ is constructed, in which $a_0 = s$ and others are generated randomly in a finite field Fp. Then, it evaluates: $f(1), ..., f(i), ..., f(n)$, which are deserved as shares and distributed to associated participants.

Given any k of these $f(i)$ values $(i = 1, 2, ..., n)$, we can obtain the coefficients $(a_0, a_1, ..., a_{k-1})$ of $f(x)$ by interpolation, and then $s = a_0$ is evaluated.

Actually, the substance is to construct the polynomial for (k, n) threshold, in which any k out of n equations can solve the system and get the coefficients of the polynomial. Thus, we introduce matrix theory to review this problem in a wider perspective. Furthermore, based on matrix theory, we propose a general (k, n) threshold SIS construction method [19]. Thus, there are two contributions in this paper:

(1) Based on the analysis of the polynomial-based method proposed by Shamir, we summarize the necessary and sufficient conditions of constructing the polynomial, which are the basis of (k, n) threshold SIS.

(2) Based on matrix theory, we propose a general (k, n) threshold SIS construction. The effectiveness of the proposed construction is indicated by experimental results and analyses.

The following main content of the paper is as follows: Section 2 introduces some preliminary techniques as the basis of the proposed construction. In Section 3, the proposed (k, n) threshold SIS construction method is presented in detail. Section 4 gives experimental results and analyses. Finally, Section 5 concludes this paper.

2. Preliminaries

Some preliminaries are given here as the basis of our work. The goal of (k, n) threshold SIS is to share the secret image S into n shadow images $SC_1, SC_2, ..., SC_n$ in such a way that: (1) knowledge of any k or more shadow images makes S easily computable; (2) knowledge of any $k-1$ or fewer shadow images leaves S completely undetermined.

First of all, Shamir's polynomial-based scheme is given in Section 2.1. Furthermore, we will introduce analysis of Shamir's polynomial-based scheme based on matrix theory. At the end of this section, we propose the necessary and sufficient condition for (k, n) threshold SIS construction.

2.1. Shamir's Polynomial-Based Scheme

Shamir's scheme is based on polynomial interpolation. The scheme encrypts the secret into the constant coefficient of a random $(k-1)$-degree polynomial in a finite field. In the recovery phase, the secret can be reconstructed by Lagrange interpolation. For example, we take a pixel value s as

the gray value of the first secret pixel, and then to split s into n pixels corresponding to n shadows. The specific scheme is listed as follows:

(1) In the sharing phase, given a pixel value s, we select a prime number p, and $p > \max(n, s)$. In order to divide s into pieces sc_i, we generate a $k-1$ degree polynomial

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod p \tag{1}$$

in which $a_0 = s$ and $a_i (i = 1, \cdots, k-1)$ are randomly selected in the finite field $D = Zp[0, p-1]$, and then compute

$$sc_1 = f(1), \cdots, sc_i = f(i), \cdots, sc_n = f(n) \tag{2}$$

and take (i, sc_i) as a secret pair, where i serves as an identifying index or a order lable and sc_i serves as a shared pixel value.

The process repeats until all pixels of the secret image are processed. In the end, n shadow images are generated.

(2) In the recovery phase, given any k pairs $\{(i_j, sc_{i_j})\}_{j=1}^{k}, (i_1, i_2, \cdots, i_k) \subseteq \{1, 2, \cdots, n\}$, we can reconstruct $f(x)$ by the Largrange's interpolation, and then evaluate $s = f(0)$. Knowledge of just $k-1$ of these values does not suffice in order to calculate s.

2.2. Analysis of Shamir's Polynomial Based on Matrix Theory

In Shamir's sharing polynomial shown in Equation (1), equations in Equation (2) are calculated in the sharing phase. In the recovery phase, when any k participants with k pairs get together, the polynomial $f(x)$ can be reconstructed by solving the k equations. Without loss of generality, we can assume that their pairs are $(1, f(1)), (2, f(2)), \cdots, (k, f(k))$. Thus, we can get k equations as follows:

$$\begin{cases} f(1) = a_0 + a_1 + \cdots + a_{k-1} \\ f(2) = a_0 + 2^1 a_1 + \cdots + 2^{k-1} a_{k-1} \\ f(3) = a_0 + 3^1 a_1 + \cdots + 3^{k-1} a_{k-1} \\ \vdots \\ f(k) = a_0 + k^1 \cdot a_1 + \cdots + k^{k-1} \cdot a_{k-1} \end{cases} \pmod p. \tag{3}$$

Here, the parameter k is fixed, and $a_0, a_1, ..., a_{k-1}$ are unknown. Thus, Equation (3) is a linear system with k equations and k unknowns. In another point of view, Equation (3) is equivalent to the following vector where **a** deserves as a variable:

$$\mathbf{Ka} = \mathbf{f}. \tag{4}$$

According to Equation (4), we can rewrite Equation (3) as Equation (5):

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{k-1} \\ 1 & 3 & 3^2 & \cdots & 3^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & k & k^2 & \cdots & k^{k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix} \pmod p = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \\ \vdots \\ f(k) \end{bmatrix} \pmod p. \tag{5}$$

Actually, linear equations in Equation (3) and vector equation in Equation (4) is equivalent. In addition, solution and solution vector are indiscriminate.

Using the rank of the coefficient matrix **K** and the augmented matrix $(\mathbf{K}, \mathbf{f})$, we can easily discuss whether the linear system in Equation (3) has a unique solution according to the following theorem.

Theorem 1. *Assume that there is a k-variables linear equations* $\mathbf{Ka} = \mathbf{f}$. *The necessary and sufficient condition for a unique solution is: rank(*$\mathbf{K}$*) = rank(*$\mathbf{K}$,$\mathbf{f}$*) = k.*

According to this theorem, to solve the Equation (3) and then get the coefficients of $f(x)$, we must ensure that the rank of the coefficient matrix $\mathbf{K}$ is k.

In Shamir's polynomial-based SS scheme, the coefficient matrix $\mathbf{K}$ of the equations is:

$$\mathbf{K} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{k-1} \\ 1 & 3 & 3^2 & \cdots & 3^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & k & k^2 & \cdots & k^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & n & n^2 & \cdots & n^{k-1} \end{bmatrix}. \tag{6}$$

The coefficient matrix is a Vandermonde matrix. Because the Vandermonde matrix has a property that the rank of any k order submatrix is k, the equation system in Shamir's scheme is solvable with a unique solution [20].

One of the efficient methods to get the sharing polynomial is to use the Langrange interpolation. More generally, considering that the recovery phase is equivalent to equation solving, we can use matrix theory to solve equations and obtain the coefficients. According to Equation (5) and Theorem 1, we can solve $\mathbf{a}$ through the inverse matrix of k order submatrix.

2.3. The Design Rule of Generating the Coefficient Matrix of Sharing Polynomial

The analysis in Section 2.2 proves that the principle of Shamir's scheme is to select a Vandermonde matrix as the coefficient matrix to construct a polynomial and reconstruct the polynomial by Langrange interpolation.

In fact, Shamir's sharing polynomial constructed by the Vandermonde matrix is only a special case of constructing a sharing polynomial satisfying a (k, n) threshold. We can use a more general coefficient matrix to construct sharing polynomial equations, to encrypt the secret into n shares and to decrypt the secret by any k shares if and only if the coefficient matrix satisfies the following theorem:

Theorem 2 (Objective Theorem)**.** *Given an* $n \times k$ *matrix* $\mathbf{K}$ *and a vector* $\mathbf{a} = (a_0, a_1, \cdots, a_k)^T$ *in which* $a_0 = s$ *and others are generated randomly, we can construct a linear system of equations* $\mathbf{Ka} = \mathbf{f}$ *to encrypt s into n shares. In the recovery phase, in order to reconstruct vector* $\mathbf{a}$ *by any* $k \times k$ *submatrix of* $\mathbf{K}$ *and corresponding shares,* $\mathbf{K}$ *must satisfy the following condition:*

Any k row vectors of the coefficient matrix $\mathbf{K}$ *are linearly independent.*

The correctness of this theorem is obvious. Once the coefficient $\mathbf{K}$ meets Theorem 2, the rank of any k order submatrix of $\mathbf{K}$ is k. According to Theorem 1, k-variables' linear equations $\mathbf{Ka} = \mathbf{f}$ in Equation (3) has a unique solution. Hence, a coefficient matrix satisfying Theorem 2 can be applied to construct the sharing polynomial. In addition, in the recovery phase, we can decrypt the shares to secret by solving the inverse matrix instead of using Langrange interpolation. Thus, a (k, n) threshold SIS scheme could be constructed.

The question now is how to construct the coefficient matrix satisfying the requirement in Theorem 2. In the following section, we will first introduce a coefficient matrix generation approach and further propose a general (k, n) threshold SIS construction based on matrix theory.

3. The Proposed Construction Method

3.1. The Basic Idea

In order to construct the SIS, we first need to construct a matrix **K** with size of $n \times k$, which satisfies Theorem 2. Let the constructed matrix serve as the coefficient matrix shown in Equation (4) and compute $\mathbf{f} = \mathbf{Ka}$ to get shared pixel values of shadow images. The shadows are distributed to participants, and every row vector of **K** is distributed to corresponding participants as well.

In the recovery phase, suppose that k participants get together to reconstruct the sharing polynomial. After the polynomial is reconstructed, the secret is obtained by a_0. Next, we will introduce our method and proof in Section 3.2, and we will also do a feasibility study showed in Section 3.3. Section 3.4 gives a detailed construction method of the proposed general (k, n) threshold SIS scheme.

3.2. Construction Method of the Coefficient Matrix **K**

This part will show how to construct the matrix **K** satisfying Theorem 2. Based on the analysis, we summarize a construction method as Theorem 3. According to Theorem 3, the $n \times k$ coefficient matrix **K** is constructed by a special matrix **G**, in which the determinant of all submatrices is non-zero.

Given matrix **G** and $\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix}$, and the k-dimensional row vectors $(\alpha_1, \alpha_2, \cdots, \alpha_k)$ are linearly independent. For example, α can be a Vandermonde matrix. We note that **G** and α are generated by random assignment and validation. In addition, the feasibility analysis is given in Section 3.3. Then, we compute $\beta = \mathbf{G}\alpha$. Thus, we can get another matrix $\beta = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{pmatrix}$, in which the k-dimensional row vectors are linearly independent. Then, we create a new matrix **K** by concatenating the two matrices α and β:

$$\mathbf{K} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \\ \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} \tag{7}$$

and the size of matrix **K** is $2k \times k$.

That is to say, any vector β_i $(i = 1, \cdots, k)$ can be expressed linearly by row vectors in α. Gathering these linear expressed into a matrix form, we have

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & \vdots & g_{kk} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix}, \tag{8}$$

in which **G** serves as a temporary coefficient matrix. By computing $\beta = \mathbf{G}\alpha$ and concatenating α and β, we will get a matrix **K** which satisfies Theorem 2.

We note that the row vector group of α and β are all linearly independent. However, any k vectors selected between α and β are not apparently linearly independent, which is the reason why we give Theorem 3 and the corresponding proof.

Theorem 3 (Conditional Theorem). *Given a set of linearly independent k-dimensional row vectors* $\alpha_1, \alpha_2, \cdots, \alpha_k$, *which form a* $k \times k$ *matrix* $\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix}$. *Let matrix* $\mathbf{G}$ *satisfy that all the minors of matrix* $\mathbf{G}$ *are nonzero. Let* $\mathbf{G}\alpha = \beta$ *and* $\mathbf{K} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \\ \beta_1 \\ \vdots \\ \beta_k \end{pmatrix}$. *Thus, we can conclude that any k vectors of the coefficient matrix* $\mathbf{K}$ *are linearly independent.*

Proof. Select any k vectors to form $\mathbf{C} = \{\chi_1, \chi_2, \cdots, \chi_k\}$. The aim is to prove that $\chi_1, \chi_2, \cdots, \chi_k$ are linearly independent.

(1) For the case of $\mathbf{C} = \alpha$, since the vectors of α are linearly independent, the vectors of $\mathbf{C}$ are linearly independent.
(2) For the case of $\mathbf{C} = \beta$, since $\beta = \mathbf{G}\alpha$ and $\mathbf{G}$ is invertible, the vectors of $\mathbf{C}$ are linearly independent.
(3) For the case of $\mathbf{C} \cap \alpha \neq \emptyset, \mathbf{C} \cap \beta \neq \emptyset$, let $|\mathbf{C} \cap \alpha| = \mathbf{s}, |\mathbf{C} \cap \beta| = \mathbf{t}$, thus there are s vectors in $\mathbf{C} \cap \alpha$ and t vectors in $\mathbf{C} \cap \beta$ are linearly independent and $s + t = k$. Without loss of generality, we assume that $\mathbf{C} \cap \alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_s\}$ and $\mathbf{C} \cap \beta = \{\beta_1, \beta_2, \cdots, \beta_t\}$ in which

$$\beta_i = g_{i1}\alpha_1 + g_{i2}\alpha_2 + \cdots + g_{ik}\alpha_k. \tag{9}$$

Consider the equation

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_s\alpha_s + x_{s+1}\beta_1 + x_{s+2}\beta_2 + \cdots + x_k\beta_t = 0, \tag{10}$$

according to Equations (8) and (9), we have

$$\begin{aligned} &(x_1 + x_{s+1}g_{11} + x_{s+2}g_{21} + \cdots + x_kg_{t1})\alpha_1 + (x_2 + x_{s+1}g_{12} + x_{s+2}g_{22} + \cdots + x_kg_{t2})\alpha_2 \\ &+ \cdots + (x_s + x_{s+1}g_{1s} + x_{x+2}g_{2s} + \cdots + x_kg_{ts})\alpha_s + (x_{s+1}g_{1(s+1)} + x_{s+2}g_{2(s+1)} + \cdots + \\ &x_kg_{t(s+1)})\alpha_{s+1} + (x_{s+1}g_{1(s+2)} + x_{s+2}g_{2(s+2)} + \cdots + x_kg_{t(s+2)})\alpha_{s+2} + \cdots \\ &+ (x_{s+1}g_{1k} + x_{s+2}g_{2k} + \cdots + x_kg_{tk})\alpha_k = 0. \end{aligned} \tag{11}$$

Since $\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_s, \alpha_{s+1}, \cdots, \alpha_k\}$ are linearly independent, according to matrix theory, we get

$$\begin{aligned} &x_1 + x_{s+1}g_{11} + x_{s+2}g_{21} + \cdots + x_kg_{t1} = 0 \\ &x_2 + x_{s+1}g_{12} + x_{s+2}g_{22} + \cdots + x_kg_{t2} = 0 \\ &\vdots \\ &x_s + x_{s+1}g_{1s} + x_{x+2}g_{2s} + \cdots + x_kg_{ts} = 0 \\ &x_{s+1}g_{1(s+1)} + x_{s+2}g_{2(s+1)} + \cdots + x_kg_{t(s+1)} = 0 \\ &x_{s+1}g_{1(s+2)} + x_{s+2}g_{2(s+2)} + \cdots + x_kg_{t(s+2)} = 0 \\ &\vdots \\ &x_{s+1}g_{1k} + x_{s+2}g_{2k} + \cdots + x_kg_{tk} = 0, \end{aligned} \tag{12}$$

which can be written as

$$\begin{bmatrix} 1 & 0 & 0 & 0 & g_{11} & g_{21} & \cdots & g_{t1} \\ 0 & 1 & 0 & 0 & g_{12} & g_{22} & \cdots & g_{t2} \\ 0 & 0 & \cdots & 0 & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & g_{1s} & g_{2s} & \cdots & g_{ts} \\ 0 & 0 & 0 & 0 & g_{1(s+1)} & g_{2(s+1)} & \cdots & g_{t(s+1)} \\ 0 & 0 & 0 & 0 & g_{1(s+2)} & g_{2(s+2)} & \cdots & g_{t(s+2)} \\ 0 & 0 & 0 & 0 & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & g_{1k} & g_{2k} & \cdots & g_{tk} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \\ x_{s+1} \\ x_{s+2} \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{13}$$

Let

$$G' = \begin{bmatrix} g_{1(s+1)} & g_{2(s+1)} & \cdots & g_{t(s+1)} \\ g_{1(s+2)} & g_{2(s+2)} & \cdots & g_{t(s+2)} \\ g_{1(s+3)} & g_{2(s+3)} & \cdots & g_{t(s+3)} \\ \vdots & \vdots & \cdots & \vdots \\ g_{1k} & g_{2k} & \cdots & g_{tk} \end{bmatrix}.$$

Then, the size of $\mathbf{G}'$ is $t \times t$, and t range from 1 to k. Now, look at the coefficient matrix in Equation (13) whose rank is $s + rank(G')$. Since all the minors of matrix $\mathbf{G}$ are full rank, the rank of $\mathbf{G}'$ is t, that is, $rank(G') = t$. Thus, the determinant of the coefficient matrix in Equation (13) is nonzero. Hence, from Equation (13), we get:

$$x_1 = x_2 = \cdots = x_s = x_{s+1} = \cdots = x_k = 0. \tag{14}$$

Thus, according to Equation (10), $\alpha_1, \alpha_2, \cdots, \alpha_s, \beta_1, \beta_2, \cdots, \beta_t$ are linearly independent, that is to say, $\chi_1, \chi_2, \cdots, \chi_k$ are linearly independent. □

Thanks to the matrix $\mathbf{G}$ has the special property, the matrix $\mathbf{K}$ has such a property: any k vectors of the coefficient matrix $\mathbf{K}$ are linearly independent. Because of that, we can construct a (k, n_x) threshold SS (n_x ranges from k to $2k$). For the purpose of simplicity, we assume a (k, n_x) as (k, n) threshold in the rest of this paper, which is enough for real applications.

Based on the constructed coefficient matrix $\mathbf{K}$, we will introduce a method of constructing (k, n) threshold SIS schemes.

3.3. Feasibility Analysis

Generating linearly independent vectors is a difficult problem in mathematics. However, the random search method can be a solution. Estimates of the density of matrix show that one could easily find the initial matrix α and the temporary matrix $\mathbf{G}$ satisfying Theorem 3.

Randomly select n vectors in a set $\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \in Z_p^n$; the probability of these vectors being linearly independent is P_r:

$$\begin{aligned} P_r &= (p^n - 1) \cdot (p^n - p) \cdot (p^n - p^2) \cdot \cdots \cdot (p^n - p^{n-1}) / p^{n^2} \\ &= (1 - \tfrac{1}{p^n}) \cdot (1 - \tfrac{1}{p^{n-1}}) \cdot (1 - \tfrac{1}{p^{n-2}}) \cdot \cdots \cdot (1 - \tfrac{1}{p}) \\ &\geq 1 - \tfrac{1}{p^n} - \tfrac{1}{p^{n-1}} - \tfrac{1}{p^{n-2}} - \cdots - \tfrac{1}{p} \geq 1 - \tfrac{1}{p-1}. \end{aligned} \tag{15}$$

For example, when $p = 23, P_r \geq 0.95$; $p = 131, P_r \geq 0.992$; $p = 251, P_r \geq 0.996$. Thus, when p is a big prime number, the probability of any n vectors being linearly independent is very high. That is to say, the initial matrix α of which the vectors are linearly independent is easily to be generated.

Furthermore, when taking into consideration that all the minors of an $n \times n$ **G** are nonzero, we can analyze the probability by way of the method mentioned above. Let P_i be the probability of that all the $i \times i$ minors of **G** (i range from 1 to n)are nonzero. Hence, we get:

$$\begin{aligned}
&P_1 = \left(1-\tfrac{1}{p}\right)^{\binom{n}{1}^2} \geq \left(1-\tfrac{1}{p-1}\right)^{\binom{n}{1}^2} \\
&P_2 = \left[\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right)\right]^{\binom{n}{2}^2} \geq \left(1-\tfrac{1}{p-1}\right)^{\binom{n}{2}^2} \\
&\vdots \\
&P_i = \left[\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right)\cdots\left(1-\tfrac{1}{p^i}\right)\right]^{\binom{n}{i}^2} \geq \left(1-\tfrac{1}{p-1}\right)^{\binom{n}{i}^2} \\
&\vdots \\
&P_n = \left[\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right)\cdots\left(1-\tfrac{1}{p^n}\right)\right]^{\binom{n}{n}^2} \geq \left(1-\tfrac{1}{p-1}\right)^{\binom{n}{n}^2}.
\end{aligned} \tag{16}$$

Thus, we can get the value of P_r, the probability of that any minors of matrix **G** is nonzero, as follows:

$$P_r = P_1 \cdot P_2 \cdot \cdots \cdot P_n \geq \left(1-\tfrac{1}{p-1}\right)^{\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2} = \left(1-\tfrac{1}{p-1}\right)^{\binom{2n}{n}-1} \approx \left(1-\tfrac{1}{p-1}\right)^{\binom{2n}{n}}. \tag{17}$$

When $p = 251, n = 3$,

$$P_r \geq \left(1-\frac{1}{250}\right)^{\binom{6}{3}} = \left(1-\frac{1}{250}\right)^{20} = 0.92297,\ \frac{1}{P_r} = 1.08,$$

which implies that we need average every 1.08 times to get such a matrix **G** that satisfies our Theorem 3.

When $p = 251, n = 6$,

$$P_r \geq \left(1-\frac{1}{250}\right)^{\binom{12}{6}} = \left(1-\frac{1}{250}\right)^{924} = 0.02464,\ \frac{1}{P_r} = 40.58.$$

Thus, we can get randomly generate a qualified **G** matrix by average 40.58 times. This implies that the construction is feasible.

3.4. The Algorithms of Secret Image Sharing

At the beginning of this section, we first connect the theorems to each other. Theorem 1 is the necessary and sufficient condition that the linear equations $\mathbf{Ka} = \mathbf{f}$ have a unique solution. The objective theorem Theorem 2 is the principle that **Ka** must satisfy according to Theorem 1. The conditional theorem, Theorem 3, is the method of constructing coefficient matrix **Ka** to satisfy our objective theorem. Hence, we could get a general (k, n) threshold SIS construction.

In this section, we use the constructed coefficient matrix **K** to achieve polynomial-based SIS. In what follows, the original grayscale secret image is represented by S, and the size is $M \times N$. Without loss of generality, we split the first secret pixel s into n pixels corresponding to n shadows' images.

3.4.1. The Sharing Phase

In the sharing phase, to divide the secret s into pieces sc_i, we generate a matrix **K** constructed by the way mentioned in Section 3.2. We select a prime number p. We generate a vector $\mathbf{a} = (a_0, a_1, \cdots, a_{k-1})$ where $a_0 = s$ and the others are $k-1$ random integer numbers generated in the finite field $Zp = [0, p-1]$. Then, compute $\mathbf{Ka} = \mathbf{f}$ as follows:

$$\mathbf{Ka} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \\ \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} \bullet \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} sc_1 \\ \vdots \\ sc_i \\ \vdots \\ sc_n \end{pmatrix} (\mathrm{mod}\, p). \tag{18}$$

sc_i is distributed to the ith participant, as well as the corresponding ith row vector $\mathbf{k_i}$ of the matrix $\mathbf{K}$. We take $(\mathbf{k_i}, sc_i)$ as a share, where $\mathbf{k_i}$ serves as an identifying index or a key and sc_i serves as a pixel value. The steps are described in Algorithm 1.

Algorithm 1. The proposed general (k, n) threshold SIS construction by matrix theory for sharing phase
Input: The threshold parameters (k, n), a matrix $\mathbf{K}$ constructed by Theorem 3, a secret image S with size of $M \times N$ and a prime number p **Output**: n shadow images $SC_1, SC_2, \cdots SC_n$
Step 1: For every secret pixel s in each position $(i, j) \in \{(i, j) \vert 1 \le i \le M, 1 \le j \le N\}$, repeat Step 2–3. **Step 2:** Generate a vector $\mathbf{a} = (a_0, a_1, \cdots, a_{k-1})$, set $s = a_0$, and generate others randomly in the finite domain $[0, p-1]$. **Step 3:** Compute $\mathbf{f} = \mathbf{Ka} (\mathrm{mod}\ p)$, where $sc_1(i, j) = f(1), \cdots, sc_n(i, j) = f(n)$. **Step 3:** Output n shadow images $SC_1, SC_2, \cdots SC_n$

The pseudo code of Algorithm 1 is presented as follows:

Algorithm 1 Matrix $(k, n, \mathbf{K}, S, M, N, P)$

```
for i = 1 to M do
    for j = 1 to N do
        a_0 = S[i, j]
        generate (a_0, a_1, ··· , a_{k-1}) randomly
        f = f = Ka(mod p)
        for k = 1 to n do
            sc_k(i, j) = f(k)
        end for
    end for
end for
```

Finally, according to Algorithm 1, the n shadow images are generated succesfully by the proposed SIS scheme based on matrix theory. It should be noted that we utilize the largest prime number less than 255; however, the grayscale pixel value of an image ranges from 0 to 256, so our construction is not totally lossless. However, it is still a high resolution SIS construction method.

3.4.2. The Recovery Phase

In the recovery phase, given any k pairs $\{(\mathbf{k_{i_j}}, SC_{i_j})\}_{j=1}^{k}, (i_1, i_2, \cdots, i_k) \subseteq \{1, 2, \cdots, n\}$, we can concatenate k vectors $\mathbf{k_{i_j}}$ to generate a submatrix $\mathbf{K_{mini}}$. Thus, we can finally obtain the vector $\mathbf{a} = (a_0, a_1, \cdots, a_{k-1})$ by solving the following linear equation:

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix} = \mathbf{K_{mini}^{-1}} \bullet \begin{bmatrix} sc_{i_1} \\ sc_{i_2} \\ \vdots \\ sc_{i_k} \end{bmatrix} (\mathrm{mod}\ p), \tag{19}$$

the secret pixel s is the value of a_0. Note that all the calculations are performed in a finite field. The value of a_0 will not be solved if the number of linearly independent vectors is less than k. The specific recovery steps are shown in Algorithm 2.

Algorithm 2. The proposed general (k, n) threshold SIS construction in matrix method in recovery phase
Input: The k shadow images which are randomly selected from n secret shadow images $SC_1, SC_2, \cdots, SC_n$ and corresponding k vectors $\mathbf{k_{i_j}}$ **Output**:The original secret image S
Step 1: According to the k vectors $\mathbf{k_i}$, concatenate k vectors $\mathbf{k_i}$ to a matrix $\mathbf{K_{mini}}$. **Step 2:** For each position $S(i,j) \in \{(i,j)\|1 \leq i \leq M, 1 \leq j \leq N\}$, repeat Step 3–4. **Step 3:** According to the Equation (4), construct linear system. **Step 4:** Get the coefficient a_0 of $f(x)$ by computing linear system according to Equation (19), and set the pixel $S(i,j) = a_0$. **Step 5:** Output the secret image S.

The pseudo code of Algorithm 2 is presented as follows.

Algorithm 2 recover $(k, \mathbf{K}, M, N, P)$

```
for c = 1 to M do
  for l = 1 to N do
    for j = 1 to k do
      K_mini[j] = k_{i_j}
      SC[j] = SC_{i_j}[c, l]
      a = K_mini^{-1} * SC
      SC[c, l] = a_0
    end for
  end for
end for
```

3.5. Complexity Evaluation

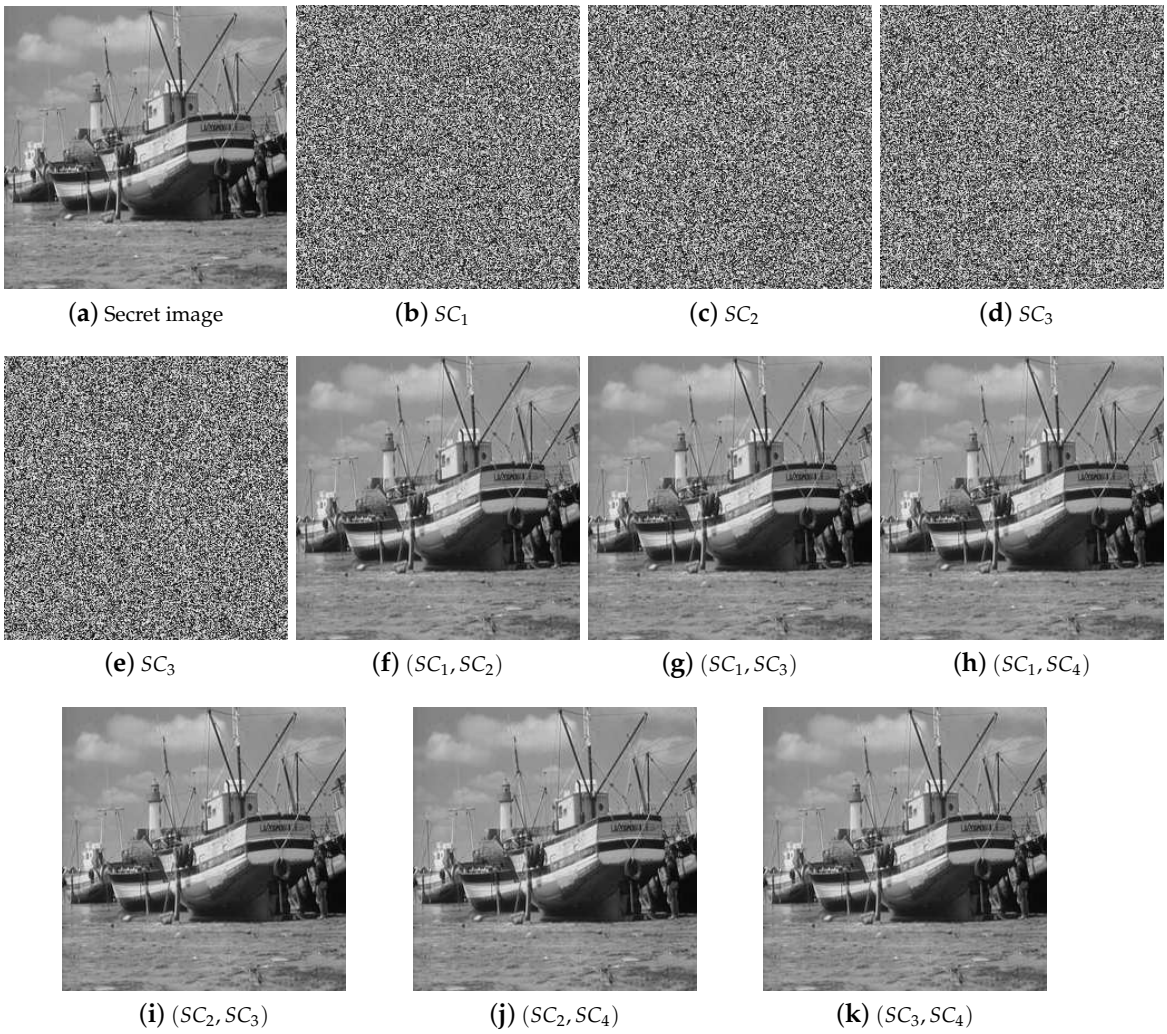
The algorithm complexity for decryption of Shamir's scheme is $O\left(k \log^2 k\right)$, while k is the total number of shares participating in recovery. In addition, the algorithm complexity for equation system solution is $O(k^2) \sim O(k^3)$. Since the coefficient matrix is not a sparse matrix, the algorithm complexity of the proposed method is $O(k^3)$, which is a little higher than that of Shamir.

4. Experimental Results and Analyses

4.1. Image Illustration

In this section, this paper carries on the experiments and analyses of the proposed method. Experimental images demonstrate the effectiveness intuitively while corresponding histograms draw the probability distribution of pixel values to present features from the view of statistic analysis.

In the experiments, first, as shown in Figure 1, we adopt Shamir's polynomial-based $(2, 4)$ threshold scheme. Second, as shown in Figure 2, we perform an experiment with our construction, where the threshold is $(2, 4)$. In addition, corresponding histograms will follow, as shown in Figure 3. Finally, simulation results of the proposed construction are presented in Figure 4, where threshold is $(3, 6)$. Figures 1a and 4a are used as the original gray secret images, with a size of 256×256.



(a) Secret image **(b)** SC_1 **(c)** SC_2 **(d)** SC_3

(e) SC_3 **(f)** (SC_1, SC_2) **(g)** (SC_1, SC_3) **(h)** (SC_1, SC_4)

(i) (SC_2, SC_3) **(j)** (SC_2, SC_4) **(k)** (SC_3, SC_4)

Figure 1. Simulation results of Shamir's polynomial-based scheme, where $k = 2, n = 4$. (**a**) the secret image; (**b**–**e**) four original shadow images SC_1, SC_2, SC_3 and SC_4; (**f**) revealing results by SC_1 and SC_2; (**g**) revealing result by SC_1 and SC_3; (**h**) revealing results by SC_1 and SC_4; (**i**) revealing results by SC_2 and SC_3; (**j**) revealing results by SC_2 and SC_4; (**k**) revealing results by SC_3 and SC_4.

As a special case of our construction method, Figure 1 shows an experiment based on Shamir's polynomial-based scheme, where the coefficient matrix is a 4×2 Vandermonde matrix:

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix}. \tag{20}$$

In this case, $\alpha = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$. In addition, $\mathbf{K} = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}$, which satisfies Theorem 3. Hence, it is obvious that the matrix in Equation (20) satisfies the objective theorem that any k row vectors are linearly independent. Figure 1b–e are four noise-like shadow images SC_1, SC_2, SC_3 and SC_4, which are generated from $(2, 4)$ threshold construction. The result revealed by any two shadow images are shown in Figure 1f–k.

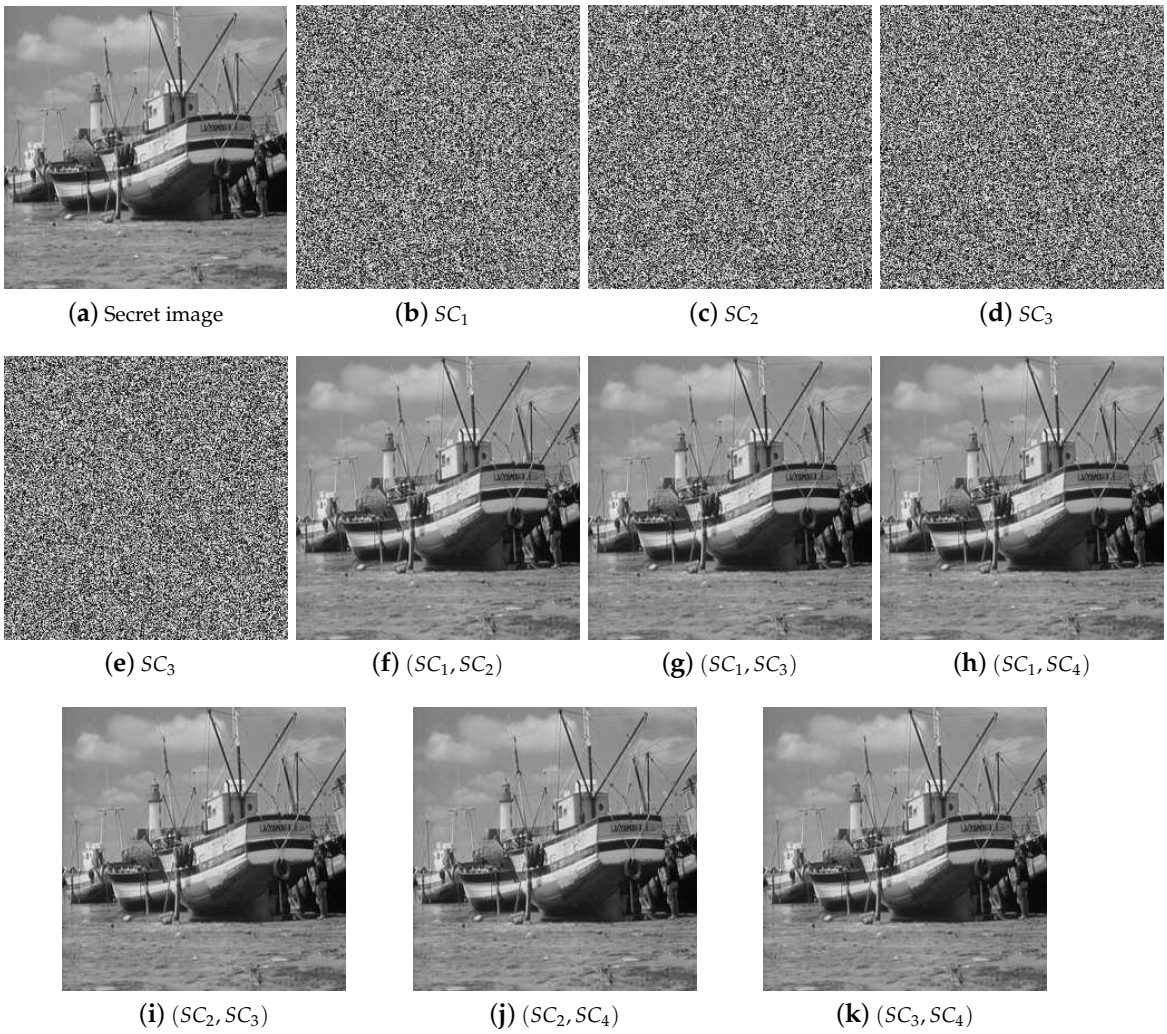


Figure 2. Simulation results of the proposed method with the coefficient matrix as Equation (21), where $k = 2, n = 4$. (**a**) the secret image; (**b**–**e**) four original shadow images SC_1, SC_2, SC_3 and SC_4; (**f**) revealing results by SC_1 and SC_2; (**g**) revealing results by SC_1 and SC_3; (**h**) revealing results by SC_1 and SC_4; (**i**) revealing results by SC_2 and SC_3; (**j**) revealing results by SC_2 and SC_4; (**k**) revealing results by SC_3 and SC_4, using our general (k, n) threshold SIS construction based on matrix theory.

This coefficient matrix used to construct the polynomial is a Vandermonde matrix, which is the basis of Shamir's polynomial-based scheme. Hence, it is proved that Shamir's polynomial-based scheme is a special case in our construction method.

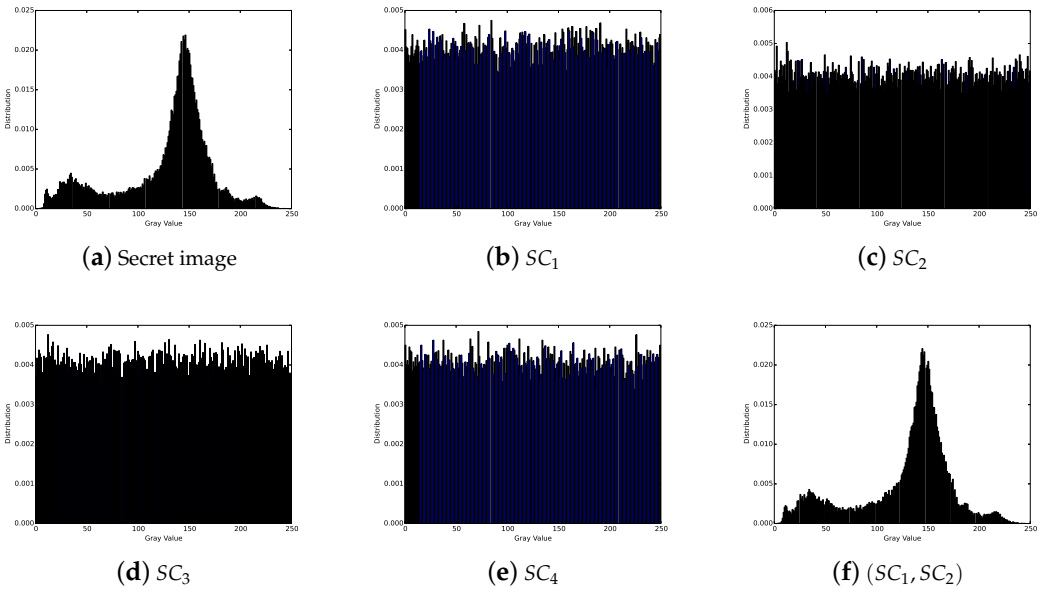
Next, in a more general case, using the coefficient matrix construction method, we generate a random 4×2 matrix $\mathbf{K}$. Let $\alpha = \begin{bmatrix} 7 & 6 \\ 3 & 3 \end{bmatrix}$. Then, we generate a temporary matrix $\mathbf{G} = \begin{bmatrix} 6 & 9 \\ 4 & 5 \end{bmatrix}$ who satisfies Theorem 3. Compute $\beta = \mathbf{G}\alpha$. We have $\beta = \begin{bmatrix} 69 & 63 \\ 43 & 39 \end{bmatrix}$. Thus, a 4×2 coefficient matrix $\mathbf{K}$ for a $(2, 4)$ threshold SS scheme is obtained by concatenating α and β as follows:

$$\begin{pmatrix} 7 & 6 \\ 3 & 3 \\ 69 & 63 \\ 43 & 39 \end{pmatrix}. \tag{21}$$

(However, of course, we can use any two row vectors to generate a (2, 2) threshold scheme; we can surely use any three row vectors to get a (2, 3) threshold scheme. Here, we take the (2, 4) threshold as an example.) Then, as shown in Figure 2b–e, we generate four noise-like shadows' images SC_1, SC_2, SC_3 and SC_4 using Algorithm 1. In the recovery phase, Figure 2f–k is secret images revealed by any two shadow images.

The experimental results in Figure 2 imply that the coefficient matrix $\mathbf{K}$ which satisfies Theorem 3 could construct the polynomial for a $(2,4)$ threshold SIS scheme.

Furthermore, corresponding histograms draw the probability distribution of pixel values to verify the security of the construction method from the view of statistic analysis, as shown in Figure 3.



(**a**) Secret image (**b**) SC_1 (**c**) SC_2

(**d**) SC_3 (**e**) SC_4 (**f**) (SC_1, SC_2)

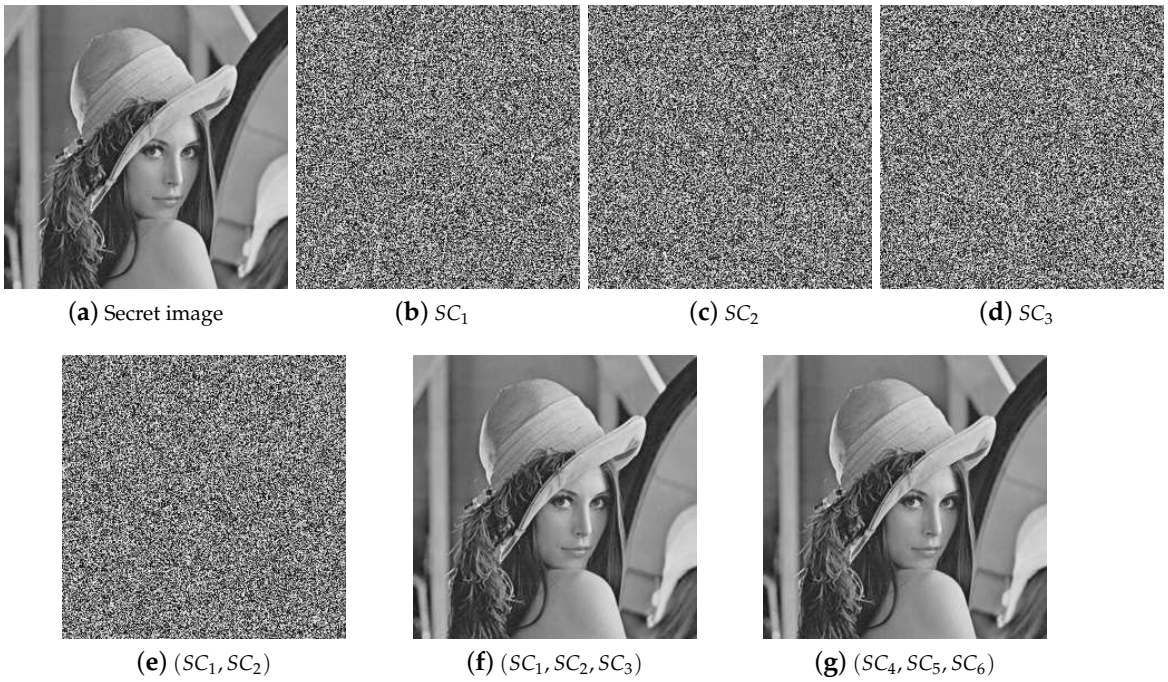
Figure 3. The statistical histogram of experimental images in the $(2,4)$ threshold scheme. (**a**) the secret image S; (**b**) shadow image SC_1; (**c**) shadow image SC_2; (**d**) shadow image SC_3; (**e**) shadow image SC_4; (**f**) revealing result by SC_1 and SC_2.

From the Figure 3b–e, we can see that the probability distribution of pixel values in shadow images is equally distributed, which proves that the construction method is secure.

In addition, we generate a random 6×3 matrix $\mathbf{K}$ as follows. Let $\alpha = \begin{bmatrix} 8 & 8 & 6 \\ 3 & 4 & 1 \\ 3 & 2 & 7 \end{bmatrix}$; then, we generate a temporary matrix $\mathbf{G} = \begin{bmatrix} 3 & 2 & 5 \\ 2 & 4 & 9 \\ 6 & 5 & 4 \end{bmatrix}$, which satisfies Theorem 3. Compute $\beta = \mathbf{G}\alpha$. We have $\beta = \begin{bmatrix} 45 & 42 & 55 \\ 55 & 50 & 79 \\ 75 & 76 & 69 \end{bmatrix}$. Thus, a 6×3 coefficient matrix $\mathbf{K}$ for a $(3,6)$ threshold SIS is obtained by concatenating α and β as follows:

$$\begin{pmatrix} 8 & 8 & 6 \\ 3 & 4 & 1 \\ 3 & 2 & 7 \\ 45 & 42 & 55 \\ 55 & 50 & 79 \\ 75 & 76 & 69 \end{pmatrix}. \tag{22}$$

Using this matrix to construct a general SIS scheme, we can get experimental results of $(3, 6)$ threshold, as shown in Figure 4. Figure 4a presents the grayscale secret image. Six shadow images $SC_1, SC_2, ..., SC_6$ are generated, three of which are shown in Figure 4b–d. The image recovered by the first two shadow images is shown in Figure 4e. From Figure 4e, we can see that the recovered image with less than three shadow images gives no clue about the secret image. Figure 4f shows the image recovered by SC_1, SC_2 and SC_3; Figure 4g shows the image recovered by SC_4, SC_5 and SC_6.



(**a**) Secret image (**b**) SC_1 (**c**) SC_2 (**d**) SC_3

(**e**) (SC_1, SC_2) (**f**) (SC_1, SC_2, SC_3) (**g**) (SC_4, SC_5, SC_6)

Figure 4. Simulation results of the proposed method with the coefficient matrix as Equation (22), where $k = 3, n = 6$. (**a**) the secret image S; (**b**–**d**) three shadow images SC_1, SC_2, SC_3 of the six shadow images; (**e**) revealing result by SC_1 and SC_2; (**f**) revealing result by SC_1, SC_2 and SC_3; (**g**) revealing result by SC_4, SC_5 and SC_6.

The experimental results in Figure 4 imply that the coefficient matrix **K** who satisfies Theorem 3 could construct the polynomial for a $(3, 6)$ threshold SIS scheme. As a result, it is demonstrated that the proposed objective theorem and conditional theorem are correct.

The proposed method is a construction for more SIS schemes since every different coefficient matrix **K** can be used to construct a SIS scheme. Hence, there is no comparison between the proposed method and other SIS schemes.

4.2. Brief Summary

Based on experimental results shown in Figures 1–3, we can conclude that:

(1) The proposed objective theorem and conditional theorem are effective.
(2) The shares are noise-like, hence either every single share gives no clue about the secret.

(3) The proposed construction achieves (k, n) threshold SIS. With k or more shares, the secret image could be recovered precisely, while the images recovered with less than k shares give no clue about the secret image.

(4) Our general (k, n) threshold secret image sharing construction based on matrix theory is effective. Furthermore, Shamir's polynomial-based scheme is a special case of our construction method.

5. Conclusions

Based on the analysis of the principle of Shamir's polynomial-based scheme, we proposed the objective theorem and conditional theorem, by which we can generate the coefficient matrix of (k, n) threshold sharing polynomials. Furthermore, based on matrix theory, we proposed a general (k, n) threshold SIS construction method. Theoretic proofs and experimental results demonstrate that our construction is effective, and Shamir's polynomial-based scheme is a special case of our construction method. Exploring the situation of $n > 2k$ and achieving a lossless recovery will be the future work.

Author Contributions: Conceptualization, W.D. and X.Y.; Data Curation, L.L.; Formal Analysis, W.D.; Funding Acquisition, X.Y.; Methodology, K.L., X.Y. and H.W.; Supervision, K.L.; Validation, W.D. and L.L.; Writing—Original Draft, W.D.; Writing—Review and Editing, W.D., K.L., X.Y., L.L. and Q.G.

Funding: This research was funded by the National Natural Science Foundation of China Grant No. 61602491 and the Key Program of the National University of Defense Technology Grant No. ZK-17-02-07.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the National Computer Conferenceon IEEE Computer Society, New York, NY, USA, 4–7 June 1979; pp. 313–317.
3. Naor, M.; Shamir, A. Visual cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
4. Weir, J.; Yan, W. A comprehensive study of visual cryptography. In *Transactions on Data Hiding and Multimedia Security V*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 70–105.
5. Yan, X.; Liu, X.; Yang, C.N. An enhanced threshold visual secret sharing based on random grids. *J. Real-Time Image Process.* **2015**, 1–13. [CrossRef]
6. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
7. Yang, C.N.; Ciou, C.B. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image Vis. Comput.* **2010**, *28*, 1600–1610. [CrossRef]
8. Yang, C.N.; Chen, T.S.; Yu, K.H.; Wang, C.C. Improvements of image sharing with steganography and authentication. *J. Syst. Soft.* **2007**, *80*, 1070–1076. [CrossRef]
9. Li, P.; Ma, P.J.; Su, X.H.; Yang, C.N. Improvements of a two-in-one image secret sharing scheme based on gray mixing model. *J. Vis. Commun. Image Represent.* **2012**, *23*, 441–453. [CrossRef]
10. Li, P.; Yang, C.N.; Wu, C.C.; Kong, Q.; Ma, Y. Essential secret image sharing scheme with different importance of shadows. *J. Vis. Commun. Image Represent.* **2013**, *24*, 1106–1114. [CrossRef]
11. Guo, C.; Chang, C.C.; Qin, C. A hierarchical threshold secret image sharing. *Pattern Recognit. Lett.* **2012**, *33*, 83–91. [CrossRef]
12. Chen, C.C.; Tsai, Y.H. An Expandable Essential Secret Image Sharing Structure. *J. Inf. Hiding Multimed. Signal Process.* **2016**, *7*, 135–144.
13. Chen, W.K.; Chen, H.P.; Tso, H.K. A Friendly and Verifiable Image Sharing Method. *J. Netw. Intell.* **2016**, *1*, 46–51.
14. Zhou, Z.; Yang, C.N.; Cao, Y.; Sun, X. Secret Image Sharing Based on Encrypted Pixels. *IEEE Access* **2018**, *6*, 15021–15025. [CrossRef]
15. Wu, X.; Yang, C.N.; Zhuang, Y.T.; Hsu, S. Improving recovered image quality in secret image sharing by simple modular arithmetic. *Signal Process. Image Commun.* **2018**. [CrossRef]

16. Lin, C.C.; Tsai, W.H. Secret image sharing with steganography and authentication. *J. Syst. Softw.* **2004**, *73*, 405–414. [CrossRef]
17. Lin, S.J.; Lin, J.C. VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. *Pattern Recognit.* **2007**, *40*, 3652–3666. [CrossRef]
18. Li, P.; Ma, P.; Su, X. Image Secret Sharing and Hiding with Authentication. In Proceedings of the First International Conference on Pervasive Computing, Signal Processing and Applications, Harbin, China, 17–19 September 2010; pp. 367–370.
19. Ding, W.; Liu, K.; Yan, X.; Liu, L. *A General (k, n) Threshold Secret Image Sharing Construction Based on Matrix Theory*; Data Science; Springer: Singapore, 2017; pp. 331–340.
20. Zhao, Y.J. The General Structure of Secret Sharing Scheme. *Sci. Technol. Inf.* **2011**, *11*, 144.