





## Article

# Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography

Yuyuan Sun <sup>1,2</sup> , Yuliang Lu <sup>1,2,\*</sup> , Jinrui Chen <sup>1,2</sup> , Weiming Zhang <sup>3</sup> and Xuehu Yan <sup>1,2</sup> 

<sup>1</sup> National University of Defense Technology, Hefei 230037, China; sun\_yuyuan@nudt.edu.cn (Y.S.);  
cjr@mail.ustc.edu.cn (J.C.); yanxh17@nudt.edu.cn (X.Y.)

<sup>2</sup> Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

<sup>3</sup> School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China; zhangwm@ustc.edu.cn

\* Correspondence: publicluy1@126.com; Tel.: +86-0558-66927640

Received: 27 May 2020; Accepted: 24 August 2020; Published: 30 August 2020



**Abstract:** The  $(k, n)$ -threshold Secret Image Sharing scheme (SISS) is a solution to image protection. However, the shadow images generated by traditional SISS are noise-like, easily arousing deep suspicions, so that it is significant to generate meaningful shadow images. One solution is to embed the shadow images into meaningful natural images and visual quality should be considered first. Limited by embedding rate, the existing schemes have made concessions in size and visual quality of shadow images, and few of them take the ability of anti-steganalysis into consideration. In this paper, a meaningful SISS that is based on Natural Steganography (MSISS-NS) is proposed. The secret image is firstly divided into  $n$  small-sized shadow images with Chinese Remainder Theorem, which are then embedded into RAW images to simulate the images with higher *ISO* parameters with NS. In MSISS-NS, the visual quality of shadow images is improved significantly. Additionally, as the payload of cover images with NS is larger than the size of small-sized shadow images, the scheme performs well not only in visual camouflage, but also in other aspects, like lossless recovery, no pixel expansion, and resisting steganalysis.

**Keywords:** meaningful secret image sharing; Chinese Remainder Theorem; Natural Steganography; small-sized shadow images; steganalysis

## 1. Introduction

### 1.1. Secret Image Sharing

Nowadays, the acquisition and transmission of information exist in all aspects and all the time, so that information protection is increasingly important. In order to perform well in this field, various methods are used for this purpose, such as cryptography, steganography, secret sharing, and so on. Among these methods, secret sharing scheme (SSS) has attracted a lot of attentions. The  $(k, n)$ -threshold SSS is a method that secret information is divided into  $n$  portions, called shares or shadows. Only  $k$  or more than  $k$  portions are accessed that the secret can be reconstructed correctly, and there will be no information leakage without sufficient shares.

Based on the characteristics of SSS, it has the advantages of unconditional security, loss tolerance, access control, and so on. Moreover, secret image sharing scheme (SISS) can also be applied to improvement of the security levels by exploiting the images and in general content retrieval based on user preferences [1].

Since Shamir [2] firstly proposed SSS in 1979, many researchers have paid lots of attentions to this aspect. Additionally, SSS also has different research directions according to techniques used.

With the development of technology, other secret sharing schemes, including SSS based on polynomial (PSSS) [3], SSS based on Chinese Remainder Theorem (CRT-SSS) [4], visual cryptography or visual secret sharing (VC or VSS) [5], SSS based on boolean operation [6], have been proposed. Among these schemes, CRT-SSS has attracted the interests of researchers.

CRT is a method of solving a group of congruences in ancient China. Mignotte [7], Asmuth and Bloom [8] proposed a SSS based on CRT in 1982. When compared with P-SSS, this scheme has moderate computational complexity and lossless recovery. Yan et al. [9] and Li et al. [10] introduced CRT to  $(k, n)$ -threshold secret image sharing scheme, which has the advantages of lossless recovery and high decryption efficiency. However, the value of  $n$  is generally limited to six because it is necessary to select the  $p, m_1, \dots, m_n$  that meets the requirements and only several thresholds can be implemented. The shadow images of these schemes are the same size as the secret images. Chen et al. [11] exhibited a SISS based on CRT with small-sized shadow images by adding random bits to binary representations of random parameters in CRT. This scheme can not only make the shadow images flexible, but also has no leakage of secret information. In this paper, Chen et al.'s scheme will be employed to generate the small-sized shadow images.

## 1.2. Meaningful Secret Image Sharing Schemes

In the traditional SISS, the shares are noise-like, which is useful to avoid information leakage. However, on the one hand, noise-like shares are easily suspected by attackers, which may be destroyed or intercepted during transmission process. On the other hand, shares and public values need to correspond one-by-one in recovery process and noise-like ones will lead to problems in the management of shares. All in all, it is necessary that the shares seems the same as meaningful images without any additional information and it is our initial purpose.

Meaningful secret image sharing scheme (MSISS), also called extended secret image sharing scheme (ESISS) in some articles, is a kind of SISS that the generated shadow images are with natural meaning. This concept was first proposed by Ateniese et al. [12]. To achieve this purpose, two solutions have been proposed, SISS with coverless images [13] and SISS with cover images.

“Coverless” does not mean that no cover is needed, but directly driven by secret information to “generate” or “acquire” the stego images. Coverless SISS is to focus more on the secret sharing principle itself. With this thinking mind, the sharing sequences similar to the pixel value of the cover images are generated under the constraint of the secret pixel value and the corresponding pixel value of cover images, which makes the shadow image have the comprehensible property. For example, Yan et al. [14] gave a general secret scheme that shadow images can be understood by using the characteristics of random elements, which included the meaningful secret sharing scheme based on polynomial,  $(2, n)$ -threshold random grids, and CRT. In the sharing process, appropriate screening operations were added to make the pixels in each grayscale shadow images as close as possible to the cover images. This kind of MSISS may take plenty time to filter the qualified sharing values, the embedding rate is relatively low and the quality of results is not always satisfactory. These lead to a certain distance from the practical application of this aspect.

Another solution is SISS with cover images, embedding the noise shadow images into meaningful cover images by steganography, which is not constrained by the sharing principle and all kinds of SS schemes can be exploited. Lin et al. [15] introduced a  $(k, n)$ -threshold SSS with authentication function, which divided the image into  $n$  shadow images, hid the shadow images into the corresponding camouflage images of  $n$  participants, and then embedded watermarking into stego images. Li et al. [16] proposed a SISS with authentication. The secret image is shared based on PSNR estimation and then hidden in ordinary cover images, so as to be transmitted securely with the meaningful images. The new scheme optimized the visual quality and the size of the stego images in some degree. In 2014, Yuan et al. [17] introduced a SISS with multi-cover adaptive steganography. While the two above schemes exist pixel expansion. The shadow images are almost four times larger than secret image in [16]. The secret image in [17] is two-tone or four-tone image, and shadow images are grayscale.

Derya [18] showed up a meaningful secret image sharing method based on Arabic letters. In the proposed method, secret shares were embedded into R, G, and B channels, respectively, and Arabic letters were used for camouflage. Cheng et al. [19] applied the Absolute Moment Block Truncation Coding (AMBTC) to compress transmission bit rate. In 2017, He et al. [20] put forward an image sharing scheme based on steganography with the use of LOCO-I compression to reduce the size and statistical correlations between neighboring pixels. In recent years, more methods about MSISS based on VSS have appeared. Chiu et al. [21] put forward a  $(2, n)$  progressive VSS with meaningful shares. Besides, Maurya et al. [22] mainly focused on medical image security through EVSS and the sharing and recovering process were lossless and had less complexity. These two methods above are limited by the threshold.

All of the above schemes focus on getting meaningful shadow images. However, there are still several problems. Many schemes are based on VSS and it is not easy to reconstruct secret losslessly and the visual quality needs to be improved. What is more, due to the embedding rate of steganography, the designers have to reduce the size of shadow images, which may be not able to achieve unconditional security. At the same time, the stego images are often several times larger than original secret images in order to achieve high visual quality, leading to large pixel expansion. Besides, steganalysis can be adopted to distinguish the stego images embedded into shadow images by LSB or other information hiding technologies easily and, thus, new steganography should be considered.

### 1.3. Motivations

To summarize, the existing MSISS remains several aspects to be improved. Firstly, the frequently-used VSS in MSISS may lead to the loss of recovered results and in some specific areas, like medical or military, lossless recovery is indispensable. Additionally, then it is better that the stego images are the same size as secret image so that unnecessary storage space and transmission bandwidth can be reduced. Last but not least, as a MSISS, the visual quality of shadow images is the most significant factor in measuring the scheme and visual quality. The higher the visual quality, the better the scheme is, so that the concealment and security of shadow image can be enhanced.

In addition, in the era of big data, the Internet is full of information, so it is hard to distinguish the true from the false [23]. Although MSISS seems like natural images, there are still differences with those images. The identification and supervision of network media content makes the hidden information more easily discovered. Therefore, MSISS should be able to resist similar attacks as much as possible, such as steganalysis, etc.

### 1.4. The Proposed Method

In this paper, a meaningful SISS based on Natural Steganography (MSISS-NS) is proposed. This scheme combines SSS and steganography in order to improve the visual quality of shadow images. The cover images of MSISS-NS are RAW images, which contain data processed from an image sensor of a digital camera or scanner. They are so named, because they have not been processed, printed, or used for editing. Therefore, RAW images will record the detail data, such as the exposure time, white balance, ISO sensitivity, and others about taking pictures. In other words, all relevant information is stored in RAW images without loss or with slight loss.

In a nutshell, MSIS-NS utilizes CRTSIS-SSI [11] (the details will be introduced in Section 2.1) to generate small-sized shadow images that will be embedded into the RAW images to imitate the higher ISO ones by Natural Steganography (NS will be explained in Section 2.2). The payload of the cover images with NS is high enough to embed the shadow images without other extra encoding or compressing operations. Additionally, the shadow images are meaningful and have no pixel expansion. Besides, no previous work has ever reported its capability to resist steganalysis except [17]. Our scheme performs well in resisting steganalysis through experiments.

The arrangement of this article is as follows. Section 2 introduces the preliminaries crucial to understand the scheme. Section 3 presents the detail sharing and recovering algorithm of MSISS-NS. In Section 4, the experimental results and summaries about the scheme are illustrated. Additionally, Section 5 focuses on the conclusion of MSISS-NS and future work.

## 2. Preliminaries

For better understanding the method proposed, some background knowledge is introduced in this section, including some notations of symbols and the classifier this paper used.

### 2.1. Chinese Remainder Theorem-Based Secret Image Sharing with Small-Sized Shadow Images

Even for the most advanced steganography scheme, it cannot embed a secret image with the same size to the cover image. Chinese Remainder Theorem-Based Secret Image Sharing with Small-Sized Shadow Images (abbreviated as CRTSIS-SSI [11]) realized sharing a secret image losslessly incorporating the advantages of small-sized shadow images, no auxiliary encryption, and low computation complexity [9].

To share a secret image  $S$  with the size of  $W \times H$ , there are always two processes, named the sharing process and the recovery process. The sharing process of CRTSIS-SSI is carried, as follows:

Step 1: set the initial parameters  $(k, n)$  threshold, and a set of integers  $m_1, m_2, \dots, m_n$  subject to:

1.  $128 \leq p < m_1 < m_2 < \dots < m_n \leq 256$ .
2.  $\gcd(m_i, m_j) = 1, i \neq j$ .
3.  $\gcd(m_i, p) = 1$  for  $i = 1, 2, \dots, n$ .
4.  $M > pN$ .

Here,  $p$  is usually fixed at 128 or 131 [9].

Step 2: Compute  $M, N, T$  according to the above parameters and the following formulas.

1.  $M = \prod_{i=1}^k m_i$ .
2.  $N = \prod_{i=1}^{k-1} m_{n-i+1}$ .
3.  $T = \left\lceil \frac{\left\lfloor \frac{M}{p} - 1 \right\rfloor - \left\lfloor \frac{N}{p} \right\rfloor}{2} \right\rceil + \left\lceil \frac{N}{p} \right\rceil$ .

$p, N$ , and  $T$  are public among all the participants.  $m_1, m_2, \dots, m_n$  are the privacy modular integers corresponding to the shadow images  $SSC_1, SSC_2, \dots, SSC_n$  held by each participant.

Step 3: binarize the secret image  $S$  to a string of binary data  $D$ . Divide  $D$  into blocks of size  $8k - 1 - r$ , where  $r \in [1, 7]$ .

Step 4: for each block, the first 8 bits are transformed to a decimal number  $x$ , and the next  $8(k - 1) - 1 - r$  bits of  $D$  plus  $r$  random bits totally  $8(k - 1) - 1$  to express a decimal integer  $A^*$ . Subsequently, if  $0 \leq x < p$ ,  $A = A^* + (T + 1)$ ,  $y = x + Ap$ ; otherwise,  $A = A^* + \left\lceil \frac{N}{p} \right\rceil$ ,  $y = x - p + Ap$ .

Step 5: for each block, compute  $a_i \equiv y \pmod{m_i}$  and let  $SSC_i = a_i$  for  $i = 1, 2, \dots, n$ .  $SSC_i$  represents the pixel value of the  $i$ th shadow corresponding to the same block.

Through the sharing process, the secret image  $S$  is divided into  $n$  shadow images, and any  $k$  ones of them can reconstruct  $S$ . Subsequently, the recovery process is described below:

Step 1: collect  $k$  shadow images  $SSC_{i_1}, SSC_{i_2}, \dots, SSC_{i_k}$  with size of  $L \times F$ , corresponding privacy modular integers  $m_{i_1}, m_{i_2}, \dots, m_{i_k}$ , and public parameters  $p, T, N, r$ .

Step 2: for  $(l, f) \in \{(l, f) | 1 \leq l \leq L, 1 \leq f \leq F\}$ , let  $a_{i_j} = SSC_{i_j}(l, f)$  for  $j = 1, 2, \dots, k$ . Get the unique solution  $y$ , which is part of the original secret image  $S$  by solving the following linear equations.

$$y \equiv a_{i_1} \pmod{m_{i_1}}.$$

$$y \equiv a_{i_2} \pmod{m_{i_2}}.$$

$$\dots$$

$$y \equiv a_{i_k} \pmod{m_{i_k}}.$$

Repeat Step 2 until all of the pixels in shadow images have been solved.

Step 3: compute  $T^* = \left\lfloor \frac{y}{p} \right\rfloor$ . If  $T^* \geq T$ , let  $x \equiv y \pmod{p}$ ,  $A^* = \frac{y-x}{p} - (T+1)$ . Else, let  $x = y \pmod{p} + p$ ,  $A^* = \frac{y-x}{p} - \left\lceil \frac{N}{p} \right\rceil$ . Binarize  $x$  and  $A$ , then, 8 bits of  $x$  and  $8(k-1) - 1 - r$  ( $r \in [1, 7]$ ) bits of  $A$  are added in sequence to a binary string  $D'$ , which is empty initially.

Step 4: convert the binary data  $D'$  per 8 bits to a string of decimal numbers. Shape and output the recovered secret image  $S'$ .

In CRTSIS-SSI,  $r$  random bits are the crucial factors that will affect the security of the shadow images. The reduction of shadow image size in CRTSIS-SSI is  $\frac{1}{k-(1+r)/8}$ . As mentioned above, the range of  $r$  is  $[1, 7]$ . With the increase of  $r$ , the security of the scheme CRTSIS-SSI is enhanced. For natural images,  $r = 2$  performs well, as, for images with lots of consecutive pixels,  $r = 7$  is adequate. The bigger  $r$  is, the larger the size of the shadow images is. It is even the same as the original secret image when  $k = 2$  and  $r = 7$ .

## 2.2. Natural Steganography

Natural Steganography (NS) [24] is a model-based image steganography scheme that relies on simulating the noise naturally exists in the RAW images captured by a monochrome sensor. The concepts are elaborated below.

The scene of NS is first described. As we all know, cover-source mismatch is one of the most serious challenges in steganalysis. It refers to the discrepancy between training and testing images [25]. In the case of NS, it is the possible cover-source mismatch that is used to improve steganographic security. Actually, NS is a kind of side-informed steganography [26] utilizing the precover that is a cover with a higher quality to embed secret messages. The empirical security of steganographic schemes can be improved by embedding in the process of converting the high quality precover to a lower quality image. The RAW image produced straight from the camera sensor is taken as the precover in NS. The procedure of outputting a RAW image from the camera is depicted, as follows.

There are four basic steps in the RAW image generation process. And Figure 1 shows the general procedure of a RAW image.

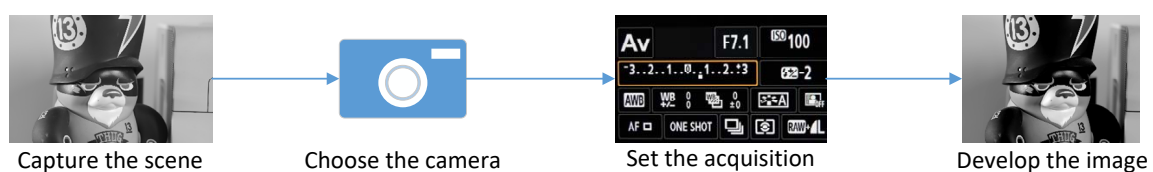


Figure 1. The general procedure of a RAW image.

- (1) Choose the scene to capture, including landscape, portrait, illumination and so on.
- (2) Decide the camera to use. The sensor of the camera may be CCD or CMOS. The mode of the sensor can be color or monochrome.
- (3) Set the acquisitions of the camera, such as ISO sensitivity, exposure time, white balance, etc.
- (4) Develop the original RAW image. Many developing steps can be done before the image output from the camera, containing quantization, downsampling, gamma correction, lossy coding, and so on.

When capturing a scene using a camera with linear sensors, such as CCD or CMOS sensors, the photos will contain fixed noises. Additionally, the amount of noise will increase accompanied by

the higher *ISO*. The noise model can be approximated as normally and independently distributed satisfying Equation (1).

$$N \sim \mathcal{N}(0, a\mu_{i,j} + b) \quad (1)$$

$N$  is the global sensor noise of the image captured at a given *ISO* setting.  $\mathcal{N}$  represents the normal and independent distribution. Parameters  $(a, b)$  are obtained by the protocol proposed in [27] to estimate the noise model.  $\mu_{i,j}$  is the expectation of the photo-site at location  $(i, j)$ . Consequently, the pixel value  $x_{i,j}$  is given by Equation (2):

$$x_{i,j} = \mu_{i,j} + n_{i,j} \quad (2)$$

where  $n_{i,j}$  is the sensor noise at position  $(i, j)$  and  $X \sim \mathcal{N}(\mu_{i,j}, a\mu_{i,j} + b)$ .

For a given scene and a given camera, two images are captured at  $ISO_2 > ISO_1$ . All of the other acquisition parameters remain the same, including focus, white balance, and aperture, except the exposure time. According to Equations (1) and (2), for  $ISO_1$  the pixel value at position  $i, j$  and the sensor noise is

$$x_{i,j}^{(1)} = \mu_{i,j} + n_{i,j}^{(1)} N^{(1)} \sim \mathcal{N}(0, a_1\mu_{i,j} + b_1) \quad (3)$$

For  $ISO_2$ , the equivalents are:

$$x_{i,j}^{(2)} = \mu_{i,j} + n_{i,j}^{(2)} N^{(2)} \sim \mathcal{N}(0, a_2\mu_{i,j} + b_2) \quad (4)$$

Because the sum of two normally and independently distributed signals is also normal, it gains that:

$$S = N^{(2)} - N^{(1)} \sim \mathcal{N}(0, (a_2 - a_1)\mu_{i,j} + b_2 - b_1) \quad (5)$$

Thus, the relational expression of  $x_{i,j}^{(1)}$  and  $x_{i,j}^{(2)}$  is deduced as:

$$x_{i,j}^{(2)} = \mu_{i,j} + n_{i,j}^{(2)} = \mu_{i,j} + n_{i,j}^{(1)} + s_{i,j} = x_{i,j}^{(1)} + s_{i,j} \quad (6)$$

Subsequently, the model-based steganography scheme of NS is built on Equation (6). The secret messages are converted to mimic the noise signal  $s_{i,j}$  and added on the pixel value of the image captured at  $ISO_1$ . Hence, the generated stego image is similar to the image captured at  $ISO_2$ . It is also named to be Cover-Source Switching [24]. The model of NS is shown as Equation (6), and steganography is based on Syndrome-Trellis Codes (STC) [28]. Meanwhile, this scheme can enhance the difficulty in dealing with cover-source mismatch and improve the safety of steganography further.

### 3. The Proposed Meaningful Secret Image Sharing Based on Natural Steganography

In this section, the proposed meaningful secret image sharing scheme based on Natural Steganography (abbreviated as MSISS-NS) is demonstrated. Section 3.1 displays the model of the scheme. Section 3.2 describes the detail algorithms of the sharing and recovery processes. In Section 3.3, we will discuss the remarkable tips and relevant questions regarding MSISS-NS.

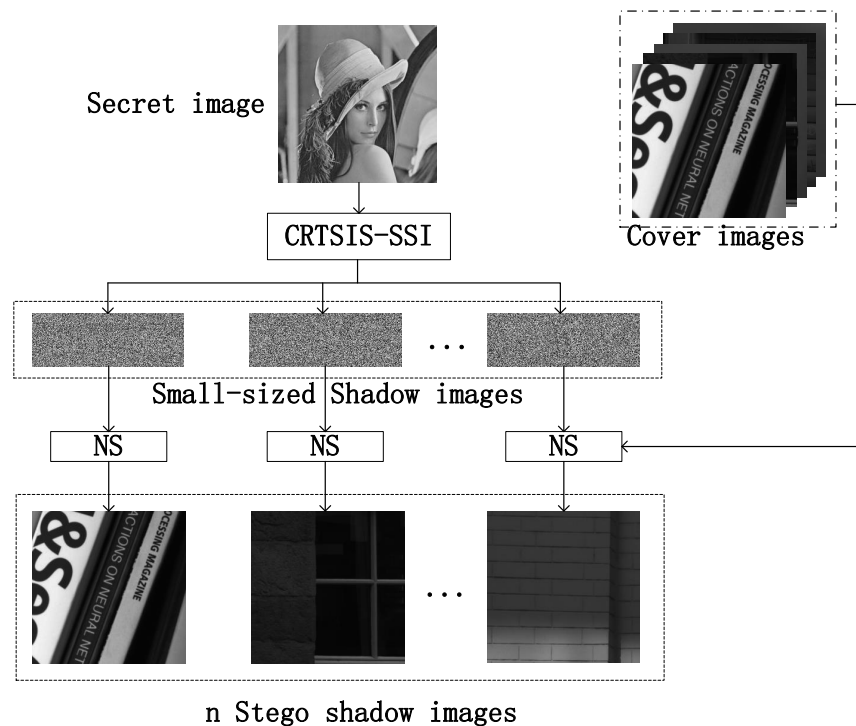
#### 3.1. The Proposed Model

The proposed model is a combination of SISS and steganography. The SISS adopted is CRTSIS-SSI, which incorporates the advantages of small-sized shadow images, lossless recovery, low computation complexity, and  $(k, n)$  threshold. The steganography scheme is based on NS with the priorities of large payload and excellent anti-steganalysis ability.

The proposed scheme MSISS-NS can be separated to two parts, including the sharing and recovery process. The flow of the model is described, as follows.

### 3.1.1. Sharing Process

The sharing model of MSISS-NS is shown in Figure 2.



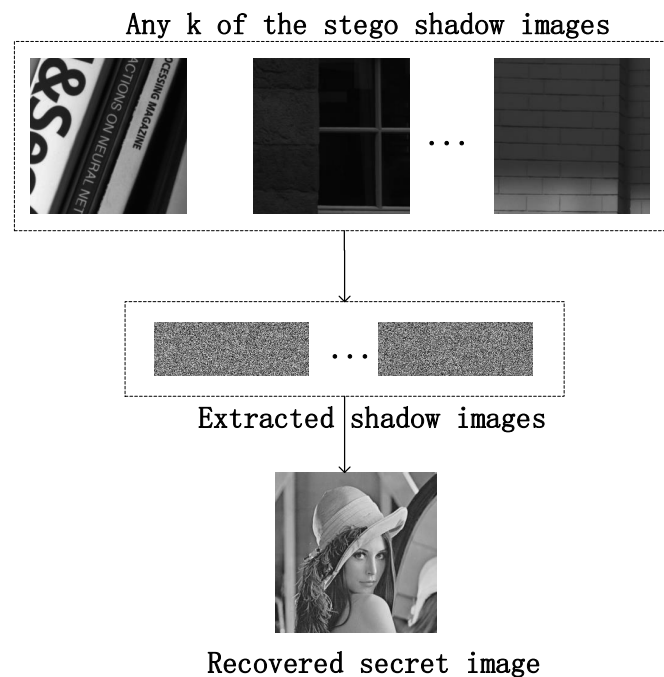
**Figure 2.** The sharing model of the proposed scheme MSISS-NS.

The sharing process can be roughly divided into two steps. The first step is to share the secret image  $S$  into several small-sized shadow images  $SSC$  using CRTSIS-SSI. The second step is to embed the shadow image  $SSC_i$  into a cover image  $C_i$ , which is chosen from the database of the cover images  $C$  separately by using STC. Consequently, the generated images are called the meaningful shadow images  $MSC$  similar to the covers. It is noteworthy that the small-sized shadow images produced in step 1 can be embedded directly without additional operations, such as encryption or compression. And there are no strict restrictions on the content of the cover images even an image that looks blank. All in all, the wide selection range of cover images avoids the detection of steganalysis to some extent. Although the cover images are not limited by the content, it is better to select meaningful images in order to avoid suspicion from stego cover images and it is also the initial purpose of MSISS-NS.

### 3.1.2. Recovery Process

The sharing model of MSISS-NS is shown in Figure 3.

The reconstruction of the secret image is an inverse procedure of the sharing process. Accounting for the proposed scheme with the threshold  $(k, n)$ , any  $k$  of the meaningful shadow images  $MSC_1, MSC_2, \dots, MSC_k$  can recover the secret image. First, the  $k$  recovered small-sized shadow images  $SSC'_1, SSC'_2, \dots, SSC'_k$  are extracted from  $MSC_1, MSC_2, \dots, MSC_k$ . Second, the recovered secret image  $S'$  are reconstructed from  $SSC'_1, SSC'_2, \dots, SSC'_k$  while using CRTSIS-SSI.



**Figure 3.** The recovery model of the proposed scheme MSISS-NS.

### 3.2. Algorithms

The details of sharing and recovery algorithms are described in the following sections of this part. The steps, formulas, and symbols are all included in the Algorithms 1 and 2.

When  $MSC_l (1 \leq l \leq n)$  are generated through Algorithm 1, they will be distributed to  $n$  participants and  $MSC_l$  are transmitted by various paths and means as general RAW images.

### 3.3. Discussions

For the two algorithms, there are several tips that need to be remarked.

1. The threshold of MSISS-NS is limited by CRTSIS-SSI, and more details can be referred to [11]
2. The embedding rate of NS is larger than other steganography method, and there are various options for embedding. The further experiments and results will be displayed in Section 4.
3. The secret image is grayscale image, its file name extension is '.bmp', and the shadow images are also grayscale with '.pgm' as extension. For the same size image, the spaces occupied by the two images are almost the same. For example, when the image is  $(512 \times 512)$ , the '.bmp' image is 257 kb and '.pgm' image is 256 kb.
4. In Step 2 of Algorithm 1, the choice of  $r$  and  $k$  is related to the size of shadow images, which is also restricted by the embedding rate of cover images.
5. The embedding method NS comes from [24], but, in Algorithm 1 Step 4, the cost function  $\rho_{ij}(q)$  has been changed, which leads to different embedding rate and detectability results.
6. STC is utilized in NS, it approaches the theoretical limit of coding and more details are described in [28].
7. In practical operation, it is a challenging issue to capture two images differing only in  $ISO$ .

---

**Algorithm 1** The sharing process of  $(k, n)$  threshold meaningful secret image sharing scheme based on Natural Steganography

---

**Input:** 1. The secret image  $S$  with the size of  $W \times H$ . 2. The set of cover images  $C$  with each size of  $W \times H$ .

**Output:** 1.  $n$  meaningful shadow images  $MSC_1, MSC_2, \dots, MSC_n$  with corresponding privacy modular integers  $m_1, m_2, \dots, m_n$ .

**Step 1:** set the initial parameters  $(k, n)$  threshold, a set of integers  $\{128 \leq p < m_1 < m_2 < \dots < m_n \leq 255\}$ , and the number of random bits  $r$ .

**Step 2:** share the secret image  $S$  using CRTSIS-SSI. Get the small-sized shadow  $SSC_l (1 \leq l \leq n)$  images whose size is  $\frac{1}{k-(1+r)/8}$  of  $S$  with corresponding privacy modular integers  $m_1, m_2, \dots, m_n$ . The parameters  $p, N, r$ , and  $T$  produced in the sharing process are all public among all the participants.

**Step 3:** set the initial parameters  $a, b$  and  $ISO_1$  of the cover images. Compute the modifications probabilities  $p_{ij}(q), (1 \leq i \leq W, 1 \leq j \leq H, 1 \leq q \leq Q)$  of each pixel in the cover image for a Q-array embedding. Meanwhile, the embedding rate  $er_t, t \in C$  of each cover image can be output for further selection on the steganography scheme.

**Step 4:** compute the cost  $\rho_{ij}(q)$  on cover image pixels according to  $\rho_{ij}(q)$  subject to:

$$\rho_{ij}(q) = \ln \frac{\rho_{ij}(0)}{\rho_{ij}(q)}, q \in Q, 1 \leq i \leq W, 1 \leq j \leq H \quad (7)$$

**Step 5:** embed the small-sized shadow images  $SSC_l, (1 \leq l \leq n)$  into the proper cover images  $C_l, (1 \leq l \leq n)$  using STC. The shadow images  $SC_l$  embedded  $SSC_l$  should satisfy the conditions, as follows:

$$Emb(C_l, SSC_l) = \arg \min_{MSC_l} \rho_{ij}(q) \quad (8)$$

If the size of the shadow image  $SSC_l$  is far less than the payload of the cover image  $C_l$ , the embedding process can be executed directly. If the size of  $SSC_l$  is close to the payload of the cover image  $C_l$ , the small-sized shadow image  $SSC_l$  should be embedded into the cover  $C_l$  together with additional random binary bits, in order to achieve a close approximation of the payload of  $C_l$ .

**Step 6:** output  $n$  meaningful shadow images  $MSC_1, MSC_2, \dots, MSC_n$  and their corresponding privacy modular integers  $m_1, m_2, \dots, m_n$ .

---



---

**Algorithm 2** The recovery process of  $(k, n)$  threshold meaningful secret image sharing scheme based on Natural Steganography

---

**Input:** 1. The  $k$  meaningful shadow images  $MSC_1, MSC_2, \dots, MSC_k$ , corresponding privacy modular integers  $m_1, m_2, \dots, m_k$  and the number of bits hidden in every layer  $b_{tr}, 0 \leq t < \lceil \frac{Q}{2} \rceil, 0 < r < k$ . 2. Public parameters  $p, T$  and  $N$ .

**Output:** The  $W \times H$  recovered secret image  $S'$ .

**Step 1:** for  $k$  meaningful shadow images  $MSC_1, MSC_2, \dots, MSC_k$ , repeat Step 2.

**Step 2:** extract the small-sized shadow image  $SSC'_r$  from the meaningful shadow image  $MSC_r, r = 1, 2, \dots, k$ , using the extraction method of STC with the parameters  $b_{tr}$ .

$$Ext(MSC_l) = HP(MSC_l) \quad (9)$$

where  $H \in \{0, 1\}^{m \times n}$  is a parity-check matrix and  $P(MSC_l)$  is the function between cover images and stego images.

**Step 3:** reconstruct the secret image  $S'$  from the  $k$  extracted small-sized shadow image  $SSC'_r, r = 1, 2, \dots, k$  using CRTSIS-SSI with the public parameters  $p, T$ , and  $N$ .

---

What is more, as an image protection method, the efficiency of MSISS-NS should be taken into consideration. As for SSS, one of the efficiency factors is recovery complexity. Additionally, in the

recovery process, the cost of time can be divided into two parts, the time of extracting  $SSC_l'$  from  $k$  or more than  $k$   $MSC_l$  and the time of recovering  $SSC_l'$  by CRTSIS-SSI. The complexity of these two parts will be analyzed separately.

The steganographic applications of CRT have been approved that the time and space complexity are  $O(e)$ , where  $e$  is the number of cover elements [28]. Additionally, the recovery process of CRTSIS-SSI requires only  $O(k)$  operations of modular method based on  $(k, n)$ -CRTSIS [8,11]. As these two parts are calculated serially and the time and space complexity can be seen as the superposition of two steps and MSISS-NS has linear time and space complexity.

#### 4. Experimental Results and Summaries

In this section, the experimental results and discussions will be introduced in order to show the effectiveness of our proposed scheme. Firstly, the shadow images and recovered results will be displayed, including the quality of shadow images. Additionally, then, the steganalysis experimental results between cover images and stego images will be exhibited to prove the undetectability and safety of the scheme. The comparisons with other related works will be presented. At last, brief summaries of the experiments will be given.

##### 4.1. Image Illustration

The database used to embed shares comes from [29] called MonoBase and the initial parameter of sensitivity  $ISO$  is 1000. The initial parameters of cover images are set:  $a = 2.5 \times 10^{-5}$ ,  $b = 8.0 \times 10^{-7}$ .

Figure 4 illustrates the histogram of embedding rate for MonoBase with cover sources switching  $ISO$  from 1000 to 1250 and  $E[E_r] = 1.30$  pbb. The embedding rate in [24] under the same condition is  $E[E_r] = 1.24$  pbb. When considering the size of shadow images, it can be inferred that the payload of cover images is more than the shadow images and the small-sized shadow images need no extra encoding or compressing operations to guarantee the safety.

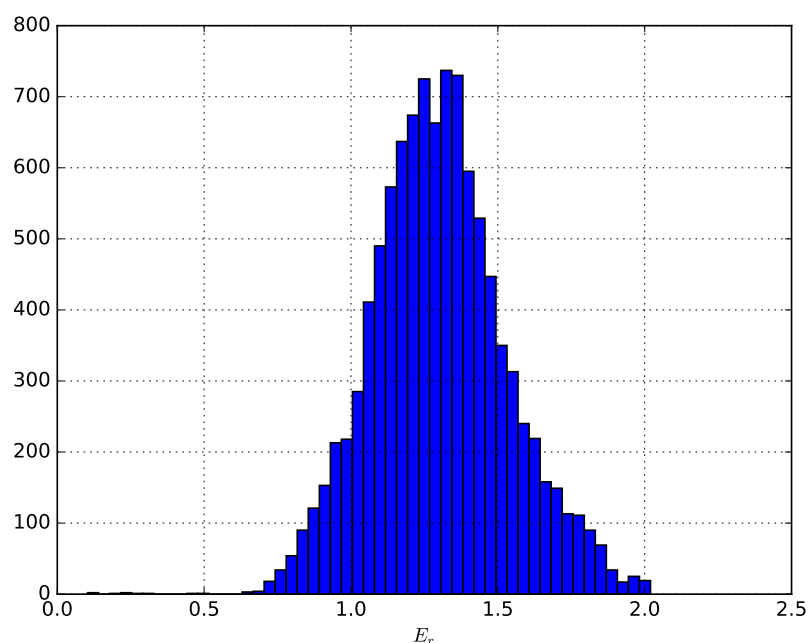
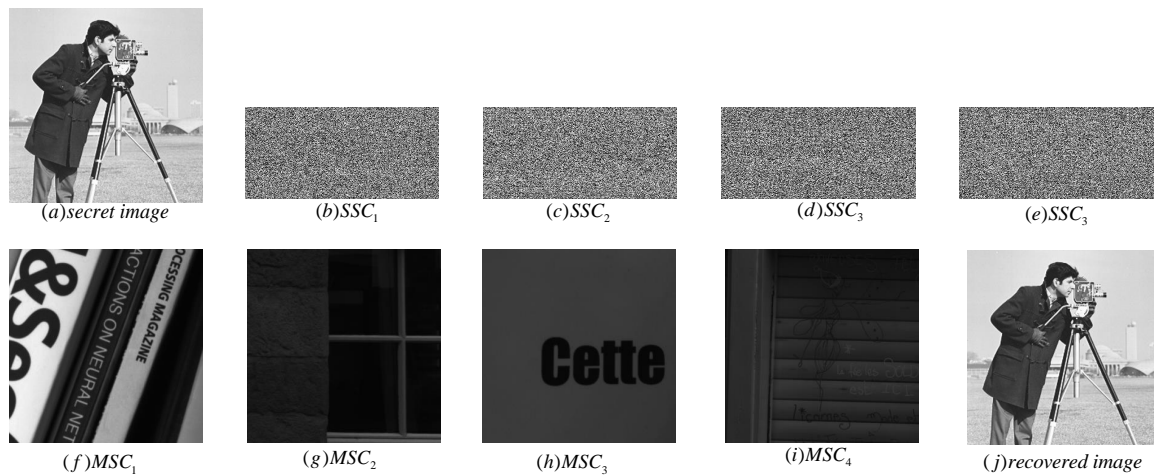


Figure 4. The histogram of embedding rate for MonoBase.

In Figure 5, the sharing results of  $(2, 4)$ -threshold MSISS-NS are presented. Figure 5a is the secret image with size  $(512 \times 512)$ . Figure 5b–e represent the shadow images after CRTSIS-SSI where  $r = 2$ ,  $p = 131$  and the size of (b)–(e) is  $\frac{5}{13}$  of (a). Figure 5f–i exhibits the meaningful shadow images embedded (b)–(e) with size  $(512 \times 512)$  and Figure 5j is the recovered image without loss. The cover

images are RAW images with 1000 *ISO* and the corresponding stego images *MSC* are generated by imitating ones with 1250 *ISO*.

As for the recovering process of MSISS-NS, the shadow images  $SSC_i$  are extracted from  $MSC_i$  and the recovery image is lossless.



**Figure 5.** The sharing results of (2,4)-threshold meaningful Secret Image Sharing scheme (Natural Steganography (MSIS-NS)).

Here, the quality of the shadow images is evaluated by peak signal to noise ratio (*PSNR*) and structural similarity (*SSIM*) to demonstrate the camouflage effect of the secret image. *PSNR* is defined as Equation (10).

$$PSNR = 10 \log_{10} \left( \frac{MAX_S^2}{MSE} \right) dB \quad (10)$$

where

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H [S'(i, j) - S(i, j)]^2 \quad (11)$$

*SSIM* is defined as Equation (12).

$$SSIM(x, y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [s(x, y)]^\gamma \quad (12)$$

where

$$\begin{aligned} l(x, y) &= \frac{2\mu_x\mu_y + C_1}{\mu_x^2\mu_y^2 + C_1} \\ c(x, y) &= \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2\sigma_y^2 + C_2} \\ s(x, y) &= \frac{2\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \end{aligned} \quad (13)$$

In Table 1, the visual quality of sharing images in Figure 5 is illustrated. Although NS is adopted to simulate the images with higher *ISO*, the high embedding rate of cover images leads to the similarity to cover images with 1000 *ISO*.

**Table 1.** The visual quality of the sharing images in Figure 5.

	Compared with Cover Images with 1000 ISO		Compared with Cover Images with 1250 ISO	
	PSNR	SSIM	SPNR	SSIM
MSC <sub>1</sub>	71.75	0.9999	27.79	0.9995
MSC <sub>2</sub>	79.93	0.9999	30.79	0.9989
MSC <sub>3</sub>	76.75	0.9999	45.94	0.9999
MSC <sub>4</sub>	78.66	0.9999	39.50	0.9977
Means	76.77	0.9999	36.01	0.9990

Several examples cannot absolutely show off the feasibility of MSIS-NS and more experiments are expected. [24] provides the cover images database MonoBase, including 10,320 images captured at 1000 ISO. However, some of these can be embedded successfully and the intersection of all methods is 9933, in other words, 96.25% RAW images provided can be adopted to contain secret information SSC. The visual quality of all meaningful shadow images is presented in Table 2. It turned out that the stego images are quite similar to cover images with 1000 ISO.

**Table 2.** The visual quality of the sharing images in MonoBase.

	Compared with Cover Images with 1000 ISO		Compared with Cover Images with 1250 ISO	
	PSNR	SSIM	SPNR	SSIM
Means	78.0787	0.9999	38.4145	0.9952

#### 4.2. Anti-Steganalysis Experiments

The sharing and recovering processes are displayed in Section 4.1, which just exhibits the visual quality of the sharing images. As the shadow images are hidden into the MonoBase, it is necessary and significant for steganalysis, while seldom previous work paid attention to that.

The spatial rich model (SRM) [30] is recognized as the most successful spatial steganalysis algorithm in the traditional steganalysis field because of its superior feature extraction method. It should be noted that the SRM feature sets combined with the Ensemble Classifier [31] (EC) are adopted for the following experiments. The performance of schemes is evaluated by detection error  $P_E$ , which is defined in Equation (14).

$$P_E \triangleq \min_{P_{FA}} \frac{1}{2} (P_{FA} + P_{MD}) \quad (14)$$

Table 3 displays the undetectability results of MSISS-NS and NS. There are two databases of cover images, consisting of 9933 RAW images captured at 1250 ISO (Cover-1250) and 9933 RAW images captured at 1000 ISO (Cover-1000). The database of stego images with MSISS-NS (denoted by Stego-MSISS) involves the 9933 RAW images that have been embedded with SSC to simulate the ones with 1250 ISO. The stego images embedded with shadow images by NS (denoted by Stego-NS) will be compared with Stego-MSISS to confirm the effect of MSISS-NS. From the results,  $P_E$  between Stego-MSISS and Cover-1250 is lower than that of Stego-NS and the value of  $P_E$  is higher between Stego-MSISS and Cover-1000, which means that Stego-MSISS is more similar to Cover-1000 than Cover-1250. Although NS is adopted in the scheme to simulate higher ISO images, the payload is sufficient to embed shadows so that stego images cannot be distinguished from Cover-1000 easily. And the more information is hidden into the cover images, the more resemble the stego images are to Cover-1250.

**Table 3.** The undetectability results between cover images with NS and MSISS-NS.

		Stego-NS	Stego-MSISS
$P_E$	Cover-1250	44.33%	30.23%
	Cover-1000	23.50%	45.12%

From above experiments, the cover images can be embedded with more information, how to deal with the redundant space also remains to be solved. One method is to attach random bits to the binary data string of shadow images, so that the embedded secret information is close to the maximum payload of each cover images and the stego images will be more alike to Cover-1250; another is to ignore extra space and operate as Stego-MSISS. What is more, pure random binary data strings are generated with the size close to the payload of each cover images and then embedded into covers, which is used to verify whether our shadow image is a random binary string, and whether it will affect the experimental results.

In Table 4, we compare the different results between two cover images databases and the above embedding contents. In this table, Stego-add represents the stego images that the steganography information is attached with random bits; Stego-ran is the stego images where random data is embedded.

**Table 4.** The comparison of undetectability results between Cover-1250, Cover-1000 with different embedding contents.

		Stego-Add	Stego-Ran
$P_E$	Cover-1250	39.44%	39.57%
	Cover-1000	20.64%	20.44%

The results presented in Table 4 prove that our shadow images, which have no influence on the results, are random, and with the increasing of embedded information, the stego images are closer to cover images with higher ISO.

Through above experiments, we have got 6 kinds of databases: the cover images with 1000 ISO (Cover-1000), the cover images with 1250 ISO (Cover-1250), the stego images embedded into information with [24] (Stego-NS), the stego images embedded into secret images directly by MSISS-NS (Stego-MSISS), the stego images embedded into secret images with random bits added by MSIS-NS (Stego-add), the stego images embedded into pure random bits by MSISS-NS (Stego-ran).

In the above Tables 3 and 4, the steganalysis results between the initial two cover images databases are exhibited. Additionally the steganalysis results among the stego images will be presented in Tables 5–7.

**Table 5.** The comparison of undetectability possibility results between Stego-NS and other stego images with different embedding contents.

Stego-NS	Stego-MSISS	Stego-Add	Stego-Ran
$P_E$	27.7%	44.84%	43.97%

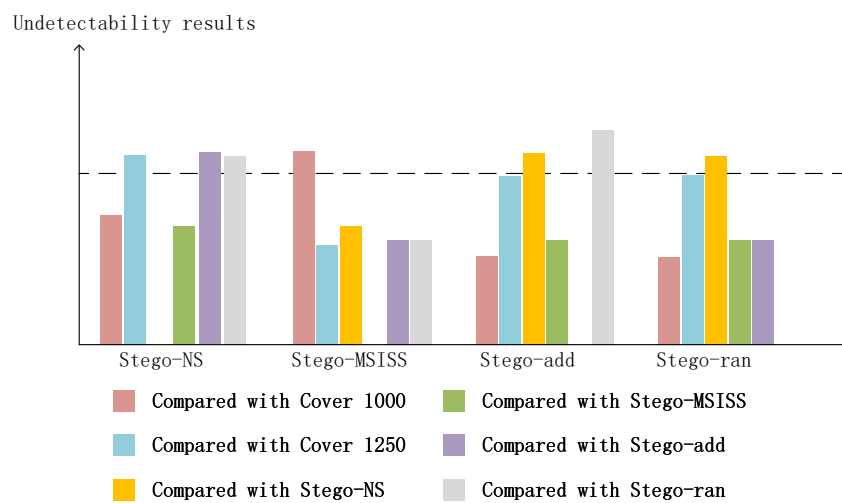
**Table 6.** The comparison of undetectability possibility results between Stego-MSISS with other embedding contents.

Stego-MSISS	Stego-Add	Stego-Ran
$P_E$	24.46%	24.33%

**Table 7.** The comparison of undetectability possibility results between embedding contents.

Stego-Add	Stego-Ran
$P_E$	50.01%

The above steganalysis results can be more intuitively observed in the Figure 6. The higher the bar is, the higher the undetectability possibility is, and the more similar the stego images are to the cover images. When the bar is near or even higher than the dotted line, it is considered that the stego images can hardly be separated from the cover images. Consequently, Stego-MSISS cannot be distinguished from cover images Cover-1000 and the remaining images are more similar to each other.

**Figure 6.** The undetectability possibility results among various kinds of images.

#### 4.3. Comparison with Other Works

In Section 1.2, several MSISS have been illustrated and MSISS-NS will be compared with them. Table 8 shows the comparison on characteristics among MSISS-NS and others works. Threshold, type of cover images and stego images, lossless recovery, pixel expansion, and steganalysis resistance will all be considered.

**Table 8.** The comparison on characteristics among different schemes.

Methods	Threshold	Secret Images	Shadow Images	Lossless Recovery	Pixel Expansion	Anti-Steganalysis
Li [16]	$(k, n)$	Grayscale	Grayscale	Yes	Yes	Not referred
Yuan [17]	$(n, n)$	Two-tone or four-tone image	Grayscale	Yes	Yes	Yes
He [20]	$(k, n)$	Grayscale	Grayscale	Yes	Yes	Not referred
Cheng [19]	$(n, n)$	Grayscale	Grayscale	No	No	Not referred
Chiu [21]	$(2, n)$	Binary Image	Binary Image	Progressive	No	Not referred
Maurya [22]	$(3, 3)$	Grayscale	Grayscale or color images	Yes	Yes	Not referred
Our Method	$(k, n)$	Grayscale	Grayscale	Yes	No	Yes

Additionally, in Table 9, the visual quality of related schemes will be measured by the means of PSNR and SSIM (MPSNR and MSSIM).

**Table 9.** The comparison on visual quality among different schemes.

Method	MPSNR (dB)	MSSIM
Li [16]	41.52	0.99
Yuan [17]	51.25	0.99
He [20]	54.01	0.99
Cheng [19]	42.44	0.98
Chiu [21]	12.84	0.19
Maurya [22]	43.42	0.29
Our Method	78.07	0.99

From the comparison results in Tables 8 and 9, we can conclude that our MSISS-NS scheme not only performs better in the visual quality than other methods, but also makes a good balance in lossless recovery and pixel expansion.

#### 4.4. Summaries

Moreover, according to the above results, several points can be summarized and explained, as follows.

- (1) The shadow images generated in sharing process by CRTSIS-SSI are random and safe and the detail inference and proof can be accessed in [11].
- (2) The shadow images generated by our MSISS-NS are understandable and the visual quality of sharing images is quite better than other similar schemes.
- (3) The capability of cover images, which is larger than that in [24], is actually enough to contain the generated small-sized shadow images. Thus no pixel expansion will occur.
- (4) Through the experiments above, two kinds of stego images are generated: Stego-MSISS, more similar to Cover-1000; and Stego-add, more similar to Cover-1250. According to the steganalysis results, Stego-MSISS compared with Stego-NS is more similar to Cover-1000. In the two pairs it is difficult to distinguish with each other. It may be because that the payload of NS with STC is really sufficient, and it is difficult to steganalyze the little change.
- (5) Nowadays, one of the serious challenges of steganalysis is mismatching. When we put four kinds of images, Cover-1000, Cover-1250, Stego-MSIS and Stegoadd, on the Internet at the same time, it will lead to a more serious mismatch problem and better confuse the judgment of steganalyzers to achieve the purpose of covert communication better.

## 5. Conclusions

In this paper, a  $(k, n)$ -threshold meaningful secret image sharing scheme that is based on Natural Steganography (MSISS-NS) is proposed. The scheme divides the secret image into  $n$  small-sized shadow images, which will be embedded into RAW images to simulate the ones with higher *ISO* parameters by STC. Additionally the computation complexity of MSISS-NS is approximately linear increasing. From the experimental results, the visual quality of the scheme is better than other methods. Besides, in the secret sharing process of MSISS-NS, the payload of NS is larger than the size of generated shadow images and as a result, which makes it possible for new embedding mode by adding random bits. When the two stego images and cover images can be accessed together, it will arouse mismatching problem to confuse steganalysis.

In addition, there are still some problems worthy for further study and discussion. There are other types of pictures besides RAW images and whether MSISS-NS can be extended to other types of images, e.g., JPEG images, is of great significance in practical application.

**Author Contributions:** Conceptualization J.C.; Data curation, J.C.; Formal analysis, X.Y.; Investigation, Y.L.; Methodology, Y.S.; Validation W.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491).

**Acknowledgments:** The authors would like to thank the editor and the anonymous reviewers for their valuable comments.

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

## References

1. Pouli, V.; Kafetzoglou, S.; Tsiropoulou, E.E.; Dimitriou, A.; Papavassiliou, S. Personalized multimedia content retrieval through relevance feedback techniques for enhanced user experience. In Proceedings of the 2015 13th International Conference on Telecommunications (ConTEL), Graz, Austria, 13–15 July 2015.
2. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [\[CrossRef\]](#)
3. Yang, C.N.; Yu, K.H.; Lukac, R. User-Friendly Image Sharing in Multimedia Database Using Polynomials with Different Primes. In *International Conference on Multimedia Modeling, Proceedings of the MMM 2007: Advances in Multimedia Modeling, Singapore, 9–12 January 2007*; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2007; Volume 4352 LNCS, pp. 443–452. [\[CrossRef\]](#)
4. Yan, X.; Lu, Y.; Liu, L.; Song, X. Reversible Image Secret Sharing. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3848–3858. [\[CrossRef\]](#)
5. Naor, M.; Shamir, A. Visual cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques, Proceedings of the EUROCRYPT 1994: Advances in Cryptology—EUROCRYPT'94, Perugia, Italy, 9–12 May 1994*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
6. Yang, C.N.; Chen, C.H.; Cai, S.R. Enhanced Boolean-based multi secret image sharing scheme. *J. Syst. Softw.* **2016**, *116*, 22–34. [\[CrossRef\]](#)
7. Mignotte, M. How to Share a Secret. *Eurocrypt* **1982**, *149*, 371–375.
8. Asmuth, C.A.; Bloom, J. A Modular Approach to Key Safeguarding. *Inf. Theory IEEE Trans.* **1983**, *29*, 208–210. [\[CrossRef\]](#)
9. Yan, X.; Lu, Y.; Liu, L.; Wan, S.; Ding, W.; Liu, H. Chinese Remainder Theorem-Based Secret Image Sharing for  $(k, n)$  Threshold. In *International Conference on Cloud Computing and Security, Proceedings of the ICCCS 2017: Cloud Computing and Security, Krakow, Poland, 11–14 July 2017*; Springer: Cham, Switzerland, 2017; pp. 433–440.
10. Li, L.; Lu, Y.; Yan, X.; Liu, L.; Tan, L. Lossless  $(k, n)$ -Threshold Image Secret Sharing Based on the Chinese Remainder Theorem Without Auxiliary Encryption. *IEEE Access* **2019**, *7*, 75113–75121. [\[CrossRef\]](#)
11. Chen, J.; Liu, K.; Yan, X.; Liu, L.; Zhou, X.; Tan, L. Chinese remainder theorem-based secret image sharing with small-sized shadow images. *Symmetry* **2018**, *10*, 340. [\[CrossRef\]](#)
12. Ateniese, G.; Blundo, C.; Santis, A.D.; Stinson, D.R. Extended capabilities for visual cryptography. *Theor. Comput. Sci.* **2001**, *250*, 143–161. [\[CrossRef\]](#)
13. Zhou, Z.; Mu, Y.; Wu, Q.M.J. Coverless image steganography using partial-duplicate image retrieval. *Soft Comput.* **2018**. [\[CrossRef\]](#)
14. Yan, X.; Lu, Y.; Liu, L. General Meaningful Shadow Construction in Secret Image Sharing. *IEEE Access* **2018**, *6*, 45246–45255. [\[CrossRef\]](#)
15. Lin, C.C.; Tsai, W.H. Secret image sharing with steganography and authentication. *J. Syst. Softw.* **2004**, *73*, 405–414. [\[CrossRef\]](#)
16. Li, P.; Kong, Q.; Ma, Y. Image Secret Sharing and Hiding with Authentication Based on PSNR Estimation. *J. Inf. Hiding Multimed. Signal Process.* **2014**, *5*, 353–366.
17. Yuan, H.D. Secret sharing with multi-cover adaptive steganography. *Inf. Sci.* **2014**, *254*, 197–212. [\[CrossRef\]](#)
18. Avci, D. A novel meaningful secret image sharing method based on Arabic letters. *Kuwait J. Sci.* **2016**, *43*.
19. Cheng, T.F.; Chang, C.C.; Liu, L. Secret sharing: Using meaningful image shadows based on Gray code. *Multimed. Tools Appl.* **2017**, *76*, 1–26. [\[CrossRef\]](#)
20. He, J.; Lan, W.; Tang, S. A secure image sharing scheme with high quality stego-images based on steganography. *Multimed. Tools Appl.* **2017**, *76*, 7677–7698. [\[CrossRef\]](#)
21. Chiu, P.L.; Lee, K.H. Efficient constructions for progressive visual cryptography with meaningful shares. *Signal Process.* **2019**, *165*, 233–249. [\[CrossRef\]](#)

22. Maurya, R.; Kannojiya, A.K.; Rajitha, B. An Extended Visual Cryptography Technique for Medical Image Security. In Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 415–421.
23. Hassanien, A.E.; Azar, A.T.; Snasael, V.; Kacprzyk, J.; Abawajy, J.H. Big data in complex systems. In *SBD*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9.
24. Bas, P. Steganography via cover-source switching. In Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, 4–7 December 2016.
25. Bas, P.; Filler, T.; Pevn, T. “Break Our Steganographic System”: The Ins and Outs of Organizing BOSS. In Proceedings of the Information Hiding—13th International Conference, IH 2011, Prague, Czech Republic, 18–20 May 2011. Revised Selected Papers.
26. Denemark, T.; Fridrich, J. Side-informed steganography with additive distortion. In Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 16–19 November 2015; pp. 1–6.
27. Foi, A.; Alenius, S.; Katkovnik, V.; Egiazarian, K. Noise measurement for raw-data of digital imaging sensors by automatic segmentation of nonuniform targets. *IEEE Sens. J.* **2007**, *7*, 1456–1461. [\[CrossRef\]](#)
28. Filler, T.; Judas, J.; Fridrich, J. Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 920–935. [\[CrossRef\]](#)
29. Bas, P. Monobase. Available online: <http://patrickbas.ec-lille.fr/MonoBase/> (accessed on 22 July 2016).
30. Fridrich, J.; Kodovsky, J. Rich models for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 868–882. [\[CrossRef\]](#)
31. Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 432–444. [\[CrossRef\]](#)



© 2020 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 (<http://creativecommons.org/licenses/by/4.0/>).