RESEARCH ARTICLE

A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes

Dong Xie^{1,2,3}, Lixiang Li^{1,3*}, Haipeng Peng^{1,3}, Yixian Yang^{1,3,4}

1 Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China, **2** School of Mathematics and Computer Science, Anhui Normal University, Wuhu, 241000, China, **3** National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing, 100876, China, **4** State Key Laboratory of Public Big Data, Guizhou, 550025, China

* lixiang@bupt.edu.cn

Abstract

In a general (k, n) scalable secret image sharing (SSIS) scheme, the secret image is shared by n participants and any k or more than k participants have the ability to reconstruct it. The scalability means that the amount of information in the reconstructed image scales in proportion to the number of the participants. In most existing SSIS schemes, the size of each image shadow is relatively large and the dealer does not have a flexible control strategy to adjust it to meet the demand of different applications. Besides, almost all existing SSIS schemes are not applicable under noise circumstances. To address these deficiencies, in this paper we present a novel SSIS scheme based on a brand-new technique, called compressed sensing, which has been widely used in many fields such as image processing, wireless communication and medical imaging. Our scheme has the property of flexibility, which means that the dealer can achieve a compromise between the size of each shadow and the quality of the reconstructed image. In addition, our scheme has many other advantages, including smooth scalability, noise-resilient capability, and high security. The experimental results and the comparison with similar works demonstrate the feasibility and superiority of our scheme.

OPEN ACCESS

Citation: Xie D, Li L, Peng H, Yang Y (2017) A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes. PLoS ONE 12 (1): e0168674. doi:10.1371/journal.pone.0168674

Editor: Yeng-Tseng Wang, Kaohsiung Medical University, TAIWAN

Received: May 17, 2016

Accepted: December 1, 2016

Published: January 10, 2017

Copyright: © 2017 Xie et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All relevant data are within the paper.

Funding: This paper is supported by the National Key Research and Development Program of China (Grant no. 2016YFB0800602), the National Natural Science Foundation of China (Grant nos. 61472045 and 61573067), the Beijing City Board of Education Science and Technology Key Project (Grant nos. KZ201510015015 and KM201510015009).

Competing Interests: The authors have declared that no competing interests exist.

Introduction

To safeguard cryptographic keys, Shamir [1] and Blakley [2] presented a novel method for constructing secure and robust key management schemes, called secret sharing (SS), which can overcome many vulnerabilities when one possesses a single master key for a certain cryptosystem. From a cryptographic perspective, SS scheme refers to some methods for distributing a secret among a group of participants and each one in the group is allocated a share or shadow of the secret. The secret can be reconstructed only when a sufficient number of shadows are combined together and individual shadow serves no useful purpose for obtaining it. As a secure and fault-tolerant technique, SS has been widely used in many fields, such as distributed storage system, secure multiparty computation, and electronic voting [3, 4]. In Shamir's (k, n) ($2 \leq k \leq n$) threshold SS scheme [1], the secret is divided into n shadows and any k

of them can reconstruct the whole original secret. However, any less than k shadows cannot obtain any information about the secret. Although this construction method is information theoretically secure, each participant requires relatively large storage space because the size of each shadow is equal to that of the secret data. Therefore, using Shamir's SS scheme will result in huge communication burden when we share image or video data at the pixel level. In fact, the topic of designing SS scheme for image data has attracted wide attention in the past fifteen years.

In 2002, Thien and Lin [5] proposed a (k, n) secret image sharing (SIS) scheme based on Shamir's (k, n) threshold SS scheme. In their scheme, the dealer first generates a $k - 1$ degree polynomial by letting the k coefficients be the gray values of k pixels in the image and then computes the corresponding shadow for each participant according to the polynomial. In fact, the main difference between their method and Shamir's scheme is that they use no random coefficient. In 2004, Lin and Tsai [6] proposed a SIS scheme with the additional capabilities of steganography and authentication. Unfortunately, dishonest participants in their scheme can easily manipulate the stego-image for successful authentication but cannot recover the secret image. Subsequently, Yang et al. [7] presented an improved scheme to enhance authentication ability that prevents dishonest participants from cheating. In 2010, Alharthi and Atrey [8] specifically analyzed the SIS scheme presented by Thien and Lin [5], and proposed an improved scheme for secure image sharing. In addition, there are some other related research results about this topic in recent years, e.g., [9–11].

In a (k, n) threshold SIS scheme, the secret image can be completely reconstructed if more than k shadows are available and any $k - 1$ or less shadows reveal no information about the image. However, this type of reconstruction policy that reveals either the entire image or nothing limits its possible applications. In some circumstances, it may require the secret image to be gradually reconstructed, which means that the clarity or quality of the reconstructed image depend on the number or characteristics of shadows participating in the reconstruction process. To this end, Wang and Shyu [12] first proposed the concept of scalable secret image sharing (SSIS), where single shadow reveals no information about the secret image and any $k(2 \leq k \leq n)$ shadows can reconstruct the secret image in a scalable manner. In their scheme, the secret image is first divided into n disjoint sub images and generate two sub-share images using Thein and Lin's (2,2)-SIS scheme. Then the sub-share images are encoded to produce shadow images. The main drawback of their proposed scheme is that the threshold value k is limited to 2. In 2010, Yang and Huang generalized Wang and Shyu's $(2, n)$ -SSIS scheme and proposed a general (k, n) -SSIS scheme [13]. Subsequently, Yang and Chu [14] presented a (k, n) -SSIS scheme with the smooth scalability, which means that the information amount of reconstructed image is "smoothly" proportional to the number of shadows used in reconstruction. To put it another way, the more the number of available shadows, the better the quality of the reconstructed image. In 2015, Liu et al. introduced a lossy SSIS method for color images [15], which has relatively small shadow size and also achieved good noise-resilient capability. In the same year, Lee and Chen developed a new method for constructing SSIS schemes based on the Salient map [16], in which the region of interesting of the secret image can be revealed progressively.

From a high-level perspective, the reconstruction phase in Shamir-type (k, n) -SIS schemes [1, 5, 8, 12] can be regarded as the process of solving the secret image $\mathbf{I}$ from $\mathbf{Y} = \mathbf{A}\mathbf{I}$ generated by the available shadows of participants, where $\mathbf{A} \in \mathbb{R}^{k_1 \times k}$ is the known Vandermonde coefficient matrix and k_1 denotes the number of available participants. As long as k_1 is not smaller than k , the reconstruction can be performed by solving the aforementioned linear equations because the determinant of $\mathbf{A}$ is not equal to 0. Previous studies indicate that a natural image

has high correlativity between pixels in one local region and it can be represented using only a few non-zero coefficients in a suitable basis or dictionary [17, 18]. However, to the best of our knowledge, almost all previous SIS schemes do not take full advantage of this sparsity, which may play an important role in reducing the size of each shadow.

In this paper, we present a secure and efficient (k, n) -SISS with flexible shadow sizes based on compressed sensing (CS) [19–21], which has attracted considerable attention over the last ten years because it can reconstruct sparse signals using a very few measurements. Employing the sparsity of image data, we can reconstruct the secret image $\mathbf{I}$ from relatively short available shadows. To reduce the size of each participant's shadow as much as possible, we first sparsify the secret image and then compress it by chaotic sensing matrix in CS. After that, the obtained image is cut in a right-to-left fashion using a parameter λ which controls the size of each shadow. Subsequently, we divide the downsized image into n equal parts and perform two nonlinear operations on each part, including permutation and diffusion. Hence all shadows of the secret image $\mathbf{I}$ are formed. Roughly speaking, our proposed scheme in fact consists of two major steps, linear transformations (CS and downsizing) and nonlinear operations (permutation and diffusion). The linear procedures are used for decreasing the size of each participant's shadow, and the nonlinear operations are used for improving security. In general, the advantages of our scheme can be summarized as follows:

- *High security.* The key space in our original scheme is large enough to make brute-force attacks infeasible and it can also resist ciphertext-only attack and known-plaintext attack. In addition, the generated shadows have small correlation coefficients of adjacent pixels because of linear transformations and nonlinear operations. Therefore, our construction provides a high-level security.
- *High efficiency.* In our scheme, the dealer needs to perform two important procedures, i.e., compression and downsizing. These two procedures play an important role in reducing the size of each shadow. The experimental results indicate the superiority of our scheme.
- *Noise-resilient capability.* In the real-world applications, noise exists everywhere. Unfortunately, most existing SSIS schemes are not applicable under noise circumstances. With the help of CS, our SSIS scheme can still work when there exist some types of noise in the communication channel.
- *Flexibility.* To the best of our knowledge, our proposed scheme is the first SSIS scheme with flexible shadows. The size of each shadow in our scheme can be controlled by a parameter. Thus it achieves a compromise between the size of each shadow and the quality of the reconstructed image.

The rest of this paper is organized as follows. Section 2 recalls some basic background, including Shamir's (k, n) -SS scheme and CS. We describe our main idea in Section 3 and introduce our proposed scheme explicitly in Section 4. The experimental results and security analysis will be shown in Section 5. The comparison with similar works is described in Section 6. Finally, we conclude this paper in Section 7.

1 Background Knowledge

For any positive integer n , $[n]$ denotes the set $\{1, 2, \dots, n\}$. Throughout this paper, all vectors are assumed to be in column form and are written using bold lower-case letters (e.g. $\mathbf{a}$). We use bold capital-case letters (e.g. $\mathbf{A}$) to represent matrices. For a matrix $\mathbf{A}$, the vectorization of $\mathbf{A}$, denoted by $\text{vec}(\mathbf{A})$, is a long column vector obtained by stacking the columns of $\mathbf{A}$ on top of one another. Given two functions f and g defined on some subset of the real numbers, $f(x) = 0$

$(g(x))$ if and only if there is a positive constant C and a real number x_0 such that $|f(x)| \leq C|g(x)|$ for all $x \geq x_0$.

1.1 Shamir's (k, n) -SS scheme

Based on polynomial interpolation, Shamir presented a (k, n) -SS scheme [1] in 1979, which has been widely used in various practical applications. In his scheme, the dealer shares a secret a_0 into n parts for n participants by computing a random $k - 1$ degree polynomial. The reconstruction phase requires at least k participants and with even $k - 1$ or less, recovery is impossible. In detail, the dealer first chooses a large prime number p ($p > a_0$) and $k - 1$ integers $\{a_i\}_{i \in [k-1]}$ such that each integer is smaller than p . Therefore, the random $k - 1$ degree polynomial is formed as:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} \mod p. \quad (1)$$

The dealer then computes the i -th shadow $y_i = f(i)$ for the i -th participant, where $1 \leq i \leq n$. Using Lagrange interpolation, any k or more than k shadows can reconstruct the secret a_0 through

$$a_0 = f(0) = \sum_{i=1}^k y_i \prod_{j=1, j \neq i}^k \frac{-j}{i-j} \mod p. \quad (2)$$

1.2 Compressed Sensing

The theory of CS [19–22] breaks the limitation of Nyquist-Shannon sampling theorem because it can reconstruct sparse signals using a very few measurements. It has attracted considerable attention and been widely used in many fields such as image processing, wireless communication, medical imaging, and identification problem [23]. The standard model of CS is an under-determined linear system defined as follows,

$$\mathbf{y} = \mathbf{A}\mathbf{x}, \quad (3)$$

where $\mathbf{A} \in \mathbb{R}^{M \times N}$, $\mathbf{x} \in \mathbb{R}^N$, $\mathbf{y} \in \mathbb{R}^M$ and $M < N$. From a signal processing perspective, $\mathbf{A}$, $\mathbf{x}$ and $\mathbf{y}$, respectively, represent the sensing matrix, the signal vector, and the compressed measurements.

To recover the original signal $\mathbf{x}$ from the compressed measurements $\mathbf{y}$, it requires that $\mathbf{x}$ is sparse and the sensing matrix $\mathbf{A}$ must satisfy some special properties. We say a vector $\mathbf{x}$ is s -sparse if it has at most s non-zero entries. Previous studies showed that if the sensing matrix $\mathbf{A}$ satisfies the Restricted Isometry Property (RIP) [19–21], then the sparse signal $\mathbf{x}$ can be exactly recovered with overwhelming probability. Next, we will recall the condition for uniqueness of sparse solutions to Eq (3) and the definition of the RIP.

Definition 1 ([19]) The spark of a given matrix $\mathbf{A}$ is the smallest number of columns of $\mathbf{A}$ that are linearly dependent.

Lemma 1 ([24]) For any vector $\mathbf{y} \in \mathbb{R}^M$, there exists at most one s -sparse signal $\mathbf{x}$ such that $\mathbf{y} = \mathbf{A}\mathbf{x}$ if and only if $\text{spark}(\mathbf{A}) > 2s$.

Definition 2 A matrix $\mathbf{A}$ satisfies the restricted isometry property (RIP) of order s if there exists a $\delta_s \in (0, 1)$ such that

$$(1 - \delta_s) \|\mathbf{v}\|_2^2 \leq \|\mathbf{A}\mathbf{v}\|_2^2 \leq (1 + \delta_s) \|\mathbf{v}\|_2^2, \quad (4)$$

holds for all s -sparse vectors $\mathbf{v}$.

Given the sensing matrix $\mathbf{A}$, there are a great variety of algorithms to recover the original signal $\mathbf{x}$ efficiently, such as the classical greedy Orthogonal Matching Pursuit (OMP) algorithm [25] and l_1 optimization algorithm [26]. We use the OMP algorithm in our experiments.

To reduce storage space of sensing matrices, Yu et al. [27] proposed a novel method for constructing sensing matrices using chaotic (logistic map) sequences, and also proved that it satisfy the RIP with overwhelming probability if the sparsity $s \leq O(M / \log(N/s))$. However, the probability density function of logistic map does not follow the uniform distribution in the interval $(0, 1)$. In order to enhance the security, it is necessary to select a chaotic map which can produce pseudo random sequences. Frunzete et al. [28] proposed to construct sensing matrices using the one-dimensional skew tent map, whose probability density function follows the uniform distribution. Specifically, the skew tent map with parameter μ is given by

$$z(n+1) = \begin{cases} \frac{z(n)}{\mu} & 0 < z(n) < \mu \\ \frac{1-z(n)}{1-\mu} & \mu \leq z(n) < 1 \end{cases}, \quad (5)$$

where $z(0) \in (0, 1)$ is the initial value and $\mu \in (0, 1)$ is a parameter.

Lemma 2 ([27, 28]) *Chaotic sensing matrix $\mathbf{A} \in \mathbb{R}^{M \times N}$ constructed by the logistic map or the skew tent map satisfies the RIP for constant $\delta_s > 0$ with overwhelming probability providing that $s \leq O(M / \log(N/s))$.*

2 Main idea

All arithmetic operations in Shamir's (k, n) -SS scheme [1] are performed over the finite field $\mathbb{Z}_p^*$. Naturally, the proposed method can be directly extended to the real number field $\mathbb{R}$. We assume that these two cases are not to be distinguished throughout this paper. For $i = 1, \dots, n$, let P_i denote the i -th participant. From a linear algebra point of view, the sharing phase can be viewed as a problem of computing the following linear equations:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & 2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & k & \dots & k^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \dots & n^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \\ \vdots \\ y_n \end{pmatrix}. \quad (6)$$

Support that the k participants $\{P_{i_j}\}_{j \in [k]}$ want to reconstruct the secret a_0 , then the reconstruction phase can be viewed as a problem of solving the following linear equations:

$$\begin{pmatrix} 1 & i_1^1 & \dots & i_1^{k-1} \\ 1 & i_2^1 & \dots & i_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i_k^1 & \dots & i_k^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_k} \end{pmatrix}. \quad (7)$$

$$\text{Let } \mathbf{A} = \begin{pmatrix} 1 & i_1^1 & \cdots & i_1^{k-1} \\ 1 & i_2^1 & \cdots & i_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i_k^1 & \cdots & i_k^{k-1} \end{pmatrix}, \mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix}, \text{ and } \mathbf{y} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_k} \end{pmatrix}. \text{ Note that } \mathbf{A} \text{ is a } k \times k \text{ Van-}$$

dermonde matrix and its determinant is not equal to 0. Thus the vector $\mathbf{a}$ containing the secret a_0 can be obtained from the vector $\mathbf{y}$, which is formed by k shadows $\{y_{i_j}\}_{j \in [k]}$. This method is not suitable for sharing image data at the pixel level because the size of each shadow is at least the same as the size of the secret image. To overcome this disadvantage, Thien and Lin introduced a variant [5], where the gray values of k pixels in the secret image are set to all entries of $\mathbf{a}$. Therefore the size of each shadow can be reduced by a factor of k .

From Eqs (3) and (7), we can see that the model of CS is very similar to that of Shamir-type (k, n) -SIS schemes. It is worth mentioning that CS possesses the characteristic of compression, but Shamir-type schemes do not. Thus, we try to use CS to replace the method of Shamir-type schemes for sharing secret images. In fact, the compression and sensing process in CS can be regarded as the sharing and reconstruction phase in (k, n) -SIS schemes respectively. Fortunately, some image data can be represented using only a few non-zero coefficients in a suitable basis or dictionary [17, 18]. That is, the coefficient vector $\mathbf{a}$ can be viewed as a sparse vector. This meets the sparsity condition in CS. However, the formed coefficient matrix $\mathbf{A}$ is a Vandermonde matrix and it can not be used as a sensing matrix because the recovery process of CS is numerically unstable [29]. In CS, some chaotic systems can be used to produce sensing matrices because the sensing device only requires to store some private initial values. More importantly, Lemma 2 shows that sensing matrix $\mathbf{A}$ constructed by the logistic map or the skew tent map satisfies the RIP with overwhelming probability providing that $s \leq O(M / \log(M/s))$. Therefore, the dealer can use a chaotic system to produce a lower dimensional matrix $\mathbf{A}$ and compress the secret image. It is not hard to see that the reconstruction phase can be performed evidently using some reconstruction algorithms in CS. To improve the security of our scheme, we need two additional nonlinear transformations, including permutation and diffusion. The experimental results and the comparison with similar works indicate the feasibility and potential superiority of our scheme.

3 Our Proposed Scheme

In this section, we will describe our proposed SSIS scheme in detail. Fig 1 shows the schematic diagram of the proposed method. Similar to some previous related schemes, we assume that there is a trusted key distribution center in our scheme, which distributes private keys k_1, k_2 and k_3 for the dealer and the n participants over a secure channel. This section consists of three parts: the secret image sharing phase, the image reconstruction phase and several theoretical results.

3.1 The secret image sharing phase

Suppose that the dealer wants to divide the secret image $\mathbf{I} \in \{0, 255\}^{N \times N}$ into n smaller shadows $\mathbf{I}_1, \dots, \mathbf{I}_n$. Now we describe the secret image sharing phase of our SSIS scheme as follows:

1. *Sparsification*. Choose the discrete wavelet transformation (DWT) to represent the secret image $\mathbf{I}$ and obtain the corresponding sparse matrix $\mathbf{X} \in \mathbb{R}^{N \times N}$, i.e., $\mathbf{X} = \Phi \mathbf{I} \Phi^T$, where Φ is the N -dimensional orthogonal DWT matrix.

Fig 1. Schematic diagram of our proposed scheme.

doi:10.1371/journal.pone.0168674.g001

2. *Compression.* Based on the construction method for sensing matrices [28], generate the sensing matrix $\mathbf{A} \in \mathbb{R}^{M \times N}$ using the private key $k_1 = (z^1(0), \mu_1)$, where M is a multiple of n . Then compress the matrix $\mathbf{X}$ and obtain $\mathbf{Y} \in \mathbb{R}^{M \times N}$, i.e., $\mathbf{Y} = \mathbf{A}\mathbf{X}$.
3. *Downsizing.* To reduce the size of each shadow, cut $\mathbf{Y}$ in a right-to-left fashion through a control parameter $\lambda \in (0, 1]$ such that $\lambda N \in \mathbb{Z}$ and obtain a tailored matrix $\mathbf{Z} \in \mathbb{R}^{M \times \lambda N}$.

$$\mathbf{Y} = \begin{pmatrix} y_{1,1} & \cdots & y_{1,\lambda N} & \cdots & y_{1,N} \\ y_{2,1} & \cdots & y_{2,\lambda N} & \cdots & y_{2,N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ y_{M,1} & \cdots & y_{M,\lambda N} & \cdots & y_{M,N} \end{pmatrix} \xrightarrow{\text{downsizing}} \mathbf{Z} = \begin{pmatrix} y_{1,1} & \cdots & y_{1,\lambda N} \\ y_{2,1} & \cdots & y_{2,\lambda N} \\ \vdots & \vdots & \vdots \\ y_{M,1} & \cdots & y_{M,\lambda N} \end{pmatrix}. \quad (8)$$

4. *Splitting.* Split $\mathbf{Z}$ into n matrices $\{\mathbf{Z}_i\}_{i \in [n]}$ with the same size, i.e.,

$$\mathbf{Z} = \begin{pmatrix} \mathbf{Z}_1 \\ \vdots \\ \mathbf{Z}_n \end{pmatrix}, \quad (9)$$

where $\mathbf{Z}_i \in \mathbb{R}^{M/n \times \lambda N}$.

5. *Permutation.* In order to improve the security, the permutation method proposed by Wang et al. [30] has been widely used in some image encryption systems. Here we use a slight variant to perform this step.
 - a. Use the private key $k_2 = (z^2(0), \mu_2)$ to iterate the skew tent map $m + \lambda MN/n$ times and discard the first m values to obtain the sequence $\{z(i)\}_{i=m+1}^{m+\lambda MN/n}$. Note that the reason we discard the first m values is the transient effect.
 - b. Sort the remaining $\lambda MN/n$ values to obtain a new sequence $\{\tilde{z}(i)\}_{i=m+1}^{m+\lambda MN/n}$.
 - c. Search the values of $\{z(i)\}_{i=m+1}^{m+\lambda MN/n}$ in $\{\tilde{z}(i)\}_{i=m+1}^{m+\lambda MN/n}$, and form the corresponding indices $\{Ind(i)\}_{i=1}^{\lambda MN/n}$.
 - d. Perform the permutation procedure according to the indices $\{Ind(i)\}_{i=1}^{\lambda MN/n}$. For each i , let $\mathbf{q}_i = \text{vec}(\mathbf{Z}_i)$ and

$$\mathbf{q}_i^* = \begin{pmatrix} \mathbf{q}_i(Ind(1)) \\ \vdots \\ \mathbf{q}_i\left(Ind\left(\frac{\lambda MN}{n}\right)\right) \end{pmatrix} \in \mathbb{R}^{\frac{\lambda MN}{n}}. \quad (10)$$

Reshape $\mathbf{q}_i^*$ (i.e., anti-vectorization operation) and obtain $\mathbf{Z}_i^* \in \mathbb{R}^{M/n \times \lambda N}$.

6. *Diffusion.* Since permutation cannot change the statistical properties of the image, we need this step to resist some statistical attacks.
 - a. Use the private key $k_3 = (z^3(0), \mu_3)$ to produce a sequence with $m + \lambda MN/n$ values using the skew tent map and then discard the first m values.
 - b. Reshape the remaining $\lambda MN/n$ values and obtain a matrix $\mathbf{R} \in \mathbb{R}^{M/n \times \lambda N}$.
 - c. Compute $\mathbf{R}^* = 10^{15} \cdot \mathbf{R} \bmod 256$ and $\mathbf{I}_i = \mathbf{Z}_i^* + \mathbf{R}^*$ for each i .
7. *Transmission.* Each image shadow $\mathbf{I}_i$ is distributed to the i -th participant P_i .

Remark 1 Although CS is a simple linear transformation, we can view it as a symmetric encryption system whose private key is the sensing matrix. The security properties of this model have been studied in recent years, and the results show that it can provide computational security and resist some cryptographic attacks. In order to further improve the security of our scheme, we add two additional nonlinear steps, permutation and diffusion, which are widely used in classical image encryption schemes.

Remark 2 In order to reduce the size of each shadow, we cut the compressed measurements $\mathbf{Y}$ and take the left part of it through a control parameter λ in the fourth step of our scheme. In fact, if $\lambda = 1$, then the downsizing step disappears. Note that DWT provides a compact representation of a image in time and frequency that can be computed efficiently. It means that DWT has good properties of time-frequency localization and energy concentration. Thus, the most of the original image information are concentrated on the top-left corner of the image after sparsification and the left part of the image after CS. Thus the downsizing step is reasonable and the later experiments provide evidences for this claim.

3.2 The image reconstruction phase

Without loss of generality, suppose that the k participants $\{P_i\}_{i \in [k]}$ with k shadows $\{I_i\}_{i \in [k]}$ want to reconstruct the secret image $\mathbf{I}$. Then the image reconstruction phase can be performed as follows:

1. *Reverse operations.* For each i , perform the reverse operations of diffusion and permutation over I_i using the private keys k_3 and k_2 . Therefore obtain Z_i . Note that according to the secret sharing phase, the reverse operations can be implemented efficiently.
2. *Padding.* For each i , pad a $\mathbf{0}$ matrix with $M/n \times (1 - \lambda)N$ size on the right side of Z_i and form a new matrix $\mathbf{Y}_i \in \mathbb{R}^{M/n \times N}$.
3. *Extracting.* Generate the sensing matrix $\mathbf{A}$ using the private key k_1 and extract the i -th part $\mathbf{A}_i$ of $\mathbf{A}$, i.e.,

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_n \end{pmatrix}, \quad (11)$$

where $\mathbf{A}_i \in \mathbb{R}^{M/n \times N}$.

4. *Combination.* Combine $\{\mathbf{A}_i\}_{i \in [k]}$ and form a new sensing matrix $\mathbf{A}^* \in \mathbb{R}^{kM/n \times N}$. Similarly, form the compressed measurements $\mathbf{Y} \in \mathbb{R}^{kM/n \times N}$ using $\{\mathbf{Y}_i\}_{i \in [k]}$.
5. *Reconstruction.* Using the sensing matrix $\mathbf{A}^*$ and $\mathbf{Y}$ to reconstruct the secret image through some reconstruction algorithms in CS and obtain the sparse matrix $\mathbf{X}$.
6. *Anti-sparsification.* Compute the secret image $\mathbf{I} = \Phi^T \mathbf{X} \Phi$, where Φ is the orthogonal DWT matrix.

3.3 Theoretical results

Theorem 1 Suppose that the original shared image $\mathbf{I} \in \mathbb{R}^{N \times N}$ is converted into an s -sparse matrix $\mathbf{X}$ under DWT and the control parameter in our scheme is λ . Then the size of each shadow I_i is not smaller than $O(s \log N/s)/n \times \lambda N$.

Proof. From the sharing phase of our scheme, the size of I_i is the same as that of Z_i , i.e., $M/n \times \lambda N$. Lemma 2 shows that in order to reconstruct the original image, CS requires that the number of measurements M does not less than $O(s \log N/s)$ [28]. Thus, the size of each shadow is not smaller than $O(s \log N/s)/n \times \lambda N$. Note that in order to reduce the size of I_i , the dealer can set $M = O(s \log N/s)$ in the secret image sharing phase.

Theorem 2 Suppose that the original shared image $\mathbf{I} \in \mathbb{R}^{N \times N}$ is converted into an s -sparse matrix $\mathbf{X}$ under DWT. If $k \geq \frac{2ns}{O(s \log N/s)}$, then our proposed scheme is a (k, n) -SSIS scheme.

Proof. If all the n participants want to participate in the reconstruction phase, then the secret image $\mathbf{I}$ evidently can be reconstructed. If k ($k < n$) participants want to reconstruct it, then the size of formed matrix $\mathbf{Y}$ is not smaller than $kO(s \log N/s)/n \times \lambda N$. Lemma 1 indicates that the sensing matrix $\mathbf{A}$ should satisfy $\text{spark}(\mathbf{A}) > 2s$ in order to guarantee the existence of unique sparse solution of Eq (1). According to the definition of the spark, it is easy to see that $2 \leq \text{spark}(\mathbf{A}) \leq M + 1$. Therefore, we have

$$s \leq \frac{1}{2}M \leq \frac{kO(s \log N/s)}{2n}, \quad (12)$$

i.e., $k \geq \frac{2ns}{o(s \log N/s)}$. Thus, our proposed scheme is a (k, n) -SIS scheme if $k \geq \frac{2ns}{o(s \log N/s)}$. Note that in CS, the only way to improve the reconstruction quality is to gather more measurements. Hence, in our scheme, the more the number of shadows, the better the reconstruction quality. That is, our scheme is a (k, n) -SSIS scheme. This completes the proof.

4 Experimental Results and Security Analysis

In this section, we first show some experimental results to demonstrate the feasibility of our scheme, including smooth scalability, key sensitivity, noise-resilient capability and flexibility. In addition, the correlation analysis imply that our scheme can resist some statistical attacks. Last, we analyze the security of private keys in terms of outsider attacks and insider attacks.

4.1 Smooth scalability

Here we use the classic index, peak signal-to-noise ratio (PSNR), to evaluate the quality of the reconstructed images. Given a secret image I and the corresponding reconstructed image I^* , the PSNR (in dB) between them is defined as $PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE_{I,I^*}} \right)$, where MAX_I and MSE_{I,I^*} , respectively, stand for the maximum possible pixel value of I and the mean square error between I and I^* . Fig 2 shows a $(4, 8)$ -SSIS scheme constructed by our proposed method. In our experiments, the secret image I is a frequently-used test image, Lena, which can be viewed as a 512×512 matrix. The control parameter $\lambda = 0.5$ and the randomly selected private keys are $k_1 = (0.39, 0.45)$, $k_2 = (0.78, 0.63)$ and $k_3 = (0.21, 0.97)$. Hence the sensing matrix $A \in \mathbb{R}^{192 \times 512}$ can be constructed using the skew tent map with the private key k_1 according to the method of [28]. It is not hard to see that the size of each shadow is

Fig 2. Original secret image and the reconstructed images with different threshold value k . (B)PSNR = 3.0434dB; (C)PSNR = 2.4072dB; (D) PSNR = 11.786dB; (E)PSNR = 24.1027dB; (F)PSNR = 25.6763dB; (G)PSNR = 26.8478dB; (H)PSNR = 27.9183dB.

doi:10.1371/journal.pone.0168674.g002

24×256 . Fig 2 indicates that if $k < 4$, then the reconstructed image is meaningless. However, when $k \geq 4$, we can see that the larger the value of k , the higher the PSNR. Thus, our proposed SSIS scheme achieves the smooth scalability.

4.2 Key sensitivity

In our scheme, there exist three private keys, $k_1 = (z^1(0), \mu_1)$, $k_2 = (z^2(0), \mu_2)$ and $k_3 = (z^3(0), \mu_3)$, which are used for generating sensing matrix, performing permutation and diffusion, respectively. In fact, these private keys can be viewed as six chaotic seeds in $(0, 1)$. In these experiments, we randomly choose three private keys $k_1 = (0.3112, 0.5285)$, $k_2 = (0.0119, 0.3371)$ and $k_3 = (0.1622, 0.7943)$. And the control parameter λ is set to 0.5. To perform key sensitivity tests, suppose that all the n participants participate in the reconstruction phase, i.e., $k = n$, and they reconstruct the secret image using five actual chaotic seeds. They need to guess the remaining chaotic seed which they do not know. In each experiment, we also assume that the error of the remaining actual seed and the guessed seed is 10^{-16} . Fig 3C–3F indicate that using a slightly changed chaotic seed in k_1 or k_2 results in the complete failure of the reconstruction phase. However, Fig 3G and 3H show that the secret image can be reconstructed with relatively low quality if the private key k_3 is not fully matched. Even so, our proposed SSIS scheme is also practical because it is almost impossible that an adversary can correctly guess the private keys k_2 and k_3 at the same time. Even if the precision is 10^{-16} , the probability that the adversary guess k_2 and k_3 correctly is 10^{-64} , which is small enough to provide a strong security guarantee. That is, the key space of our scheme is large enough to make brute-force attacks infeasible.

Fig 3. Original secret image and some reconstructed images by using different keys.

doi:10.1371/journal.pone.0168674.g003

Fig 4. PSNR between the original image and its reconstructed image when noise exist.

doi:10.1371/journal.pone.0168674.g004

4.3 Noise-resilient capability and Flexibility

Most existing (k, n) -SSIS schemes do not provide noise-resilient capability. In some Shamir-type (k, n) -SSIS schemes, it is evidently impossible to perform the reconstruction phase correctly if there exist some types of noise in the communication channel. However, in the real word, noise cannot be avoided. Thus, designing (k, n) -SSIS schemes with noise-resilient capability is an important challenge in this field. In our construction, we first use CS to compress the secret image and then cut the compressed image through a control parameter λ . Note that CS has strong noise-resilient capability. In our experiments, the secret image I is Lena and we still choose three private keys from $(0, 1)$ at random. Suppose $n = 10$ and all the participants will reconstruct the original secret image I when there exist some types of noise in the communication channel. Here we consider two types of noise, Gaussian and Uniform noise. In Fig 4A, we consider Gaussian noise with $mean = 0$ and different *variance*, i.e., 5, 10, 30, and 50. In Fig 4B, we consider Uniform noise with different *interval*, i.e., $[-5, 5]$, $[-10, 10]$, $[-30, 30]$, and $[-50, 50]$. Experimental results reveal that the effects of Gaussian and Uniform noise on the PSNR is inappreciable. In addition, it is not difficult to find that when $\lambda > 0.5$, the PSNR is almost unchangeable. This fact provides an experimental evidence for our previous claim (Remark 2), i.e., the most of the original image information are concentrated on the left half of the image after CS. Thus, in practice, the dealer can select a optimal parameter $\lambda \approx 0.5$ to achieve a compromise between the size of each shadow and the quality of the reconstructed image.

4.4 Correlation analysis

For most nature images, the adjacent pixels are highly correlated to each other. To resist some statistical attacks, it requires that the correlation between two adjacent pixels in the shadows should be low enough. For a given image, the correlation coefficient of K pairs of adjacent pixels is defined as

$$C = \frac{\sum_{i=1}^K (x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^K (x_i - E(x))^2)(\sum_{i=1}^K (y_i - E(y))^2)}}, \quad (13)$$

where $\{x_i\}_{i=1}^K$ and $\{y_i\}_{i=1}^K$ denote the corresponding grey values that we selected randomly in

Fig 5. Correlations between two adjacent pixels in the horizontal, vertical and diagonal directions.

doi:10.1371/journal.pone.0168674.g005

the image, $E(x) = \frac{1}{K} \sum_{i=1}^K x_i$ and $E(y) = \frac{1}{K} \sum_{i=1}^K y_i$. To form the final n shadows $\{I_i\}_{i \in [n]}$, the original secret image I undergoes seven steps in our sharing phase, such as *Sparsification* and *Compression*. Here the compressed image and the final shadows are referred to the formed image after *Compression* and *Diffusion*, respectively. To measure the correlations between two adjacent pixels in the horizontal, vertical and diagonal directions, 8000 pairs of adjacent pixels are selected randomly from the secret image, the compressed image and a final shadow. Fig 5A, 5E and 5I respectively show the original image, the compressed image and a final shadow. It indicates that the nonlinear operations in our scheme are necessary for resisting statistical analysis. Fig 5B–5D show the correlations of the original image in the horizontal, vertical and diagonal directions, respectively. Similarly, Fig 5F–5H and 5J–5L show the correlations of compressed image and a final shadow in these three different directions, respectively. The experimental

Table 1. Correlation coefficients of adjacent pixels.

Correlation coefficient	Horizontal	Vertical	Diagonal
Original image	0.9740	0.9848	0.9576
Compressed image	0.0567	0.7112	0.1128
Final shadow	0.0033	0.0192	0.0191

doi:10.1371/journal.pone.0168674.t001

results show that the correlations in the horizontal and diagonal directions are greatly decreased after *Compression*. However, the correlations in the vertical is also very high. Though the nonlinear operation *Diffusion*, the final shadow has very low correlation in these three directions. The same result can be seen from Table 1.

4.5 Security analysis

The security is a critical issue that we should consider in our SSIS scheme. There are n participants in total and there exist two types of attacks, namely, outsider attacks (attacks from outside parties) and insider attacks (attacks from insider participants). No matter what type of attack might be involved, we assume that the attacker knows everything about our SIS system except the private keys because of Kerckhoffs's principle [31].

For an outsider attacker, he does not know the three private keys k_1 , k_2 and k_3 . The key sensitivity texts in Section 4.2 indicate that the key space is large enough to make brute-force attacks infeasible. Next, we will analyze our scheme from a cryptographic perspective, including ciphertext-only attack and known-plaintext attack. Ciphertext-only attack means that the attacker is assumed to have access only to a set of ciphertexts. Known-plaintext attack refers to an attack model for cryptanalysis where the attacker has access to both the plaintext and its corresponding ciphertext. In fact, Rachlin and Baron [32] proved that CS can provide a computational guarantee of secrecy and there does not exist an attacker who can reconstruct the original signal successfully under the model of ciphertext-only attack. Recently, Cambareri et al. [33] introduced a quantitative analysis to compressed sensing-based cryptosystems against known-plaintext attack. These previous studies on the security of CS model provide sufficient evidence to demonstrate that the *Sparsification* and *Compression* steps in our scheme can resist ciphertext-only attack and known-plaintext attack [32–34]. In addition, the *Permutation* and *Diffusion* steps also provide a more reliable guarantee for the security of our scheme.

However, if there exists a malicious insider participant P_i , our original (k, n) -SSIS scheme (in Section 3) has a vulnerability because each participant has the same private keys. As long as P_i obtains arbitrary other $k - 1$ image shadows in some way, such as eavesdropping on the communication channel and attacking the storage systems of other participants, he can reconstruct the secret image by himself. For this security issue, a natural solution is to transmit each shadow over a secure anti-eavesdropping communication channel and improve the security of storage systems of all participants. Obviously, this prevention method is not the best choice because of huge cost. In face of an insider attacker P_i who possesses valid chaotic keys, we provide an alternative scheme which is a slightly variant of our original scheme to overcome this deficiency. The variant is the same as our original scheme except the key distribution mechanism. In the key distribution mechanism of our variant, the dealer first chooses a random real value $k_1 \in (0, 1)$ and produces n shadows $\{k_{1i}\}_{i \in [n]}$ using Shamir's (k, n) -SS scheme. And then he chooses $2n$ different values $\{k_{2i}\}_{i \in [n]}$ and $\{k_{3i}\}_{i \in [n]}$ at random. Last, the dealer transmits the private key $\{k_{1i}, k_{2i}, k_{3i}\}$ to each participant P_i . In the image sharing phase, the dealer uses the key k_1 to produce the sensing matrix and k_{2i}, k_{3i} to perform permutation and diffusion of

Table 2. Comparison between our scheme and some typical (k, n) -SIS schemes.

Scheme	Shadow size	Scalability	Smooth scalability	Noise-resilient	Flexibility
[1]	$N \times N$	No	No	No	No
[5]	$N \times N/k$	No	No	No	No
[12]	$N \times N/2$	Yes	No	No	No
[13]	$N \times N/n$	Yes	No	No	No
[14]	$N \times N(1 + \sum_{i=k+1}^n 1/i)/n$	Yes	Yes	No	No
[15]	$M \times N/\gamma$	No	No	Yes	No
Ours	$M/n \times \lambda N$	Yes	Yes	Yes	Yes

doi:10.1371/journal.pone.0168674.t002

P_i . In the image reconstruction phase, any k participants can recover k_1 using Lagrange interpolation and then produce the sensing matrix. The *Reverse operations* can also be evidently performed because each participant knows his private key. In this variant, the malicious attacker P_{i^*} only knows his own private key and does not know the private keys of the other participants. In fact, P_{i^*} becomes an “outsider attacker” with respect to the other participants. Thus, our proposed variant with different key distribution mechanism can effectively overcome some insider attacks.

5 Comparison

In this section, we provide a comparison between our scheme and some typical existing SIS schemes [1, 5, 12–15] in terms of shadow size, scalability, noise-resilient capability and flexibility, respectively. We assume that the size of the shared image is $N \times N$. Note that the size of each shadow in our scheme is $M/n \times \lambda N$, where $M < N$ and $\lambda \in (0, 1]$. Liu et al. proposed an SIS scheme with small shadows and noise-resilient capability [15], and the parameter γ in Table 2 is the compression ratio of entropy coding in the secret image sharing phase (see Step 4 of [15]). Table 2 shows the overall results and Fig 6 specifically considers the comparison of shadow sizes under a reasonable parameter setting. Table 2 indicates the superiority of our scheme. That is, our scheme has some new functionality, such as noise-resilient capability and flexibility, which some previous SIS schemes do not possess. Evidently, we can see that the shadow size of our scheme is much smaller than those of the aforementioned schemes. Here we also provide further evidence from an experimental point of view. In Fig 6, the size of secret image $N \times N$ is 512×512 and the number of measurements M in CS is 192. To make the shadow size in [15] as small as possible, we set the parameter γ equal to 5. In Fig 6A, the number of all participants n is 32 and we investigate the number of entries in each shadow with the

Fig 6. Comparison of shadow sizes between our scheme and some existing SIS schemes.

doi:10.1371/journal.pone.0168674.g006

increasing of the threshold value k . Note that such number plays a crucial role in the communication and storage overhead. Similarly, Fig 6B investigates the number of entries in each shadow in terms of n when the threshold value k is 10. The experimental results show that no matter how large λ is, the number of entries in each shadow in our scheme is very small compared to those in the other schemes. Thus we can conclude that our proposed scheme is competitive compared to these typical existing SIS schemes.

6 Conclusion

Based on CS, a secure and efficient (k, n) -SSIS scheme with flexible shadow sizes is present in this paper. The main idea behind our construction is to reduce the size of each shadow through two procedures, i.e., *Compression* and *Downsizing*. And then the dealer performs two nonlinear operations, *Permutation* and *Diffusion*, for improving security. Thus, the dealer can achieve a compromise between the size of each shadow and the quality of the reconstructed image. Compared to some existing SSIS schemes, the experimental results and security analysis indicate the infeasibility and potential superiority of our scheme.

Author Contributions

Conceptualization: DX LXL.

Funding acquisition: LXL HPP YXY.

Methodology: DX LXL HPP.

Software: DX HPP.

Validation: HPP YXY.

Writing – original draft: DX LXL.

Writing – review & editing: DX LXL.

References

1. Shamir Adi. How to share a secret. Communications of the ACM. 1979; 22(11): 612–613. doi: [10.1145/359168.359176](https://doi.org/10.1145/359168.359176)
2. Blakley GR. Safeguarding cryptographic keys. In AFIPS Conf. Proc. 1979; 48: 313–317.
3. Martin Keith. Challenging the Adversary Model in Secret Sharing Schemes. In Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts. 2008; 45–63.
4. Iftene S. Secret sharing schemes with applications in security protocols. Sci. Ann. Cuza Univ. 2006; 16: 63–96.
5. Thien CC, Lin JC. Secret image sharing. Computers and Graphics. 2002; 26(5): 765–770. doi: [10.1016/S0097-8493\(02\)00131-0](https://doi.org/10.1016/S0097-8493(02)00131-0)
6. Lin CC, Tsai WH. Secret image sharing with steganography and authentication. Journal of Systems and Software. 2004; 73(3): 405–414. doi: [10.1016/S0164-1212\(03\)00239-5](https://doi.org/10.1016/S0164-1212(03)00239-5)
7. Yang CN, Chen TS, Yu KH and Wang CC. Improvements of image sharing with steganography and authentication. Journal of Systems and software. 2007; 80(7): 1070–1076. doi: [10.1016/j.jss.2006.11.022](https://doi.org/10.1016/j.jss.2006.11.022)
8. Alharthi S, Atrey PK. An improved scheme for secret image sharing. In Proceedings of IEEE international Conference on multimedia and Expo Workshop on Content Protection and Forensics. 2010; 1661–1666.
9. Bhadravati S, Khabbazian M, Atrey PK. On the semantic security of secret image sharing methods. In Proceedings of the seventh International Conference on Semantic Computing. 2013; 302–305.
10. Yang C, Wu C. A threshold secret image sharing with essential shadow images. Advances in intelligent systems and applications. 2013; 2: 159–166.

11. Das SK, Dhara BC. A new secret image sharing with arithmetic coding. In 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). 2015; 395–399.
12. Wang R, Shyu S. Scalable secret image sharing. *Signal Processing: Image Communication*. 2007; 22(4): 363–373.
13. Yang C, Huang S. Constructions and properties of k out of n scalable secret image sharing. *Optics Communications*. 2010; 283(9): 1750–1762. doi: [10.1016/j.optcom.2009.12.077](https://doi.org/10.1016/j.optcom.2009.12.077)
14. Yang CN, Chu YY. A general (k, n) scalable secret image sharing scheme with the smooth scalability. *Journal of Systems and Software*. 2011; 84(10): 1726–1733. doi: [10.1016/j.jss.2011.05.008](https://doi.org/10.1016/j.jss.2011.05.008)
15. Liu L, Wang AH, Chang CC, Li ZH, Liu JB. A Lossy Secret Color Image Sharing Scheme with Small Shadows and Error-resilient Capability. *Journal of Information Hiding and Multimedia Signal Processing*. 2015; 6(2): 246–253.
16. Lee JS, Chen YR. Selective scalable secret image sharing with verification. *Multimedia Tools and Applications*. 2015; 1–11.
17. Mallat S, Zhang Z. Matching pursuit with time-frequency dictionaries. *IEEE Transactions on Signal Processing*. 1993; 41(12): 3397–3415. doi: [10.1109/78.258082](https://doi.org/10.1109/78.258082)
18. Foucart S. A note on guaranteed sparse recovery via l_1 -minimization. *Applied and Computational Harmonic Analysis*. 2010; 29(1): 97–103.
19. Donoho DL. Compressed sensing. *IEEE Transactions on Information Theory*. 2006; 52(4): 1289–1306. doi: [10.1109/TIT.2006.871582](https://doi.org/10.1109/TIT.2006.871582)
20. Candés EJ, Romberg J, and Tao T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Transaction on Information Theory*. 2006; 52(2): 489–509. doi: [10.1109/TIT.2005.862083](https://doi.org/10.1109/TIT.2005.862083)
21. Candés EJ, Romberg J, and Tao T. Stable signal recovery from incomplete and inaccurate measurements. *Communications on Pure and Applied Mathematics*. 2006; 59(8): 1207–1223. doi: [10.1002/cpa.20124](https://doi.org/10.1002/cpa.20124)
22. Xie D, Peng H, Li L, Yang Y. Semi-tensor compressed sensing. *Digital Signal Processing*. 2016; 58, 85–92. doi: [10.1016/j.dsp.2016.07.003](https://doi.org/10.1016/j.dsp.2016.07.003)
23. Xie D, Li L, Niu X, Yang Y. Identification of coupled map lattice based on compressed sensing. *Mathematical Problems in Engineering*. 2016; Article ID 6435320. doi: [10.1155/2016/6435320](https://doi.org/10.1155/2016/6435320)
24. Donoho D, Elad M. Optimally sparse representation in general (nonorthogonal) dictionaries via l_1 minimization. *Proceedings of the National Academy of Sciences*. 2003; 100(5): 2197–2202. doi: [10.1073/pnas.0437847100](https://doi.org/10.1073/pnas.0437847100)
25. Tropp JA. Greed is good: algorithmic results for sparse approximation. *IEEE Transaction on Information Theory*. 2004; 50(10): 2231–2242. doi: [10.1109/TIT.2004.834793](https://doi.org/10.1109/TIT.2004.834793)
26. Nesterov Y. Smooth minimization of non-smooth functions. *Mathematical Programming*. 2005; 103: 127–152. doi: [10.1007/s10107-004-0552-5](https://doi.org/10.1007/s10107-004-0552-5)
27. Yu L, Barbot JP, Zheng G, and Sun H. Compressive sensing with chaotic sequence. *IEEE Signal Processing Letters*. 2010; 17: 731–734. doi: [10.1109/LSP.2010.2052243](https://doi.org/10.1109/LSP.2010.2052243)
28. Frunzete M, Yu L, Barbot JP, and Vlad A. Compressive sensing matrix designed by tent map, for secure data transmission. In *Signal Processing Algorithms, Architectures, Arrangements, and Applications Conference Proceedings (SPA)*. 2011; 1–6.
29. Duarte MF, Eldar YC. Structured compressed sensing: From theory to applications. *IEEE Transactions on Signal Processing*. 2011; 59(9): 4053–4085. doi: [10.1109/TSP.2011.2161982](https://doi.org/10.1109/TSP.2011.2161982)
30. Wang X, Teng L, and Qin X. A novel colour image encryption algorithm based on chaos. *Signal Processing*. 2012; 92(4): 1101–1108. doi: [10.1016/j.sigpro.2011.10.023](https://doi.org/10.1016/j.sigpro.2011.10.023)
31. Cayre F, and Bas P. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Transactions on Information Forensics and Security*. 2008; 3(1): 1–15. doi: [10.1109/TIFS.2007.916006](https://doi.org/10.1109/TIFS.2007.916006)
32. Rachlin Y, Baron D. The secrecy of compressed sensing measurements. In the 46th Annual Allerton Conference on Communication, Control, and Computing. 2008; 813–817.
33. Cambareri V, Mangia M, Pareschi F, Rovatti R, and Setti G. On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis. *IEEE Transactions on Information Forensics and Security*. 2015; 10(10): 2182–2195. doi: [10.1109/TIFS.2015.2450676](https://doi.org/10.1109/TIFS.2015.2450676)
34. Bianchi T, Bioglio V, and Magli E. Analysis of one-time random projections for privacy preserving compressed sensing. *IEEE Transactions on Information Forensics and Security*. 2016; 11(2): 313–327. doi: [10.1109/TIFS.2015.2493982](https://doi.org/10.1109/TIFS.2015.2493982)