Article

A Linear Algebraic Threshold Essential Secret Image Sharing Scheme

Mohammad Ghebleh , Ali Kansa and Abdullah Alazemi

Department of Mathematics, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait; ali.kansa@ku.edu.kw (A.K.); abdullah.alazemi@ku.edu.kw (A.A.)

* Correspondence: mohammad.ghebleh@ku.edu.kw

Abstract: A secret sharing scheme allocates to each participant a share of a secret in such a way that authorized subsets of participants can reconstruct the secret, while shares of unauthorized subsets of participants provide no useful information about the secret. For positive integers r, s, t, n with $r \leq s \leq t \leq n$, an (r, s, t, n) -threshold essential secret sharing scheme is an algorithm that decomposes a secret S into n shares, s of which are essential, in a way that authorized subsets are precisely those with at least t members, at least r of whom are essential. This work proposes a lossless linear algebraic (r, s, t, n) -threshold essential secret image sharing scheme that decomposes the secret, S , into equally-sized shares, each of size $1/t$ the size of S . For each block, B , of S , the scheme assigns to the n participants distinct signature vectors $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ in the vector space $\mathbb{F}_{2^\alpha}^t$, where α is a suitable positive integer, typically between 2 and 5, inclusive. These signature vectors must adhere to some admissibility conditions in order to satisfy the secret sharing threshold properties. The decomposition of B into n shares is obtained by partitioning B into t vectors, then computing the share y_j of the j th participant ($1 \leq j \leq n$), as a linear combination of these parts with coefficients from the signature $\mathbf{v}_j$. The presented simulations showcase the effectiveness and robustness of the proposed scheme against standard statistical and security attacks. They further demonstrate its superiority with respect to existing schemes.

Citation: Ghebleh, M.; Kansa, A.;

Alazemi, A. A Linear Algebraic Threshold Essential Secret Image Sharing Scheme. *Mathematics* **2022**, *10*, 742. <https://doi.org/10.3390/math10050742>

Academic Editor: Angel Martín-del-Rey

Received: 19 January 2022

Accepted: 23 February 2022

Published: 26 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: secret sharing; threshold secret sharing; essential secret sharing; secret image sharing; admissible tracks; chaos

MSC: 94A62, 94A60

1. Introduction

A (t, n) -threshold secret sharing scheme is any approach that decomposes a secret S into n shares such that any collection of at least t shares can reconstruct the secret S , while any collection of less than t shares does not provide any useful information about S . Most existing secret sharing schemes are based on polynomial interpolation [1], hyperplane geometry [2], and the Chinese remainder theorem [3]. In a (t, n) -threshold secret sharing scheme, referred to as a (t, n) -SS scheme, each participant P_i ($1 \leq i \leq n$) receives a share H_i , where all shares enjoy the same importance. Thus, the secret can be recovered when any t participants present their shares. In a (t, n) -SS scheme, no participant has a privilege over another, and any subset consisting of t or more participants is an authorized set for reconstructing the secret, S . However, some applications may require allowing privileged (or essential) participants. For example, in a banking application, a bank manager would be considered an essential participant among a group of bank employees sharing a bank safe password. In such a scenario, a set of participants is authorized to recover the secret whenever it has the required size, and it includes the required number of essential participants. This motivates the definition of an essential secret sharing scheme: if $r \leq s \leq t \leq n$ are positive integers, then an (r, s, t, n) -essential

threshold secret sharing scheme, or an (r, s, t, n) -ESS scheme for short, is any method of decomposing a secret, S , into s essential and $n - s$ non-essential shares, such that any set of at least t shares which contains at least r essential shares is able to reconstruct S ; while any set of shares with fewer than t shares or with fewer than r essential shares is unable to reveal any useful information about S . With n participants, s of whom are essential participants, an (r, s, t, n) -ESS scheme allocates each of the s essential shares to an essential participant and each of the $n - s$ non-essential shares to a non-essential participant.

In the last two decades, the widespread use of digital images has led scientists and engineers in developing secret image sharing techniques for decomposing secret images into shares. In a secret image sharing setting, shares are often referred to as shadow images. A number of (t, n) -threshold secret image sharing schemes based on different techniques such as polynomial interpolation, hyperplane geometry, the Chinese remainder theorem, and matrix theory have been published by researchers [4–18]. Since these schemes do not possess the essentiality condition, all participants have the same importance in the reconstruction phase. However, some applications require the presence of essential participants. Thus, (r, s, t, n) -threshold essential secret image sharing schemes, (r, s, t, n) -ESIS schemes for short, have grasped the attention of researchers [19–24]. However, some of these (r, s, t, n) -ESIS schemes suffer from at least one of the following drawbacks: (i) the non-essential shadow images and essential shadow images are of different sizes; (ii) the concatenation of sub-shadow images. These are reviewed in more detail in the present paper.

In [19,20], the proposed (r, s, t, n) -ESIS schemes are based on polynomial interpolation. Li et al. [21] proposed an (r, s, t, n) -ESIS scheme based on derivative polynomial and Birkhoff interpolation. While this scheme solves the issues of unequal size of shadows and concatenation of sub-shadows in the schemes of [19,20], it generates shadow images of size $1/r$ the size of the secret. Hence, its individual and total shadow sizes are larger than those of [19,20]. In [22], a three-layered structure (r, s, t, n) -ESIS scheme based on the Lagrange interpolation is proposed that can generate equal-sized essential and non-essential shadow images. However, this property is achieved only when the parameters are properly chosen. Li et al. [23] proposed an (r, s, t, n) -ESIS scheme, with $r = s$, while this scheme solves problems such as generating shadow images of different sizes, concatenation of sub-shadows and the use of multiple secret image sharing schemes, the $r = s$ requirement restricts application of this scheme. In [24], an (r, s, t, n) -ESIS scheme using a derivative polynomial is proposed, which generates equally sized shadow images. It also removes the concatenation operation in the sharing phase.

Kanso et al. [25] proposed a lossless linear algebraic (t, n) -SIS scheme, referred to as KGA throughout this work, that for each secret block, B , associates to the i -th participant ($1 \leq i \leq n$) a vector, $\mathbf{v}_i \in \mathbb{F}_{2^\alpha}^t$, where α is a chosen positive integer and $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ must satisfy some admissibility conditions. The vector, $\mathbf{v}_i$, is called the signature of the i -th participant (for the secret block at hand). The i -th share is then constructed as a linear combination of the t vectors from the secret block, B , with coefficients from $\mathbf{v}_i$. In this paper, we extend KGA to propose a lossless (r, s, t, n) -threshold essential secret image sharing scheme. The proposed scheme has the following properties:

- It is a linear algebraic scheme.
- It decomposes the secret S into equally-sized shares each of size $|S|/t$.
- It requires no concatenation in the share generation phase.
- It does not require multiple secret image sharing schemes.

If $P_1, \dots, P_n$ denote the n participants, then we assume without loss of generality that $P_1, \dots, P_s$ are the essential participants and $P_{s+1}, \dots, P_n$ are the non-essential participants; meanwhile, similarly to KGA, the main frame of work in the proposed scheme is to assign a signature vector, v_i , to each participant, P_i , to satisfy the different threshold properties, which now include the essentiality of the shares allocated to $P_1, \dots, P_s$; one needs to modify the admissibility conditions of the signature vectors. More specifically, the essential signatures, $v_1, \dots, v_s$, need to be linearly independent, while the non-essential signatures,

$v_{s+1}, \dots, v_n$, need to span a $(t - r)$ -dimensional space, and every $t - r$ of them must form a basis for this space. In addition to these “threshold” constraints, the signature vectors need to satisfy further conditions that guarantee security of the proposed scheme. These are defined in detail in the following sections.

Simulations demonstrate the efficiency of the proposed scheme. They also show its robustness against well-known statistical and security attacks. Moreover, in comparison with existing schemes, the proposed scheme is shown to have superior performance over existing schemes.

We can summarize the main contributions as follows:

- The proposed ESIS scheme is lossless. Therefore, it can be used for sharing any type of digital content including textual data.
- The scheme does not require multiple secret image sharing schemes.
- It requires no concatenation operation in the sharing phase.
- The scheme generates equally sized and similarly structured shadow images, thus making essential and non-essential shares indistinguishable to an intruder.
- The scheme has a preprocessing phase independent of the secret image. The signatures, $\mathbf{v}_i$, can be generated in advance if the length of S is known. There is a work-around to avoid high storage cost if the signatures are to be computed in advance.
- The proposed scheme is competitive with existing ESIS schemes.

The paper is organized as follows: Section 2 provides a brief description of the KGA scheme [25]. In Section 3, we present a detailed description of the proposed (r, s, t, n) -ESIS scheme. Section 4 is devoted to experimental results and security analysis. In Section 5, we compare the performance of the proposed scheme with existing ones. Some concluding remarks are given in Section 6.

2. Background

KGA is a (t, n) -SIS scheme proposed in [25] which uses admissible matrices with entries in the field $\mathbb{F}_{2^{8\beta}}$, for some positive integer β , to generate shadow images for sharing a secret image. Admissible matrices are defined and studied in [26,27].

Definition 1 ([27]). An $n \times t$ matrix X , where $t \leq n$, is said to be t -admissible if it satisfies the following properties:

- Every $t \times t$ submatrix of X is non-singular.
- Every $(t - 1) \times (t - 1)$ submatrix of X is non-singular.

All computations in KGA are performed in the field $\mathbb{F} = \mathbb{F}_{2^{8\beta}}$ for some chosen positive integer, β . With the number of participants, n , and the threshold, t , known, KGA produces for each secret block, B , an $n \times t$ admissible matrix X , whose rows are assigned to the participants as signature vectors. This step is independent of the secret image. Now, for a given secret image, the first step in KGA is to obtain a matrix representation, Q , in $\mathbb{F}$ of the secret image. To this end, the preprocessing phase concatenates the entries (bytes) of the secret image in groups of β bytes each, to produce 8β -bit values which correspond to elements of $\mathbb{F}$. The secret image is padded if necessary, and shuffled, then reshaped to populate the matrix Q of t rows in a column-first order. Columns of the matrix Q are then divided into groups of m (where m is a parameter) each to form $t \times m$ blocks. Shares are generated for each block, B , as explained in the following, and then block shares of each participant are concatenated and converted back to bytes to produce their shadow image. If $1 \leq i \leq n$, then the i th share of any block, B , of the secret is defined to be the i -th row of the matrix $Y = XB$, where X is an admissible matrix. Therefore, Y constitutes all the shares.

More specifically, given blocks $B_1, B_2, \dots, B_\gamma$, the shadow images of the proposed scheme are obtained using γ -distinct admissible matrices. In [25], admissible matrices are constructed using a 3-dimensional chaotic cat map [28], defined by

$$\mathbf{x}_i = A\mathbf{x}_{i-1} \pmod{1}, \quad (1)$$

where

$$A = \begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix}, \quad (2)$$

with $a_x, a_y, a_z, b_x, b_y, b_z$ being positive integers. Given an initial condition $\mathbf{x}_0$ with entries in $(0, 1)$, iterated applications of Equation (1) generate a sequence $\{\mathbf{x}_i\}_0^\infty = \{(x_i, y_i, z_i)\}_0^\infty$ of 3-tuples with pseudorandom entries in $[0, 1)$.

On the basis of the admissibility condition on the matrices X , the lossless recovery of S is straight forward in the presence of any t shares.

3. The Proposed Scheme

In this work, we extend the KGA (t, n) -SIS scheme to propose an (r, s, t, n) -ESIS scheme. Similarly to KGA, all computations are in the field $\mathbb{F}_q$, where $q = 2^{8\beta}$. We use a fixed correspondence, as follows:

$$i \longleftrightarrow f_i \quad (3)$$

to move between the field $\mathbb{F}_q$ and the group $\mathbb{Z}_q$, where $\mathbb{F}_q = \{f_0, f_1, f_2, \dots, f_{q-1}\}$ with $f_0 = 0$.

The main framework and the preprocessing of the proposed scheme are as in KGA: the shares of a secret block, B , of S are defined to be the rows of the matrix

$$Y = XB,$$

where B represents a block of the secret, X is an admissible matrix, and Y constitutes the shares. To achieve the required essentiality properties, the definition of admissibility (hence the generation of the signatures matrix X) needs to be modified.

Suppose that some rows of Y and their corresponding rows of X are presented in order to recover the secret block, B . Let $\tilde{Y}$ and $\tilde{X}$ denote the submatrices of Y and X consisting of the provided rows. If $\text{rank}(\tilde{X}) = t$, then the linear system $\tilde{Y} = \tilde{X}\tilde{B}$ has a unique solution (note that this system is consistent since $\tilde{B} = B$ is a solution). On the other hand, if $\text{rank}(\tilde{X}) < t$, then this system is under-determined, hence it has infinitely many solutions. This means that we need to design the signature vectors (rows of X) in a way that signature vectors of any unauthorized set of participants for recovery of the secret constitute a submatrix $\tilde{X}$ with rank less than t , while submatrices of X corresponding to authorized sets have rank t . This can be achieved by making sure that the essential signatures $v_1, \dots, v_s$ are linearly independent, while the non-essential signatures $v_{s+1}, \dots, v_n$ span a $(t - r)$ -dimensional space. This means that to obtain a submatrix $\tilde{X}$ of X with rank t , we may use at most $t - r$ non-essential signatures, thus we need at least r essential signatures. To make sure that any $t - r$ non-essential participants can cooperate together with at least r essential participants, we need to also require that every $t - r$ non-essential signature vectors are linearly independent. Moreover, if W_e (respectively, W_{ne}) denotes the subspace of $\mathbb{F}_q^t$ spanned by the essential (respectively non-essential) signature vectors, then we must have $W_e \cap W_{ne} = \{\mathbf{0}\}$ to assure no overlap between essential and non-essential signatures. This is achieved by requiring the vectors $\mathbf{v}_1, \dots, \mathbf{v}_{t-r}$ to be linearly independent.

3.1. The Preprocessing Phase

Let P denote the matrix of intensity values of the secret image. Given the parameters β, t and m , the preprocessing phase of the proposed (r, s, t, n) -ESIS scheme generates blocks of the secret according to Algorithm 1.

Algorithm 1: Preprocessing of the secret image

Data: Matrix P and parameters β, t and m

Result: Blocks $B_1, B_2, \dots, B_\gamma$

- 1 $M_1 \leftarrow$ reshape P into a 1-dimensional array
 - 2 $M_2 \leftarrow$ pad M_1 so that its length equals $\gamma\beta tm$ for some integer γ
 - 3 $M_3 \leftarrow$ shuffle the entries of M_2 using a pseudorandom number generator
 - 4 $M_4 \leftarrow$ concatenate every β consecutive entries of M_3 into a single entry
 - 5 $Q \leftarrow$ reshape M_4 into a $t \times m\gamma$ matrix
 - 6 Partition Q into blocks $B_1, B_2, \dots, B_\gamma$, each of size $t \times m$
 - 7 Return $B_1, B_2, \dots, B_\gamma$
-

3.2. The Construction of Shadow Images

The proposed (r, s, t, n) -ESIS scheme shares each block B_i ($1 \leq i \leq \gamma$), using an admissible matrix X_i . In [25], admissible matrices are generated from the 3-dimensional cat map defined in (1). In this work, we modify the admissible matrix generation algorithm proposed in [25] to satisfy the admissibility properties of the proposed (r, s, t, n) -ESIS scheme. Algorithm 2 presents the procedure for generating admissible matrices. The algorithm generates linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{s+t-r}$ in $\mathbb{F}_q^t$, as in KGA [25]. The first s vectors are associated with the essential participants $P_1, \dots, P_s$, and the remaining $t - r$ vectors are associated with the non-essential participants $P_{s+1}, \dots, P_{s+t-r}$. The scheme then generates $n - (s + t - r)$ vectors $\mathbf{v}_{s+t-r+1}, \dots, \mathbf{v}_n$, as linear combinations of the vectors $\mathbf{v}_{s+1}, \dots, \mathbf{v}_{s+t-r}$, and associates them with the remaining non-essential participants $P_{s+t-r+1}, \dots, P_n$.

Upon generation of the admissible matrices $X_1, X_2, \dots, X_\gamma$, the shadow images can be produced as follows. Given secret blocks, $B_1, B_2, \dots, B_\gamma$, the corresponding share matrices, $Y_1, Y_2, \dots, Y_\gamma$, can be obtained by computing the following:

$$Y_i = X_i B_i, \text{ for } 1 \leq i \leq \gamma.$$

The row vectors of Y_i , namely $\text{row}_1(Y_i), \text{row}_2(Y_i), \dots, \text{row}_n(Y_i)$ constitute the shares corresponding to block B_i . More precisely, each $\text{row}_j(Y_i)$ (for $1 \leq i \leq \gamma$ and $1 \leq j \leq s$) constitutes a share block of the shadow image H_j associated with essential participant P_j , whereas each share $\text{row}_k(Y_i)$ (for $1 \leq i \leq \gamma$ and $s + 1 \leq k \leq n$) constitutes a share block of the shadow image H_k associated with non-essential participant P_j . Algorithm 3 outlines the procedure for generating the shadow images $H_1, H_2, \dots, H_n$.

Algorithm 2: Generation of admissible matrices**Data:** Parameters β, r, s, t, n and m of the scheme**Data:** Cat matrix A and initial state $\mathbf{x}_0$ **Result:** Admissible matrices $X_1, X_2, \dots, X_\gamma$

```

1 for  $i = 1$  to  $\gamma$  do
2    $\rho \leftarrow \left\lceil \frac{t(s+t-r)}{3} \right\rceil$ 
3   for  $j = 1$  to  $\rho$  do
4      $\lfloor \mathbf{x}_j \leftarrow A\mathbf{x}_{j-1} \pmod{1}$ 
5    $\mathbf{x}_0 \leftarrow \mathbf{x}_\rho$ 
6   Arrange entries of  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_\rho$  into a 1-dimensional array  $R$ 
7    $R' \leftarrow \lfloor (q-1)R \rfloor + 1$ 
8   Let  $\Gamma$  be the sequence of elements of  $\mathbb{F}_q$  corresponding, according to
     Equation (3), to elements of  $R'$ 
9   Reshape the first  $t(s+t-r)$  elements of  $\Gamma$  into a  $(s+t-r) \times t$  matrix  $X_{\text{ind}}$ 
10  Denote the row vectors of  $X_{\text{ind}}$  by  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{s+t-r}$ 
11  if  $X_{\text{ind}}$  is  $t$ -admissible then
12    | Go to line 15
13  else
14    | Go to line 3
15   $\delta \leftarrow n - (s+t-r)$ 
16  if  $\delta > 0$  then
17     $\psi \leftarrow \left\lceil \frac{t\delta}{3} \right\rceil$ 
18    for  $j = 1$  to  $\psi$  do
19       $\lfloor \mathbf{x}_j \leftarrow A\mathbf{x}_{j-1} \pmod{1}$ 
20     $\mathbf{x}_0 \leftarrow \mathbf{x}_\psi$ 
21    Arrange entries of  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_\psi$  into a 1-dimensional array  $R$ 
22     $R' \leftarrow \lfloor (q-1)R \rfloor + 1$ 
23    Reshape the first  $\delta(t-r)$  elements of  $\Gamma$  into a  $\delta \times (t-r)$  matrix  $C$ 
24    
$$X_{\text{dep}} \leftarrow C \begin{bmatrix} \mathbf{v}_{s+1} \\ \vdots \\ \mathbf{v}_{s+t-r} \end{bmatrix}$$

25    Append  $X_{\text{dep}}$  to  $X_{\text{ind}}$  to obtain an  $n \times t$  matrix  $X = \begin{bmatrix} X_{\text{ind}} \\ X_{\text{dep}} \end{bmatrix}$ 
26    if every  $t \times t$  submatrix of  $X$  containing at least  $r$  of  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_s$  as row vectors
      is  $t$ -admissible then
27      | Return  $X$ 
28    else
29      | Go to line 18
30   $X_i \leftarrow X$ 
31 End

```

Algorithm 3: Generation of shadow images

Data: Admissible matrices $X_1, X_2, \dots, X_\gamma$
Data: Blocks $B_1, B_2, \dots, B_\gamma$
Result: Shadow images $H_1, H_2, \dots, H_n$

- 1 **for** $i = 1$ **to** γ **do**
- 2 $\lfloor Y_i \leftarrow X_i B_i$
- 3 **for** $j = 1$ **to** n **do**
- 4 $\lfloor H_j$ is a concatenation of $\text{row}_j(Y_1), \text{row}_j(Y_2), \dots, \text{row}_j(Y_\gamma)$
- 5 Convert each element of $H_1, H_2, \dots, H_n$ to an integer via the correspondence of Equation (3)
- 6 Break each integer value of $H_1, H_2, \dots, H_n$ to β bytes
- 7 Shuffle $H_1, H_2, \dots, H_n$ according to some pseudorandom sequences $R^{(1)}, R^{(2)}, \dots, R^{(n)}$, respectively, generated using Equation (1), where each sequence has length $\frac{1}{t}|P|$
- 8 Reshape $H_1, H_2, \dots, H_n$ into rectangular arrays for presentation as images
- 9 Return $H_1, H_2, \dots, H_n$
- 10 **End**

3.3. Reconstruction of the Secret Image

Suppose that t shadow images $H_{i_1}, H_{i_2}, \dots, H_{i_t}$, from which r shadow images are essential, are submitted to a central authority holding the secret key. The procedure for the construction of the secret image is as follows:

- Use the secret key to generate the sequences $R^{(i_1)}, R^{(i_2)}, \dots, R^{(i_t)}$.
- Apply the inverse of the permutations $\pi^{(i_1)}, \pi^{(i_2)}, \dots, \pi^{(i_t)}$, which sort $R^{(i_1)}, R^{(i_2)}, \dots, R^{(i_t)}$, respectively, on $H_{i_1}, H_{i_2}, \dots, H_{i_t}$ to unshuffle them.
- For each sequence resulting from the preceding step, group every β bytes into an integer and convert it to an element in $\mathbb{F}_q$ using Equation (3).
- Divide each resulting sequence into blocks each of length m .
- Construct $t \times m$ matrices $\tilde{Y}_1, \tilde{Y}_2, \dots, \tilde{Y}_\gamma$, where $\text{row}_j(\tilde{Y}_i)$ (for $1 \leq i \leq \gamma$ and $1 \leq j \leq t$) consists of the i -th blocks of the j -th sequence obtained in the preceding step. That is, each $\tilde{Y}_i$ consists of rows $i_1, i_2, \dots, i_t$ of the matrix Y_i generated in Algorithm 3.
- Use the secret key to generate the matrices $X_1, X_2, \dots, X_\gamma$. Let $\tilde{X}_j$ be the $t \times t$ submatrix of X_j , induced by the rows $i_1, i_2, \dots, i_t$.
- Since $\tilde{Y}_j = \tilde{X}_j B_j$ (for $1 \leq j \leq \gamma$), and by the admissibility of X , $\tilde{X}$ is non-singular. Thus, we obtain $B_j = (\tilde{X}_j)^{-1} \tilde{Y}_j$.
- Once all the blocks $B_1, B_2, \dots, B_\gamma$ are obtained, we can reverse Algorithm 1 to obtain the secret image P .

It is evident that if at most $r - 1$ of the t presented shadow images are essential, then from the construction of the admissible matrices $X_1, X_2, \dots, X_\gamma$, the matrices $\tilde{X}_1, \tilde{X}_2, \dots, \tilde{X}_\gamma$ are singular matrices. In such case, the scheme fails to reconstruct the secret image. In Section 4, we investigate the security of the proposed scheme, and analyze the security level of the aforementioned scenario.

The security of the proposed scheme depends on keeping the shadow images secure. The dealer has various means to deliver the shadow images to the intended participant, such as (1) a secure channel, (2) an encryption scheme, and (3) a steganographic scheme.

4. Performance Analysis

This section is devoted to showcase the performance of the proposed (r, s, t, n) -ESIS scheme. We present simulation results to demonstrate robustness of the proposed scheme against statistical and security attacks. In all simulations, we set the number of bytes per

value $\beta = 2$, hence the scheme is tested in the field $\mathbb{F} = \mathbb{F}_{2^{16}}$. For the cat map of Equation (1), we use the coefficient matrix

$$A = \begin{pmatrix} 1124 & 1123 & 3371 \\ 2249 & 2247 & 6745 \\ 1208 & 1207 & 3624 \end{pmatrix}$$

which is obtained by setting $(a_x, a_y, a_z; b_x, b_y, b_z) = (1, 2, 1123; 1207, 1, 2)$. The largest eigenvalue of A is $\lambda \approx 6994.554 \gg 1$, which guarantees the chaotic behavior of the cat map.

We study the performance of the proposed secret image sharing scheme using two standard test images: the 1024×1024 grayscale image Elaine, and the 256×256 color image Lena. Both test images are presented in Figure 1. Further parameters of the tests are presented in Table 1.

Figure 1. The 1024×1024 grayscale secret image Elaine (left) and the 256×256 color secret image Lena (right).

Table 1. Image information and test parameters.

	Elaine	Lena
Color space	Grayscale	RGB color
Image size	1024×1024	256×256
Image size (bytes)	1,048,576	196,608
Block size in $\mathbb{F}$	8192	4096
Number of blocks	64	24
Participants	$n = 6$	$n = 5$
Essential participants	$s = 3$	$s = 2$
Threshold parameters	$(r, t) = (2, 4)$	$(r, t) = (1, 4)$

Figure 2 presents the six shadow images $H_1, \dots, H_6$ corresponding to the image Elaine, each of size 512×512 . The essential shadow images are H_1, H_2 and H_3 , whereas the remaining ones are the non-essential shadow images. Similarly, Figure 3 presents the five RGB shadow images $H'_1, \dots, H'_5$ corresponding to the image Lena, each of size 128×128 . The essential shadow images are H'_1 and H'_2 , whereas the remaining ones are the non-essential shadow images.

One way to deliver the shadow images to the intended participants is using a steganographic scheme, such as that proposed in [29]. Suppose that the host image is the one presented in Figure 4 (left). The stego image carrying the shadow image H_1 presented in Figure 2 is depicted in Figure 4 (right). It is evident that one cannot distinguish between the host image and the stego image (for further details the reader is referred to [29]).

Figure 2. The 512×512 shadow images corresponding to the test image Elaine. (**Top**): the essential shadow images H_1 , H_2 , and H_3 . (**Bottom**): the non-essential shadow images H_4 , H_5 , and H_6 .

Figure 3. The 128×128 color shadow images of test image Lena. (**Top**): the essential shadow images H'_1 and H'_2 . (**Bottom**): the non-essential shadow images H'_3 , H'_4 , and H'_5 .

Figure 4. The 2048×2048 host image (left), and the stego image carrying H_1 (right).

4.1. Statistical Analysis

The proposed (r, s, t, n) -ESIS scheme is an extension of the scheme proposed in [25], where the shadow images are all essential. Therefore, the shadow images are expected to be random-looking [25]. In this section, we present histogram analysis, correlation coefficient analysis, and entropy analysis of shadow images generated by the proposed (r, s, t, n) -ESIS scheme. For further details about these tests, the reader is referred to [25]. Furthermore, we evaluated the randomness of the shadow images using one of the most common used test suites, namely the statistical test suite proposed in [30].

Figure 5 shows that the histograms of sample non-essential shadow image corresponding to the Elaine image and an essential shadow image corresponding to the Lena Image. It is evident that one cannot deduce any useful information about the secret image from the histogram of its corresponding shadow image. The histograms of the other shadow images possess similar behavior—hence, we omit them.

Table 2 presents the correlation coefficients between 10,000 random pairs of adjacent pixels in the horizontal, vertical, and diagonal directions of the test image Elaine and that of the 6 shadow images. On the other hand, Table 3 presents the correlation coefficients between Lena and that of the five shadow images. It can be concluded from the obtained values, which are close to 0, that the shadow images are almost free of any correlation.

Table 2. Correlation coefficients of adjacent pixels in the test image Elaine and the six shadow images.

Image	Elaine	H_1	H_2	H_3	H_4	H_5	H_6
Horizontal	0.994718	0.013446	−0.021501	0.004133	0.012585	0.014317	−0.007293
Vertical	0.993842	−0.006845	0.001816	0.001806	0.013245	0.008771	0.003125
Diagonal	0.989842	−0.006051	0.005808	−0.000033	0.000575	−0.020193	0.012110

Table 3. Correlation coefficients of adjacent pixels in the test image Lena and the five shadow images.

Image	Lena	H'_1	H'_2	H'_3	H'_4	H'_5
Horizontal	0.954979	−0.011065	−0.002971	0.012437	−0.007036	−0.001017
Vertical	0.979244	0.003137	−0.011179	−0.003921	0.017432	−0.005758
Diagonal	0.933190	−0.007111	−0.000770	0.001522	−0.004407	−0.022887

Figure 5. (Top): histogram of a non-essential shadow image of Elaine. (Bottom): histogram of an essential shadow image of Lena.

Tables 4 and 5 display the information entropy measures [31] of each test image and its shadow images. The fact that the resulting measures are close to 8 indicates the unpredictability of the shadow images.

Table 4. Information entropy of the test image Elaine and the six shadow images.

Image	Elaine	H_1	H_2	H_3	H_4	H_5	H_6
Entropy	7.502942	7.999197	7.999369	7.999280	7.999296	7.999258	7.999251

Table 5. Information entropy of the test image Lena and the five shadow images.

Image	Lena	H'_1	H'_2	H'_3	H'_4	H'_5
Entropy	7.730098	7.996312	7.996480	7.996662	7.996500	7.996479

To further evaluate the randomness of the shadow images, we subject the shadow images to the statistical test suite (STS) [30]. For a given secret key, the scheme generates six shadow images for the test image Elaine. We repeat this generation for 15 different initial conditions of the chaotic cat map of Equation (1), resulting in 90 shadow images of the length of 2,097,152 bits each. The STS processes each shadow image as a single binary sequence. The test results presented in Table 6 demonstrate the randomness of the shadow images. For further details about the STS results we refer the reader to [30]). Analysis of 100 similarly generated shadow images of the test image Lena produces similar results, presented in Table 6.

Table 6. Randomness analysis of shadow images using the NIST statistical test suite.

Statistical Test	Elaine (90 Sequences)		Lena (100 Sequences)	
	<i>p</i> -Value	Result	<i>p</i> -Value	Result
Frequency	0.843884	87/90	0.657933	98/100
Block frequency	0.315717	89/90	0.224821	99/100
Cumulative sums (forward)	0.201069	89/90	0.955835	98/100
Cumulative sums (reverse)	0.447593	88/90	0.262249	98/100
Runs	0.003963	90/90	0.514124	96/100
Longest run	0.368773	89/90	0.401199	100/100
Rank	0.299251	89/90	0.779188	99/100
FFT	0.671779	90/90	0.739918	100/100
Non-overlapping template	0.579479	90/90	0.595549	100/100
Overlapping template	0.717488	90/90	0.275709	100/100
Universal	0.511916	87/90	0.779188	97/100
Approximate entropy	0.602458	89/90	0.798139	99/100
Random excursions	0.551026	67/67	0.015065	46/46
Random excursions variant	0.242986	67/67	0.186566	46/46
Serial 1	0.447593	89/90	0.153763	99/100
Serial 2	0.001232	87/90	0.275709	99/100
Linear complexity	0.189397	90/90	0.023545	99/100

In addition to the STS results presented in Table 6, which confirm the randomness of shadow images generated by the proposed (r, s, t, n) -ESIS scheme, we show that there is no similarity between any pair of shadow images. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) [32] are two of the most used measures to analyze similarity between a pair of images. Figure 6 (top) reports the NPCR and UACI measures for all possible pairs $\{H_i, H_j\}$ ($1 \leq i, j \leq 6$) of shadow images corresponding to the test image Elaine, and Figure 6 (bottom) reports the same for all possible pairs $\{H'_i, H'_j\}$ ($1 \leq i, j \leq 5$) of shadow images corresponding to the test image Lena. Each point in Figure 6 corresponds to a pair of NPCR and UACI measures for a pair of shadow images. It is evident that the reported measures are close to the ideal NPCR and UACI measures reported in [32], which are 99.6094% and 33.4635%, respectively. We conclude that the shadow images look random in comparison with each other.

The statistical results demonstrate the excellent randomness properties of the shadow images generated by the proposed (r, s, t, n) -ESIS scheme.

Figure 6. The NPCR and UACI measures of pairs of shadow images. **(Top):** pairs $\{H_i, H_j\}$ corresponding to the test image Elaine. **(Bottom):** pairs $\{H'_i, H'_j\}$ corresponding to the test image Lena.

4.2. Speed

Testing admissibility of the signature matrices X (Algorithm 2) is the bottle-neck of the proposed (r, s, t, n) -ESIS scheme. However, such matrices do not depend on the content of the secret image and can be generated independently of it. Indeed the number of admissible matrices needed for sharing a secret, S , depends on the size of S , but one can generate a large number of signature matrices in advance, and only generate more when needed. On the other hand, to avoid the cost of storing these signature matrices, we can record only the number of times the main for-loop in Algorithm 2 is executed to produce an admissible signature matrix. It is demonstrated in [25] that with probability higher than 99%, the first randomly generated matrix X is indeed admissible. Hence the majority of the stored numbers equal 1, and the list can be compressed if needed.

As an example, with initial condition

$$\mathbf{x}_0 = (0.069900244020546, 0.980562455826779, 0.540757742994215),$$

all admissible matrices for sharing the secret image Elaine are generated in the first attempt. The running time for generating the six shares corresponding to the secret image Elaine, using MATLAB R2016a on a desktop machine with an Intel® Core™ i7-3520 processor and 8 GB of memory running Windows 10, was 0.392514 s.

4.3. Security Analysis

Similar to the scheme proposed in [25], the proposed (r, s, t, n) -ESIS scheme is highly sensitive to its initial conditions and control parameters. Thus, it is highly sensitive to its secret key (for further details please see [25]). The secret key, K , of the proposed (r, s, t, n) -ESIS scheme consists of

- (i) initial conditions and control parameters of the pseudorandom generator used for shuffling the secret image;
- (ii) initial conditions and control parameters of the 3-dimensional cat map used in generation of admissible matrices;
- (iii) initial conditions and control parameters of the pseudorandom generators used to generate the sequences $R^{(1)}, R^{(2)}, \dots, R^{(n)}$.

Note that when the 3-dimensional cat map of Equation (1) is used as the pseudorandom generator, the initial conditions, $\mathbf{x}_0$, consist of three double-precision real numbers and the control parameters, $a_x, a_y, a_z, b_x, b_y, b_z$, are six integers. In this case, only the initial conditions of the maps used for (i) and (ii) above contribute six double-precision numbers to K . Thus, with a 64-bit double precision of 10^{-14} , the size of the key space of K is at least $(10^{14})^6 > 2^{279}$, which is large enough to render exhaustive search attacks impractical.

To assess the security of reconstruction of the secret, let us assume that $r - 1$ essential shares are present. This unauthorized set cannot derive any useful information about the secret image. It is shown in [25], that the probability for recovering a single secret block of the secret image is about $(1/q)^{t^2+m}$, where $q = 2^{16}$ and tm is the block size of the secret. When $m > 100$ this attack is impractical. Furthermore, if $t - 1$ shares are present, r from which are essential shares, then once again no useful information can be derived about the secret image. The probability for recovering a single secret block of the secret image is about $(1/q)^{t^2+m}$.

4.4. Error-Resilient Capability

The error-resilient capability of the proposed (r, s, t, n) -ESIS scheme follows from that in [25]. Figure 7 depicts the recovered (filtered) test images of Elaine obtained from an authorized set of four shadow images one of which is (i) cropped by 25% (left), and (ii) subjected to salt and pepper noise with ratio 0.2 (right).

Figure 7. The recovered test image Elaine obtained from an authorized set of four shadow images one of which is (i) cropped by 25% (left), and (ii) subjected to salt and pepper noise with ratio 0.2 (right).

5. Comparison with Existing Work

This section shows the performance of the proposed (r, s, t, n) -ESIS scheme with respect to some existing ones, such as those presented in [20–22,24,33,34]. A number of (r, s, t, n) -ESIS schemes have drawbacks caused by (i) generation of unequal-sized shadow images, and (ii) concatenation of sub-shadow images. These drawbacks result in security vulnerability and complication in the reconstruction of the secret image. Hence it is important for an (r, s, t, n) -ESIS scheme to overcome these drawbacks. In Table 7, we give a summary of the schemes under comparison with respect to these drawbacks. Some of the

schemes that overcome these drawbacks are further compared in terms of size of shadow images in Table 8. This table also reports whether the secret image is reconstructed with no distortion.

Table 7. Comparison in terms of essential and non-essential shadow images sizes, and concatenation of sub-shadow images.

Scheme	Equal-Sized Shadow Images	Concatenation of Sub-Shadows
[20]	No	Yes
[33]	No	Yes
[21]	Yes	No
[34]	Yes	No
[22]	Yes	Yes
[24]	Yes	No
Proposed scheme	Yes	No

Table 8. Size of shadow images, and the quality of the reconstructed secret image.

Scheme	Size of Shadow Images	Lossless
[21]	L/r	No
[34]	L/r	No
[24]	L/t	Yes
Proposed scheme	L/t	Yes

On the basis of the reported results, the superiority of the proposed scheme over existing schemes is evident.

6. Concluding Remarks

This work proposes a lossless linear algebraic (r, s, t, n) -threshold essential secret image sharing scheme that generates equally-sized shadow images, each of size L/t , where L is the length of the given secret image, S . For sharing a block of the secret, the proposed scheme associates distinct admissible signature vectors in the vector space, $\mathbb{F}_{2^n}^t$, to the essential participants and non-essential participants. Simulations demonstrate the effectiveness and robustness of the proposed scheme against standard statistical and security attacks. Furthermore, they show its superiority in comparison with existing schemes.

Author Contributions: Conceptualization, M.G., A.K. and A.A.; Formal analysis, M.G., A.K. and A.A.; Methodology, M.G., A.K. and A.A.; Software, M.G., A.K. and A.A.; Writing—original draft, A.K.; Writing—review—editing, M.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are thankful to the anonymous referees for their helpful comments.

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

References

- Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [\[CrossRef\]](#)
- Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the IEEE 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; pp. 313–318.

3. Mignotte, M. How to share a secret. In *Workshop on Cryptography*; Springer: Berlin/Heidelberg, Germany, 1982; pp. 371–375.
4. Thien, C.-C.; Lin, J.-C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [[CrossRef](#)]
5. Lin, C.-C.; Tsai, W.-H. Secret image sharing with steganography and authentication. *J. Syst. Softw.* **2004**, *73*, 405–414. [[CrossRef](#)]
6. Bai, L. A reliable (k, n) image secret sharing scheme. In Proceedings of the 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, USA, 29 September–1 October 2006; pp. 31–36.
7. del Rey, A.M. A matrix-based secret sharing scheme for images. In *Iberoamerican Congress on Pattern Recognition*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 635–642.
8. Ulutas, M.; Nabiye, V.V.; Ulutas, G. Improvements in geometry-based secret image sharing approach with steganography. *Math. Probl. Eng.* **2009**, *2009*, 187874. [[CrossRef](#)]
9. Hu, W.-T.; Li, M.-C.; Guo, C.; Ren, Y.-Z. Reversible secret image sharing with steganography and dynamic embedding. *Secur. Commun. Netw.* **2012**, *5*, 1267–1276. [[CrossRef](#)]
10. El-Latif, A.A.A.; Yan, X.; Li, L.; Wang, N.; Peng, J.-L.; Niu, X. A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption. *Opt. Laser Technol.* **2013**, *54*, 389–400. [[CrossRef](#)]
11. Wu, K.-S. A secret image sharing scheme for light images. *EURASIP J. Adv. Signal Process.* **2013**, *2013*, 49. [[CrossRef](#)]
12. Zarepour-Ahmadabadi, J.; Ahmadabadi, M.S.; Latif, A. An adaptive secret image sharing with a new bitwise steganographic property. *Inf. Sci.* **2016**, *369*, 467–480. [[CrossRef](#)]
13. Kalso, A.; Ghebleh, M. An efficient (t, n) -threshold secret image sharing scheme. *Multimed. Tools Appl.* **2017**, *76*, 16369–16388. [[CrossRef](#)]
14. Deng, X.; Wen, W.; Shi, Z. Threshold multi-secret sharing scheme based on phase-shifting interferometry. *Opt. Commun.* **2017**, *387*, 409–414. [[CrossRef](#)]
15. Kabirirad, S.; Eslami, Z. A (t, n) -multi secret image sharing scheme based on boolean operations. *J. Vis. Commun. Image Represent.* **2018**, *57*, 39–47. [[CrossRef](#)]
16. Ghebleh, M.; Kalso, A. A novel secret image sharing scheme using large primes. *Multimed. Tools Appl.* **2018**, *77*, 11903–11923. [[CrossRef](#)]
17. Ding, W.; Liu, K.; Yan, X.; Wang, H.; Liu, L.; Gong, Q. An image secret sharing method based on matrix theory. *Symmetry* **2018**, *10*, 530. [[CrossRef](#)]
18. Kalso, A.; Ghebleh, M. An efficient lossless secret sharing scheme for medical images. *J. Vis. Commun. Image Represent.* **2018**, *56*, 245–255. [[CrossRef](#)]
19. 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](#)]
20. Yang, C.-N.; Li, P.; Wu, C.-C.; Cai, S.-R. Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach. *Signal Process. Image Commun.* **2015**, *31*, 1–9. [[CrossRef](#)]
21. Li, P.; Yang, C.-N.; Zhou, Z. Essential secret image sharing scheme with the same size of shadows. *Digit. Signal Process.* **2016**, *50*, 51–60. [[CrossRef](#)]
22. Chen, C.-C. Essential secret image sharing scheme with equal-sized shadows generation. *J. Vis. Commun. Image Represent.* **2018**, *52*, 143–150. [[CrossRef](#)]
23. Li, P.; Liu, Z.; Yang, C.-N. A construction method of (t, k, n) -essential secret image sharing scheme. *Signal Process. Image Commun.* **2018**, *65*, 210–220. [[CrossRef](#)]
24. Wu, Z.; Liu, Y.-N.; Wang, D.; Yang, C.-N. An efficient essential secret image sharing scheme using derivative polynomial. *Symmetry* **2019**, *11*, 69. [[CrossRef](#)]
25. Kalso, A.; Ghebleh, M.; Alazemi, A. A lossless linear algebraic secret image sharing scheme. *Informatica* **2020**, *31*, 499–522. [[CrossRef](#)]
26. Schinzel, A.; Spiež, S.; Urbanowicz, J. Admissible tracks in shamir's scheme. *Finite Fields Their Appl.* **2010**, *16*, 449–462. [[CrossRef](#)]
27. Spiež, S.; Srebrny, M.; Urbanowicz, J. Remarks on the classical threshold secret sharing schemes. *Fundam. Inform.* **2012**, *114*, 345–357. [[CrossRef](#)]
28. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [[CrossRef](#)]
29. Ghebleh, M.; Kalso, A. A robust chaotic algorithm for digital image steganography. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 1898–1907. [[CrossRef](#)]
30. Bassham, L.E., III; Rukhin, A.L.; Soto, J.; Nechvatal, J.R.; Smid, M.E.; Barker, E.B.; Leigh, S.D.; Levenson, M.; Vangel, M.; Banks, D.L.; et al. *Sp 800-22 rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; 2010. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf> (accessed date: 18 January 2022)
31. Shannon, C.E. Prediction and entropy of printed English. *Bell Syst. Tech. J.* **1951**, *30*, 50–64. [[CrossRef](#)]
32. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT)* **2011**, *1*, 31–38.
33. Chen, C.-C.; Chen, S.-C. Two-layered structure for optimally essential secret image sharing scheme. *J. Vis. Commun. Image Represent.* **2016**, *38*, 595–601. [[CrossRef](#)]
34. Chen, C.-C.; Tsai, Y.-H. An expandable essential secret image sharing structure. *J. Inf. Hiding Multimed. Signal Process* **2016**, *7*, 135–144.