IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 7, 2021, accepted January 29, 2021, date of publication February 3, 2021, date of current version February 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3056893

Robust Secret Image Sharing Scheme Against Noise in Shadow Images

YUYUAN SUN, YULIANG LU, XUEHU YAN, LINTAO LIU, AND LONGLONG LI
National University of Defense Technology, Hefei 230037, China
Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

Corresponding author: Yuliang Lu (publicLuYL@126.com)

This work was supported by the National Natural Science Foundation of China under Grant 61602491.

ABSTRACT The (k, n)-threshold secret image sharing scheme is an image protection method, whose security comes partly from precise mathematical calculations, and even a little change in shadow images will lead to a false recovered image. Thus, it is crucial to recover the secret image information in the presence of possible noise on shadow images, which has rarely been considered in previous work. In this paper, a robust (k, n)-threshold polynomial-based secret image sharing scheme(RPSIS) against noise on shadow images is proposed, which depends on the randomness of the sharing phase without any other techniques, such as steganography. Additionally, pixel expansion caused by the direct application of error correction codes is avoided. Experimental results and theoretical proof confirm the effectiveness of our scheme. The shadow images of the scheme are of the same size as secret image and the security of the scheme is also maintained with no information leakage. Even though the shadow images are modified by noise, the original secret image can be reconstructed without loss under the error correction capability, which provides more possibilities for the practical application of secret image sharing.

INDEX TERMS Polynomial, secret image sharing, random elements, error-correction codes, robustness.

I. INTRODUCTION

A. SECRET SHARING SCHEME

Since the secret sharing scheme(SSS) was proposed by Shamir [1] and Blakley [2] respectively in 1979, it has been widely utilized in the field of information protection. The main concept of secret image sharing is ''sharing''. A (k, n)-threshold secret image sharing scheme involves following steps. The secret image is divided into n individual keys, which are generally called shares or shadow images, and then they are distributed and transmitted to n different participants or holders through different channels. During the recovery process, the secret information can only be obtained when at least k shares are acquired and no information will be revealed if the number of shadow images accessed is less than k. Different from other information protection methods, secret sharing scheme does not depend on the security of a single channel. Even if one shadow image is lost, the secret image can also be reconstructed.

Therefore, secret sharing has attracted much attention of researchers due to the advantages as follows: (1) guarantees the security and integrity of a secret when sufficient shares are provided to reconstruct the initial information; (2) prevents the abuse of the sharing function caused by excessive concentration of power; (3) improves the reliability of the confidential information transmission process without increasing risk. In general, secret sharing schemes have important applications in multi-party security computing, authority control, lightweight recovery, multi-channel covert communication and other areas.

Among various forms of information, visual information accounts for approximately 80% of the information obtained from the outside world. Additionally, along with the development of multi-media technology, the access and spreading of digital images are becoming more convenient. Thus, the secret image sharing scheme has a broader prospect. To date, many researchers have been involved in the development of this field. According to the techniques used, secret image sharing has many branches, including polynomial-based secret image sharing [1], [3], visual cryptography [4], [5], Boolean operation-based secret image sharing [6], cellular automaton-based secret image sharing [7], [8], Chinese Reminder Theorem-based secret image sharing [9]–[11] and so on.

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

Compared with other secret image sharing schemes, polynomial-based secret image sharing is always adopted because of lossless recovery. The other schemes, like visual secret image sharing, remain several questions, such as pixel expansion, low visual quality and loss recovery. Although the schemes have the advantage of simple recovery calculation, they are not suitable in the case of high image quality requirements.

B. IMAGE NOISE

The image noise is often expressed as an isolated pixel or a pixel block that causes a strong visual effect. Generally, the noise signal is not related to the object to be studied. It appears in the form of useless information and disturbs the observable information of the image. In other words, noise makes the image unclear.

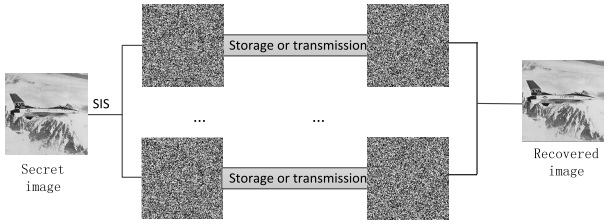
There are two main sources of image noise. One is the process of image acquisition. The noise will be produced in images due to the influence of sensor material properties, the working environment, electronic components and circuit structure. The other source is the process of image signal transmission. Because of the imperfection of the transmission medium and recording equipment, digital images are often polluted by many kinds of noise in the process of transmission and recording. In addition, when the input object is not as expected, noise will be introduced into the resulting image during some aspects of image processing,.

Image noise refers to unnecessary or redundant interference information existing in image data. Image noise hinders people's acceptance of its contents, and the impact of noise should be reduced as much as possible.

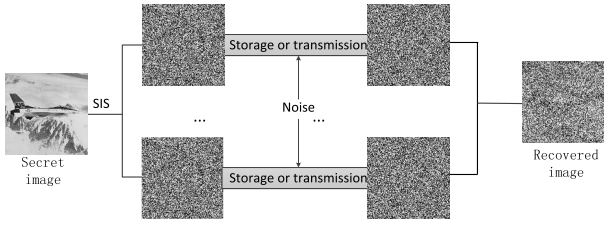
C. MOTIVATION

It is remarkable that the security and effectiveness of the above secret image sharing schemes are based on mathematical models and precise calculation. In other words, a slight change can lead to completely different recovery results. Meanwhile, due to the imperfection of transmission and storage medium, digital images are often polluted by many kinds of noises [12]. In addition, when the format of input images is not as expected, noise may also be introduced into the results in some parts of image processing [13].

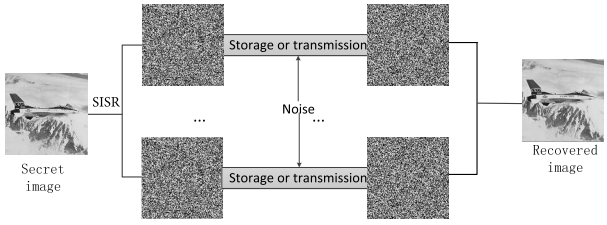
The motivation of our paper is to recover the secret image without loss or to improve the visual quality of the recovered image when the shadow images are polluted by noise. In Figure. 1 (a), the secret can be recovered correctly when there is no noise, even though the scheme has no robustness. However, it cannot be ignored that the shadow images may be affected by various kinds of noise, modification or other destruction in the process of storage or transmission. Figure. 1 (b) represents this occasion, where the shadow images are all added with the least significant bit flipping noise and the recovered image cannot be recognized at all. Thus, it is important to research secret image sharing with robustness to share noise(robust secret image sharing). In Figure. 1 (c), even if the shadow images are polluted by



(a) Recovered results with shadow images generated by scheme without robustness and not polluted by noise



(b) Recovered results with shadow images generated by scheme without robustness and polluted by noise



(c) Recovered results with shadow images generated by scheme with robustness and polluted by noise

FIGURE 1. The motivation of our scheme and the possible effect of recovered results with shadow images generated by scheme with robustness and polluted by noise. Figure 1(a) The recovered results with shadow images generated by scheme without robustness and not polluted by noise; Figure 1(b) The recovered results with shadow images generated by scheme without robustness and polluted by noise; Figure 1(c) The recovered results with shadow images generated by scheme with robustness and polluted by noise.

the same kind noise as that in Figure. 1, our robust secret image sharing scheme can resist noise on shadow images in the process of transmission or storage, and the correct secret image can be obtained, which is the main motivation of our paper.

Robust secret image sharing can be applied when the visual quality of the recovered image is high and the communication condition is poor. In addition, robustness provides more possibilities for the practical application of secret image sharing. Robust secret image sharing can also be applied in other field, like steganography and watermarking.

Although some papers claim that their secret image sharing schemes are robust, they actually pay more attention to identity authentication than resisting noise. Identity authentication focuses on the reliability and correctness of the source. We expect that the noise and errors for various reasons can be corrected without additional burden in the proposed robust secret image sharing.

Certain questions on robust secret image sharing need to be solved: how does one correct the errors in shadow images aroused during storage or transmission? How does one achieve the previous goal and ensure the shadow images have no pixel expansion in the meantime?

D. OUR CONTRIBUTION

In this paper, a robust polynomial-based secret image sharing against noise on shadow images(RPSIS) without pixel expansion is proposed.

There are some random elements in secret image sharing that can be utilized [14]. In our scheme, the share is generated by screening proper random numbers to make the share value the same as checksum of other pixels' share, and shadow images have the same size as initial secret image.

The main contribution of this paper is as follows.

1) The proposed scheme can be recovered without loss when k shadow images are accessed and there will be no information leakage when less than k shadow images are aggregated.
2) The proposed scheme is robust to some typical noise types, *e.g*, least significant bit(LSB) flipping noise, Gaussian noise, JPEG-compression noise and others.
3) Different from the existing schemes, the shadow images of the proposed scheme have no pixel expansion under the premise of ensuring the robustness of the scheme.

The arrangement of the sections is as follows. Section II introduces related work about robust secret image sharing and preliminaries utilized in our scheme; in Section III, we discuss the established RPSIS algorithm in detail; Section IV presents the performance analysis and theoretical proof; Section V provides experimental results of the algorithm and discusses parameters that may influence the effectiveness; and Section VI is the conclusion.

II. RELATED WORKS AND PRELIMINARIES

In this section, we will introduce the related work of robust secret image sharing and preliminaries used in our scheme.

A. RELATED WORKS

The security of secret image sharing is sometimes based on the rights given to the dealer and participants. When the dealer and participants are honest and reliable, the recovered result will be correct and trustworthy. While the dealer and participants are not always reliable, the level of correctness and trust reduces, and the possibility of lossless recovery are also reduced. secret image sharing can be separated into two categories according to the rights of dealer and participants [15].

1) VERIFIABLE SECRET SHARING

In this occasion, not all participants are honest, which means that attackers pretend to be the participants to get the real shadow images and secret image information from the dealer. To prevent this attack, identity authentication is necessary so that the dealer can verify the rights and correctness of the shadow images provided to prevent information from being obtained by attackers.

Rabin and Ben-Or [16] added identity authentication to the secret sharing protocol, which demonstrated the necessity and importance of the ''Information Checking'' idea. Since then, the correctness and reliability of shadow images have been investigated. Blundo and De Santis [17] showed up the lower bounds for verifiable secret sharing schemes. Liu *et al.* [18] exhibited a secret sharing scheme based on symmetric bivariate polynomial to identify faults and cheaters.

2) ROBUST SECRET SHARING

This kind of scheme allows the recovery of the secret in the case of some shares becoming corrupted due to some adversary actions.

One method is to embed the shadow images into n cover images with robust steganography so that the embedding extents will be unchanged even if the stego images are polluted by various noise. For example, Espejel *et al.* [19] exhibited a robust cheating-prevention mechanism for hierarchical secret image sharing using watermarking. Ghebleh and Kanso [20] proposed a polynomial-based secret image sharing scheme joint with steganography to achieve this purpose. However, the scheme has high computational complexity and pixel expansion. The shadow images are like 'watermarking' present in stego images. No matter how the stego images are transformed, the 'watermarking' can still be extracted. However, the approaches combine secret image sharing and robust steganography, and the information contained in cover images is limited, while the robustness comes from steganography instead of secret image sharing itself.

With the help of error-correction code, the dealer can distinguish and correct the modified shadow images. Cramer *et al.* [21] presented a linear secret sharing scheme based on linear error-correction codes and linear universal hash functions. This scheme can verify for $n/3 \leq t \leq (1-\varepsilon) \cdot n/2$ corrupted shares, while the size of each share is $O(L+\lambda)$, where λ is the security parameter, larger than that of secret $O(L)$. Cheraghchi [22] showed a nearly optimal secret sharing method, which employs Reed-Solomon codes to tag a secret image to verify $\delta n, \delta \in (0, 1/2)$ unreliable partners or shares and the size of shares is $L(1+o(1))+O(\lambda)$.

The approaches above are suitable for data secret sharing, and if they are extended to secret image sharing, image features should be considered carefully. Additionally, the above scheme can resist the change of a limited number of shadow images, and the size of each share is larger than that of the secret image.

In [23], a scheme combing secret image sharing and Reed-Solomon codes was proposed, aiming to resist the share noise. This scheme only gave the idea, instead of mentioning the specific details. Rishiwal *et al.* [24] displayed a robust secret image sharing scheme, which simply combined a sharing

algorithm and secure part. Wang *et al.* [25] put forward a secret image sharing scheme with identity authentication based on compressive sensing(CS). Although the size of shares in the scheme is flexible, the recovered image cannot be restored withour loss at all, and the ability of error resilience can be improved.

According to related research on robust secret image sharing, the following questions remained to be solved. First, some of the existing schemes only provide the function of checking correctness instead of dealing with errors and focus on the secret data sharing, which needs to apply an error-correction code into the scheme. It is better to avoid the problem of pixel expansion, wasting extra storage or transmission space.

B. POLYNOMIAL-BASED SECRET IMAGE SHARING

Shamir first proposed the (k, n)-threshold polynomial-based secret sharing scheme(PSSS). In the scheme, the dealer utilizes a $k-1$ degree polynomial in the field $GF(p)$ in Eq. 1. The constant term is replaced by secret data S, and other coefficients of the polynomial, denoted as $a_1, a_2, \ldots, a_{k-1}$, are randomly selected.

$$f(x) = S + \sum_{j=1}^{k-1} a_j x^j \bmod p. \tag{1}$$

Finally, n shares are generated by giving different variables $y_i = f(x_i)$ to participants P_i.

When any k or more than k pairs (x_i, y_i) are present, the polynomial $f(x)$ and the secret S can be recovered by using Lagrange interpolation, as shown in Eq. 2.

$$f(x) = \sum_{i=1}^{k} f(x_i) \prod_{\substack{l=1 \\ l \neq i}}^{k} \frac{(x - x_l)}{(x_i - x_l)} \tag{2}$$

Thien and Lin [26] introduced polynomial-based secret sharing into image (polynomial-based secret image sharing, PSIS), where the size of each share was $1/k$ of that of the secret image and the calculation was performed under $GF(251)$. However, the scheme utilizing all coefficients in the polynomial for secret sharing was proved to be not secure. When polynomial-based secret sharing is extended to secret image sharing, one of the problems to be solved is the choice of prime numbers. Considering that the pixel value of a bitmap image ranges from 0 to 255, there are two prime numbers close to this range. One is 251, but the secret pixel larger than 251 cannot be shared and recovered without loss. The other is 257, and the sharing value larger than 255 cannot be saved in the bitmap image, while the sharing process should be performed again until the bitmap image can save the shared value. With this choice, the secret image can be recovered without loss.

Since then, various studies focusing on polynomial-based secret image sharing have made notable progress. For example, Yang *et al.* [27] proposed a user-friendly image sharing scheme in a multimedia database using polynomials with different primes. Liu *et al.* [28] presented the polynomial-based extended secret image sharing scheme with reversible and unexpanded covers. In [29], an efficient and lossless polynomial-based secret image sharing for images in $GF(2^8)$ was presented by Gong *et al.* Li *et al.* [30]utilized visual cryptography(VC) to achieve two-in-one VC scheme. When there is no computing device, the damaged image can be previewed by superimposing the shares together; when there exists a computing device, the original secret image can be reconstructed with better quality by Lagrange interpolation.

In summary, polynomial-based secret image sharing is the most basic method in this field because of its characteristics, *e.g.*, higher restoration quality, flexible size of shadow images, fewer public parameters, unlimited (k, n)-threshold and direct application to grayscale and color images. In this paper, the shares of our scheme will be generated by polynomial-based secret image sharing.

C. ERROR CORRECTION CODE

Error correction code(ECC) [31] is a code that can automatically correct errors in data transmission at the receiving end. The basic idea of error correction code is to pick out only a part of all sequences composed of transmission symbols as the representative of information to send to the channel, and make the selected sequences have as many differences as possible. In other words, ECC must add extra symbols to the original code words to enlarge the difference between code words, so that when one code word is wrong on a certain number of symbols, it will not be wrong in another code word.

There are many kinds of error correction codes, among which the codes based on algebra are called algebraic codes, and linear codes are the most common. The information bits and supervision bits in linear codes are connected by some linear algebraic equations. Furthermore, there is an important type called cyclic code, which is established on the basis of rigorous algebraic mathematics theory. The coding and decoding equipment of this type are not too complex, and the ability to perform error detection and correction is strong.

According to the given (n_0, k_0) value, a $(n_0 - k_0)$ degree polynomial is selected as generator polynomial $g(x)$ from the factor $(x^{n_0}+1)$. In the encoding phase, multiply encoding data $m(x)$ by $x^{n_0-k_0}$, which is actually adding $n_0 - k_0$ zeros after the codes. Then, divide $g(x)$ by $x^{n_0-k_0}m(x)$ to get quotient $Q(x)$ and remainder $r(x)$, that is

$$\frac{x^{n_0-k_0}m(x)}{g(x)} = Q(x) + \frac{r(x)}{g(x)}. \tag{3}$$

And the code after coding is

$$T(x) = x^{n_0-k_0}m(x) + r(x). \tag{4}$$

In the decoding process, the receiver information code $R(x)$ is divided by the generator polynomial $g(x)$ to obtain the remainder $r(x)$. If $r(x)$ is equal to zero, there is no error during the transmission; otherwise, the wrong pattern $E(x)$ can be obtained by looking up the table or by performing some kind of calculation. By subtracting $E(x)$ from $R(x)$,

we can get the original code group $T(x)$that the error code has been corrected.

The robustness of our scheme is derived from ECC. It should be noted that capability of error correction is based on information redundancy. However, the redundancy will lead to extra storage space and transmission bandwidth, which is also the difficulty and innovation of our scheme.

III. THE PROPOSED SCHEME

In this section, we will first introduce the notations and their meanings. Then, the model of random elements utilized for RPSIS will be presented. The details of RPSIS will be described next.

A. NOTATIONS

In this (k, n)-threshold robust polynomial-based secret image sharing scheme(RPSIS), $W \times H$ is used to denote the size of the original secret image, and k_0, n_0, t_0 are the size of message length, codeword length, and error-correction capability, respectively in ECC. Additionally, $ECC(x)$ represents the operation of encoding of x, and the corresponding check bits are $r(x)$. In RPSIS, the secret image is divided into 4 blocks evenly. WL means the pixel number in each pixel block, and HL is the number of bit planes for each pixel. Furthermore, the above symbols need to satisfy following conditions: $HL \times WL \geq n_0$, $\frac{HL}{2} \times WL \leq k_0$.

During the process of generating shadow images, MAX_S means the maximum value of the image pixel value space, and MAX_b is the number of bits required to represent the pixel value of the image. In general, MAX_b and HL are equal.

In our RPSIS, the robustness comes from ECC, where binary encoding is the most common. Thus, pixel values need to be turned to binary values, and specific bits are extracted. Additionally, the high m bits for decimal value v can be obtained as Eq. 5.

$$H_m(v) = [v]_B \gg (8 - m) \tag{5}$$

While the low n bits for decimal value v are obtained as Eq. 6.

$$L_n(v) = ([v]_B \ll (l - n)) \gg n \tag{6}$$

In Eq. 5 and Eq. 6, $[v]_B$ means that v is converted to binary, $\gg$ and $\ll$ are right shift and left shift operation respectively.

B. RANDOM ELEMENTS UTILIZATION MODEL

In $f(x_t) = s + x_t a_1 + \ldots + {x_t}^{k-1} a_{k-1} (\mathrm{mod} P), t = 1, 2, \ldots, n, a_i (1 \leq i \leq k-1)$ can be chosen randomly. In fact, different elements lead to different share values. If the share values are restricted, proper a_m needs to be found, and more information can be contained in share values.

With this thought shown in Figure. 2, after the secret value is shared to n shares, their corresponding checksum of lower b bits with ECC can be obtained. If the shares of the next secret value contain the checksum, the next shares can check and correct the errors without redundancy. Considering that the lower bits are more easily changed, higher bits are chosen to monitor the change or the error of lower bits.

The random elements utilization model for RPSIS is exhibited in Eq. 7.

$$\begin{aligned} &\sum_{t=1}^{n} \left| r\left(L_{\frac{HL}{2}}\left(f_i(x_t)\right)\right) - H_{\frac{HL}{2}}\left(f_{i+1}(x_t)\right) \right| (\mathrm{mod} P) = 0 \\ &s.t. \begin{cases} f_i(x_t) = s_i + \sum_{l=1}^{k-1} a_l {x_t}^l, f_i(x_t) \in [0, 255] \\ a_l \in Z, a_l \in [0, P) \\ t = 1, 2, \ldots, n \end{cases} \end{aligned} \tag{7}$$

In Eq.7, x_t is the serial number, $f_i(x_t)$ means the t-th sharing value in the i-th pixel block, $L_{\frac{HL}{2}}(f_i(x_t))$ represents the higher $\frac{HL}{2}$ bits of $f_i(x_t)$, it is encoded by ECC and the codeword is composed of $f_i(x_t)$ and its corresponding checksum $r(L(f_i(x_t)))$, $H_{\frac{HL}{2}}(f_{i+1}(x_t))$ denotes the higher $\frac{HL}{2}$ bits of sharing value $f_{i+1}(x_t)$ in the $(i+1)$-th block.

In the random elements utilization model, it is required that the checksum of lower bits that are more likely changed after ECC encoding should be the same as that of the higher bits of the sharing value in the next pixel block.

If more secret values are encoded together, the encode data is the combination of lower bits in each value, and their checksum constitutes the higher bits of values in the next secret block. The branch and bound method or Monte Carlo method can be used to solve the above model.

C. SHARING PHASE

The flowchart of our RPSIS algorithm is exhibited in Figure. 3. In this flowchart, $WL = 4$ and $HL = 8$ are taken as examples to explain the algorithm.

In Algorithm 1, there are some points that should be noted.

1) This scheme can be used on grayscale images and color images, and in this paper we will introduce grayscale images as an example.
2) In the sharing process, it is suggested to adopt 257 as the prime number to recover the secret image without loss, which can guarantee the secret value can recovered without loss.
3) The threshold is restricted, and the details can be obtained in Section IV.
4) In order to make Algorithm 1 more understandable, we take S and $(HL, WL) = (8, 4)$ as an example in Figure. 3 to explain the idea of our algorithm. In fact they are not the unique feasible parameters. Further discussion will be introduced in Section V-D.
5) In Setp 1, the choice of pixels in the blocks should be scattered as far as possible to avoid the noise at a certain place influencing the recovery of ECC; therefore, we construct the pixel blocks in the order $'S_1 \rightarrow S_4 \rightarrow S_2 \rightarrow S_3'$. If $WL > 4$, repeat the order until the pixel number in PB_i equals to WL; if $WL < 4$, PB_{i+1} continues to form pixel block according to the above order after PB_i end.
6) Step 2 selects appropriate serial numbers $x_1, x_2, \ldots, x_n$, and not all combinations of numbers satisfy the

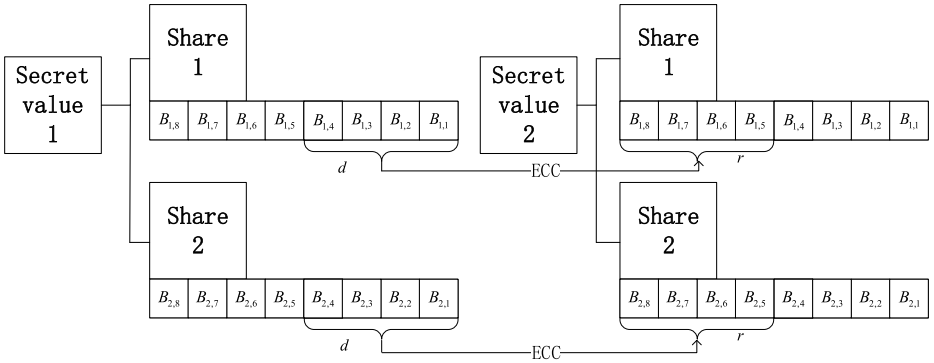


FIGURE 2. Thought for random elements utilizing model.

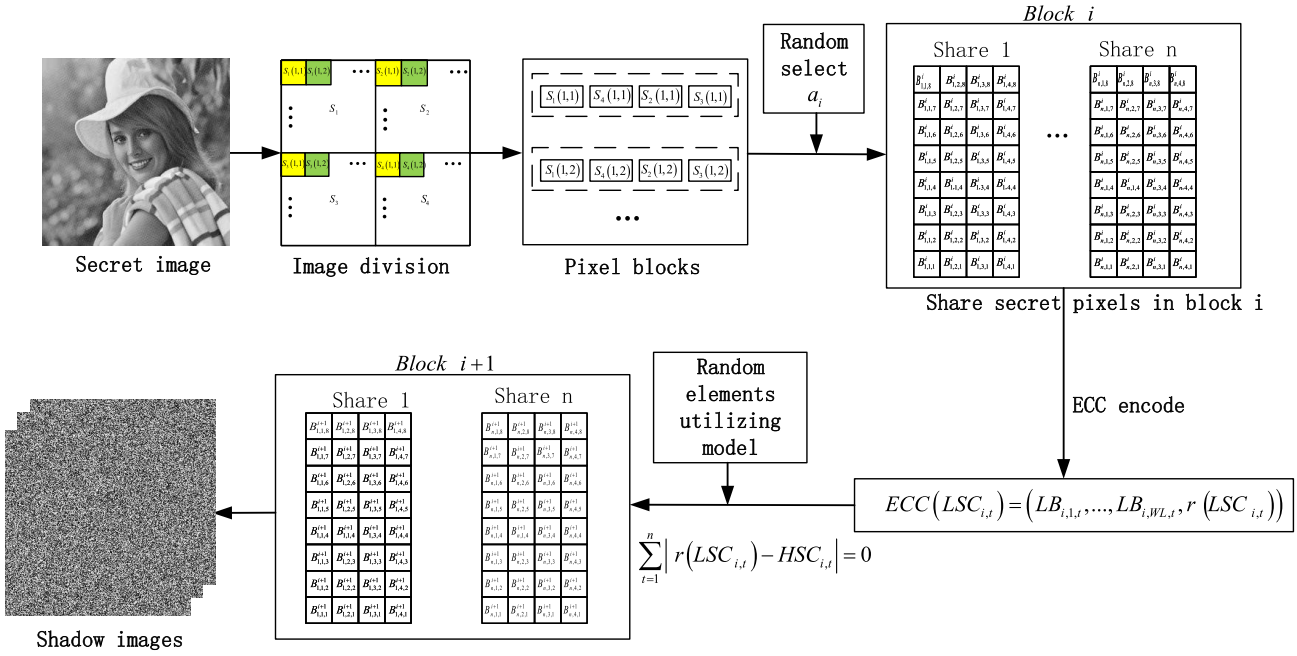


FIGURE 3. Flow chart of the sharing process of the (k, n)-threshold robust polynomial-based secret image sharing scheme.

condition that the checksum of low bit planes in the i-th block is equal to the high bit planes in the $(i+1)$-th block. If the current serial numbers fail to meet the above condition, select the numbers again. In section V-D, we will further discuss the selection of serial numbers.

7) In fact, the screening operation in Step 6 is unsuitable for the first block, which is processed independently. The last block does not require Step 5-6 because there is no extra block for storing the checksum.

D. RECOVERY PHASE

For Algorithm 2, we should clarify the following points.

1) Algorithm 2, in fact, is the reverse procedure of Algorithm 1.
2) When more than k shadow images are obtained, the secret image can be recovered.
3) Considering that the low bits of pixels are more vulnerable, the algorithm is designed to check and correct errors in $LSC_{i,t}$. While high bits of pixels are more weighted, the data bits and checksum bits can be exchanged if necessary.
4) The last block needs no error correction process in Step 3-4; it can be recovered directly.
5) The error-correction capability of the algorithm will be definitively shown in section IV.

IV. PERFORMANCE ANALYSIS AND THEORETICAL PROOF

In this section, the performance analysis and theoretical proof of the proposed RPSIS scheme will be presented.

Algorithm 1 The Sharing Process of the (k, n)-Threshold Robust Polynomial-Based Secret Image Sharing Scheme

Input: A grayscale secret image S with size of $W \times H$, (k, n)-threshold, block parameters (HL, WL), and $ECC(k_0, n_0, t_0)$.

Output: Shadow images SC_i, and their corresponding serial numbers x_i, for $i = 1, 2, \cdots n$.

Step 1: Divide the secret image S into four parts S_1, S_2, S_3, S_4 as Figure. 3. Follow the order $S_1 \rightarrow S_4 \rightarrow S_2 \rightarrow S_3$ to pick up pixels in the same position of four parts in S to construct the pixel blocks PB_i, $1 \leq i \leq \frac{W \cdot H \cdot MAX_b}{WL \cdot HL}$.

Step 2: Select appropriate serial numbers $x_1, x_2, \ldots, x_n$ to ensure that the qualified share values can be obtained during the screening process.

Step 3: Pixel blocks PB_i are shared in turn, and Step 4 is repeated to process each secret pixel in PB_i.

Step 4: Let $a_0 = PB_i(wl)$, where wl denotes the position of the current processed secret pixel in the i-th pixel block. Randomly select $a_m, m = 1, 2, \ldots, k-1$. Then, the sharing values of wl-th pixel in the block can be separately calculated as Eq.8, $t = 1, 2, \ldots, n$, $wl = 1, 2, \ldots, WL$.

$$f_{wl}(x_t) = a_0 + a_1 x_t + a_2 {x_t}^2 + \ldots + a_{k-1} {x_t}^{k-1} (\mathrm{mod} P) \tag{8}$$

Step 5: Through Step 4, the shares of all pixels in PB_p, denoted by $PSC_{i,t}$, can be exhibited as shown in Eq. 9.

$$PSC_{i,t} = (f_1(x_t), f_2(x_t), \ldots, f_{WL}(x_t)) \tag{9}$$

Step 6: The lower bits of $PSC_{i,t}$ are encoded by ECC. That is $ECC\left(LSC_{i,t}\right) = \left(LB_{i,1,t}, LB_{i,2,t}, \ldots, LB_{i,WL,t}, r\left(LSC_{i,t}\right)\right)$, where $LB_{i,wl,t} = L_{\frac{HL}{2}}\left(f_{wl}\left(x_t\right)\right)_i = \left(\left[f_{wl}\left(x_t\right)\right]_B \ll \left(\frac{HL}{2}\right)\right) \gg \frac{HL}{2}$ and $r\left(LSC_{i,t}\right)$ is checksum. For $ECC\left(LSC_{i,t}\right)$, $LSC_{i,t}$ is the t-th sharing values of pixel values in the i-th pixel block, which is saved in the position, and the checksum $r\left(LSC_{i,t}\right)$ is seen as the constraint condition to generate sharing values of pixel values in the $(i+1)$-th block.

Step 7: Repeat Step 4-6 for the pixels in the $(i+1)$-th block until $\sum_{t=1}^{n} \left| r\left(LSC_{i,t}\right) - HSC_{i+1,t} \right| = 0$.

Step 8: If all blocks are shared, goto Step 9; otherwise, let $i = i+1$ and then go to Step 4 to encrypt pixels in the next block.

Step 9: Make sure that each pixel of shares in the blocks returns to the same position as the corresponding secret pixel, and then output n grayscale shadow images $SC_1, SC_2, \ldots, SC_n$.

Algorithm 2 The Recovery Process of the (k, n)-Threshold Robust Polynomial-Based Secret Image Sharing Scheme

Input: Any t grayscale shares $SC'_{i_1}, SC'_{i_2}, \cdots SC'_{i_t}$, their corresponding serial numbers $x_{i_1}, x_{i_2}, \cdots x_{i_t}$ $(t \geq k)$, prime number p, block parameters (HL, WL), and $ECC(k_0, n_0, t_0)$.

Output: Recovered grayscale secret image S', with the size of $W \times H$.

Step 1: Pick up pixel values in all of the shadow images following the order in Figure. 3 to construct the pixel blocks, and each block has WL pixels. The total number of pixel groups of each share is $\frac{W \cdot H \cdot MAX_b}{WL \cdot HL}$.

Step 2: Check and correct the correctness of pixels bits in all shadow images from the first pixel block.

Step 3: In the i-th block, we can get the bit messages $LSC_{i,t}$, and in the $(i+1)$-th block, we can get $HSC_{i+1,t}$. Then, the whole codeword is $(LSC_{i,t}, HSC_{i+1,t}), t = 1, 2, \ldots, n$. Corrected information bits $LSC_{i,t}{}'$ can be obtained by ECC decoding. If $LSC_{i,t}$ is not equal to $LSC_{i,t}{}'$, replace it with the corrected ones.

Step 4: Set the pixels in the blocks to the original positions.

Step 5: If all the blocks are checked, goto Step 6; otherwise, $i = i+1$ and goto Step 3.

Step 6: Repeat Step 7 until all pixels of shadow images are processed.

Step 7: Calculate $f(x) = \sum_{i=1}^{k} f(x_i) \prod_{\substack{l=1 \\ l \neq i}}^{k} \frac{(x - x_l)}{(x_i - x_l)}$ according to the pixels in the same position of shadow images and the serial numbers x_i. The secret pixel is actually $f(0)$.

Step 8: Output the recovered grayscale secret image S' with the size of $W \times H$.

Theorem 1 (Necessary Condition for Generating RPSIS): As for the proposed RPSIS scheme, a necessary condition for generating grayscale shadow images is $\log_2 p \geq \frac{4n}{k-1}$, where p is the prime number, and (k, n) is the threshold during share generation.

Proof: The proposed RPSIS scheme is based on Shamir's traditional polynomial-based secret sharing, which adds an extra filtering operation to find the satisfied share values. It is proven that polynomial-based secret sharing is a perfect secret sharing scheme with unconditional security. During the sharing process of each pixel with (k, n)-threshold RPSIS, the secret value s has p^{k-1} combinations of candidate shared values, while the total possible number of n shared values is 2^{4n} when the half high bits are

considered as the constraints. Therefore, in the pixel block with WL pixels, a necessary condition for generating shares is $\left(p^{k-1}\right)^{WL} \geq \left(2^{4n}\right)^{WL}$.

Theorem 2 (Error-Correction Capability): In order to recover the secret image without loss, the changed bits in the pixels of noisy grayscale shadow images are at most $\frac{MAX_b \cdot H \cdot W \cdot t_0}{HL \cdot WL}$.

Proof: If the noise in the shadow images is evenly distributed, the maximum error correction proportion is $\frac{t_0}{HL \cdot WL}$. One shadow image has $MAX_b \cdot H \cdot W$ bits in total.

Theorem 3: The proposed (k, n)-threshold RPSIS is a secure and ideal secret image sharing scheme.

Proof: The scheme is qualified based on Lemma 1 - Lemma 3.

Lemma 1 (Shadow Image Security): The proposed RPSIS scheme is an ideal secret image sharing scheme, and the generated shadow images have no information leakage.

Proof: At the beginning of pixel block sharing, there is no constraint, so that the share value can be viewed as a random number. In the subsequent pixel blocks, the limited constraints are relevant to ECCs. The ECCs can be regarded as random elements to some degree, which are uniformly distributed in the value space. Furthermore, it is necessary for ECCs to ensure a large distance between different data bits. Therefore, no one can infer any information from the shadow images.

Lemma 2 (Security Condition): When any $k-1$ or fewer shadow images are accessed, no one can reconstruct the secret image S in a limited time.

Proof: The sharing and recovery processes of the proposed RPSIS scheme are strictly based on the polynomial secret image sharing. According to the principle of the PSIS scheme, the secret value is achieved by calculating a $k-1$ degree polynomial expression, which has k unknown values. The solution of the secret value obtained from the polynomial is not unique with less than k pairs like $(x, f(x))$.

Lemma 3 (Secret Recovery Condition): When k or more than k shadow images without noise are acquired, the secret image S can be recovered without loss.

Proof: The shadow images are added with no noise, which means that the values in shares have been stored completely and can lead to an absolute solution. When we collect $x_{i_1}, x_{i_2}, \ldots, x_{i_t} (t \geq k)$, we can obtain t equations with k unknowns $a_0, a_1, \ldots, a_{k-1}$. Therefore, the solution of secret value a_0 can be obtained by a polynomial.

V. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we will display the effects of RPSIS according to the following aspects. Shadow images and recovered results are showed first, and then the metrics are introduced; the experimental results will be illustrated next to indicate the effectiveness of our scheme, and then some parameters that may lead to different effects of the scheme will be discussed.

A. IMAGE ILLUSTRATION

In the following test, we use the original grayscale image 'Lena' as a secret image with a size of 256×256. In the RPSIS scheme, $HL = 4$, $WL = 8$, $BCH(32, 16, 3)$ are adopted as an example. The shadow images of (3, 3)-threshold RPSIS and (4, 5)-threshold RPSIS without noise and their corresponding histograms will be showed in Figure. 4 and Figure. 5. The generated shadow images all have a size of 256×256. The public numbers are (11, 13, 17) and (11, 13, 17, 19, 23) separately, and the prime number during the sharing process is 257.

In Figure. 4, (a) represents the secret image, (b-d) show shadow images successively, (e) is the recovery result with the first two shadow images, (f) is the recovery result with all three shadow images, and (g-j) are histograms of (a-d).

In Figure. 5, (a) shows the secret image, (b-f) are shadow images, (g) illustrates the recovery result with first three shadow images, (h) is the recovery result with four ones,and (i-m) represent histograms of shadow images in (b-f).

We can infer from Figure. 4 and Figure. 5 that RPSIS is secure. The secret image can be recovered without loss and without damage when k shadow images are accessed. Additionally, there is no information leakage in shadow images, and no information can be obtained when there are less than k shadow images.

However, some people may wonder: can secret image sharing without robustness still observe part of the image information, and what is the significance of the RPSIS?

An example in Figure.6 can explain the significance. The content of a recovered image with secret image sharing without robustness cannot be completely distinguished. In other words, our scheme can be applied when the visual quality of the recovered image is high and the communication condition is poor.

The robustness of RPSIS will be discussed in detail in Section V-C.

B. METRICS

Robust secret image sharing should be evaluated according to the recovery images, and the visual quality of images can be measured by $PSNR$ and $SSIM$.

Peak-signal-to-noise-ratio ($PSNR$) between the two images S and S', as shown in Eq. 10, is usually utilized to measure the similarity. The value of $PSNR$ ranges from 0 to $+\infty$, and the higher the value is, the more similar the two images are. $PSNR = 0$ means that there is no similarity between S and S', while $PSNR = +\infty$ signifies that S and S' are the same images without any difference.

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

where

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

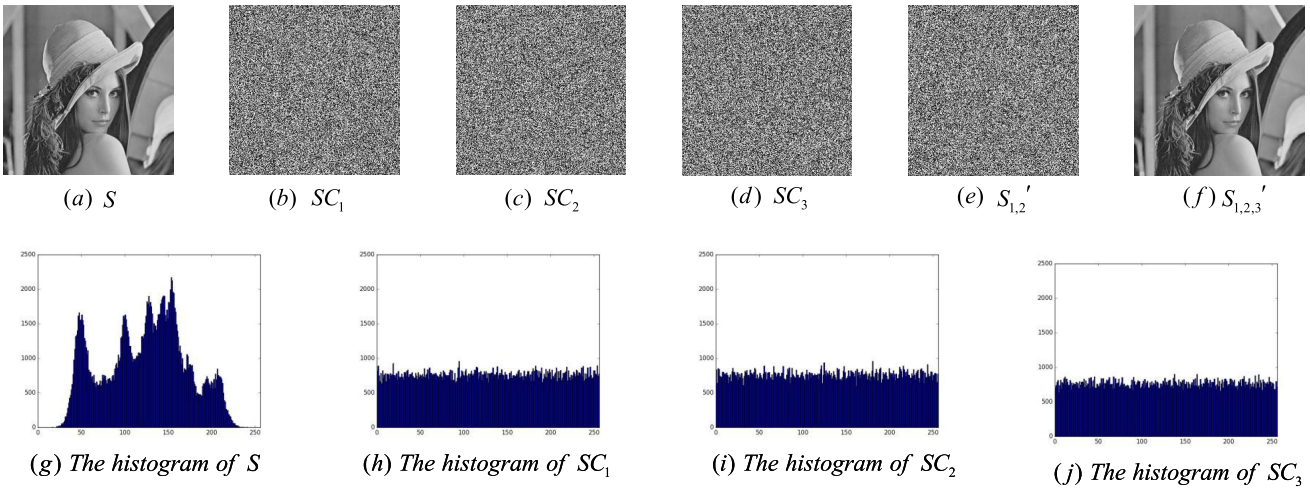


FIGURE 4. The shadow images, histograms and recovery result of (3, 3)-threshold RPSIS. (a) The initial grayscale secret image; (b)-(d) the generated three shadow images without any noise; (e) the recovery results with SC_1 and SC_2; (f) the recovery results with SC_1, SC_2 and SC_3; (g)-(j) the histograms of (a)-(d).

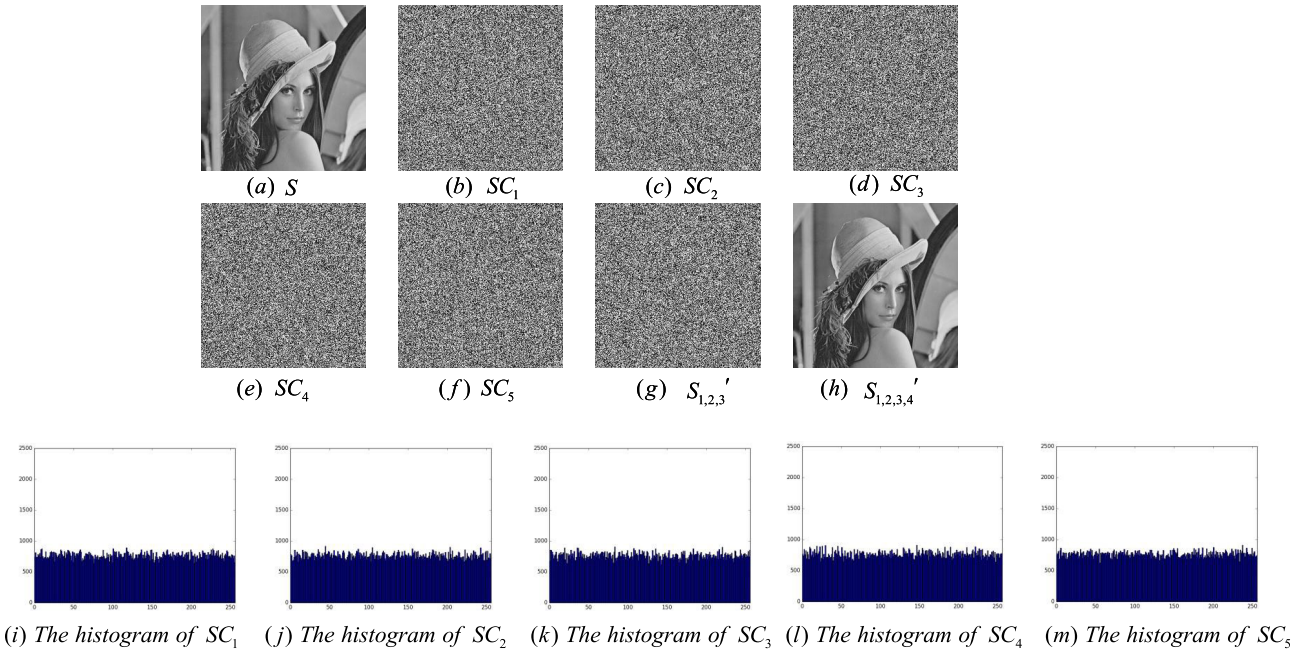


FIGURE 5. The shadow images, histograms and recovery result of (4, 5)-threshold RPSIS without noise. (a)The initial grayscale secret image; (b)-(f)the generated five shadow images without any noise; (g)the recovery results with SC_1, SC_2 and SC_3; (h)the recovery result with SC_1, SC_2, SC_3 and SC_4; (i)-(m)the histograms of (b)-(f).

the size of S and S' is $W \times H$, and MAX_S denotes the maximum value of image pixel value space. In following sections, $+\infty$ cannot be expressed in figures, and we use $PSNR = 100$ to represent lossless recovered image.

Structural similarity index ($SSIM$) is also used to measure the similarity between two images, and it is based on three comparative measures: luminance, contrast and structure. SSIM value as shown in Eq. 12 is in -1 and 1. The higher the SSIM value is, the more similar the two images are.

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

where

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

μ_x, μ_y separately represents the local means of images x, y, σ_x, σ_y denote the standard deviations, and σ_{xy} is the cross-covariance.

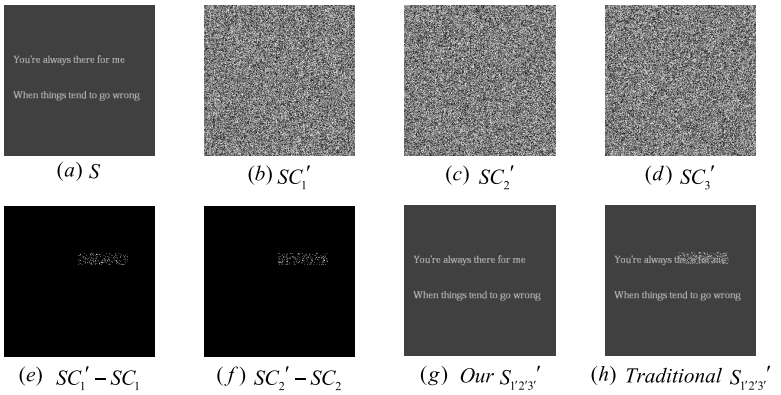


FIGURE 6. An example of the significance of robust secret image sharing. (a) The initial grayscale secret image; (b)-(d) the shadow images added with noise; (e) difference between initial shadow image SC_1 and noisy shadow image SC_1'; (f) difference between initial shadow image SC_2 and noisy shadow image SC_2'; (g) the recovery results with RPSIS from noisy shadow image SC_1', SC_2' and SC_3'; (h) the recovery results with secret image sharing without robustness from noisy shadow image SC_1', SC_2' and SC_3'.

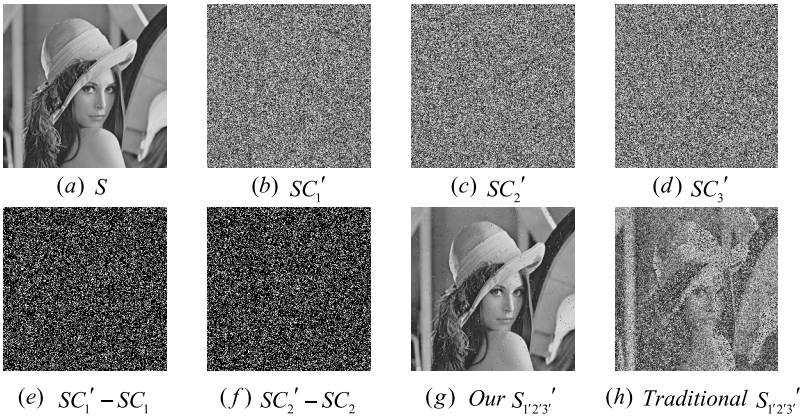


FIGURE 7. Experimental results of the proposed (3, 3)-threshold RPSIS with LSB flipping noise added to all shadow images. (a) The secret image; (b)-(d) noisy shadow images obtained by adding LSB flipping with density $d = 0.25$; (e) the difference between original shadow images Figure.4(b) and noisy shadow images (b); (f) the difference between original shadow images Figure.4(c) and noisy shadow images (c); (g) the recovered image with our proposed scheme, $PSNR = 29.6216$, $SSIM = 0.8909$; (h) the recovered image with the traditional scheme without robustness, $PSNR = 11.9313$, $SSIM = 0.0937$.

C. ROBUSTNESS TO NOISE AND IMAGE QUALITY

1) LEAST SIGNIFICANT BIT FLIPPING NOISE

Least significant bit (LSB) flipping noise refers to the lowest bit in pixel value that is flipped. Even though the change is slight, it can also affect the recovery of the secret image.

Figure. 7 represents the experimental results of our proposed (3, 3)-threshold RPSIS scheme. Figure. 7(a) is the secret image. Figure. 7(b)-(d) display the noisy shadow images where LSB flipping noise with density $d = 0.25$ is added to SC_1, SC_2 and SC_3 in Figure.4 respectively. Figure. 7(e)-(f) illustrate the differences between original shadow images and noisy ones, where the white points represent the changed position. Figure. 7(g) demonstrates the recovered secret image with the three noisy shadow images by using our proposed scheme, and Figure. 7(f) is the recovered secret image with the same shadow images by using the traditional scheme without robustness.

In Figure. 8, the experimental results are shown with density $d = 0.25$ of LSB flipping noise for the (4, 5)-threshold RPSIS. Figure. 8(a-e) are noisy shadow images, the black points in Figure. 8(f) represent the positions with added LSB flipping noise, Figure. 8(g,h) exhibit the reconstructed images with SC_1', SC_2', SC_3' and SC_4' with our proposed method and the traditional method, Figure. 8(i)-(j) are the recovery images from all five noisy shadow images.

From the above experiments, our scheme can resist the LSB flipping noise added to shadow images, and the recovered secret image is more similar to that of the traditional scheme without robustness.

In Figure. 9, different densities of LSB flipping noise are added to the shadow images to observe the quality of the recovered images with our scheme and the traditional scheme without robustness. From the experimental results above, our proposed RPSIS performs well in resisting LSB flipping

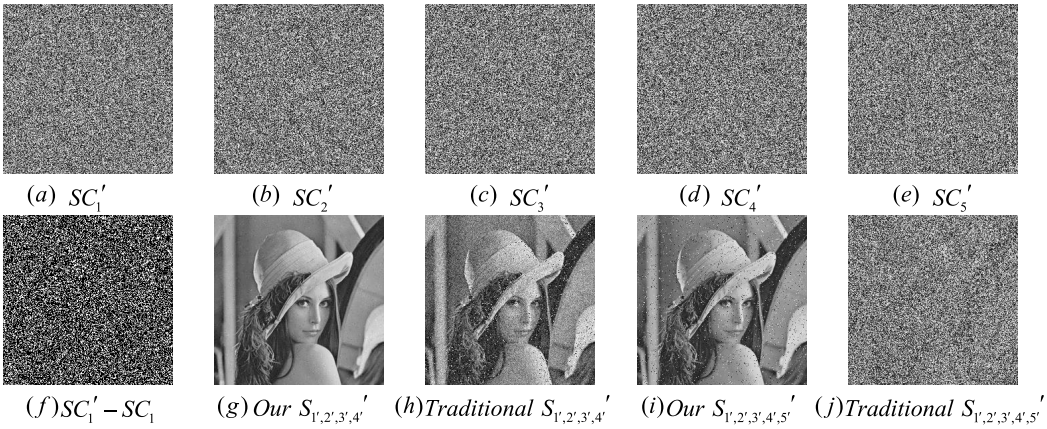
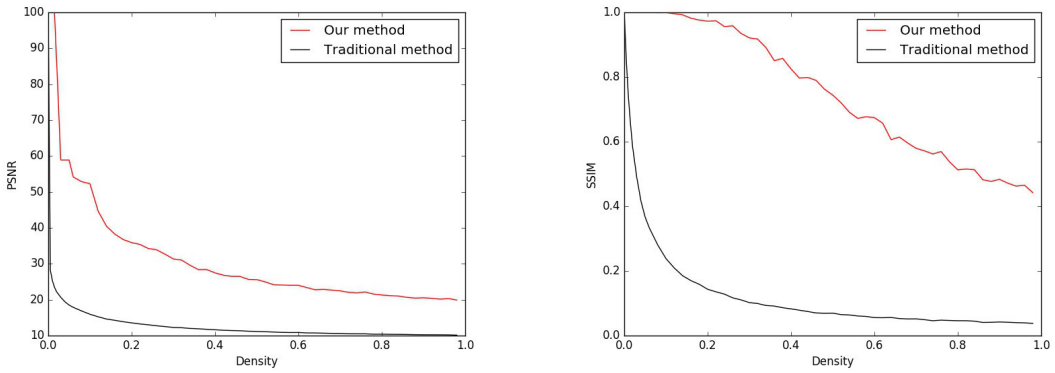


FIGURE 8. Experimental results of the proposed (4, 5)-threshold RPSIS with LSB flipping noise added to all shadow images. (a)-(e) Noisy shadow images obtained by adding LSB flipping noise with density $d = 0.25$; (f) the difference between original shadow images SC_1 and noisy shadow images (a); (g) the recovered image from (a)-(d) with our proposed scheme, $PSNR = 43.7673$, $SSIM = 0.9851$; (h) the recovered image from (a)-(d) with traditional scheme, $PSNR = 10.8632$, $SSIM = 0.0566$; (i) the recovered image from (a)-(e) with our proposed scheme, $PSNR = 31.1667$, $SSIM = 0.9116$; (j) the recovered image from (a)-(e) with traditional scheme, $PSNR = 10.8632$, $SSIM = 0.0566$.



(a) PSNR (b) SSIM

FIGURE 9. Comparison of image visual quality recovered by our scheme RPSIS and traditional scheme without robustness from the shadow images added with different densities of LSB flipping noise. 9(a)PSNR; 9(b)SSIM.

errors, and the visual quality of the recovered image has been greatly improved.

2) GAUSSIAN NOISE

Gaussian noise refers to a class of noise whose probability density function follows a Gaussian distribution (normal distribution). In Figure. 10, the experimental results recovered from shadow images added with Gaussian noise are exhibited. Figure. 10 (a)-(c) are the shadow images added with Gaussian noise, Figure. 10 (d) shows the changed pixel positions of SC_1, where white dots represent the changed pixels, and Figure. 10 (e)-(f) display the recovery results with our scheme and traditional scheme without robustness, respectively.

As for shadow images added with Gaussian noise, the bit error rate is made use of to evaluate the noise level. Bit error rate is the ratio of the number of changed bits in shadow images to the total number of bits. Fig 11 expresses the visual quality with different levels of Gaussian noise.

3) JPEG COMPRESSION

Figure. 12 presents the experimental results of the (3, 3)-threshold RPSIS with JPEG compression noise. Figure. 12(a-c) illustrates the noisy shadow images for which the JPEG-compressed shadow images possess a quality of 100, Figure. 12(d) displays the recovery results using our scheme, and Figure. 12(e) is the reconstructed image with the traditional method.

Figure. 13 presents the experimental results of the (4, 5)-threshold RPSIS with JPEG compression noise. Figure. 13(a-e) illustrates the noisy shadow images for which the JPEG-compressed file equals 100 to SC_i, for $i = 1, 2, 3,$

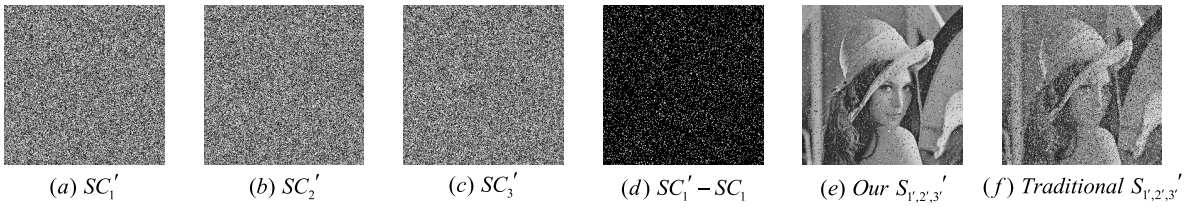
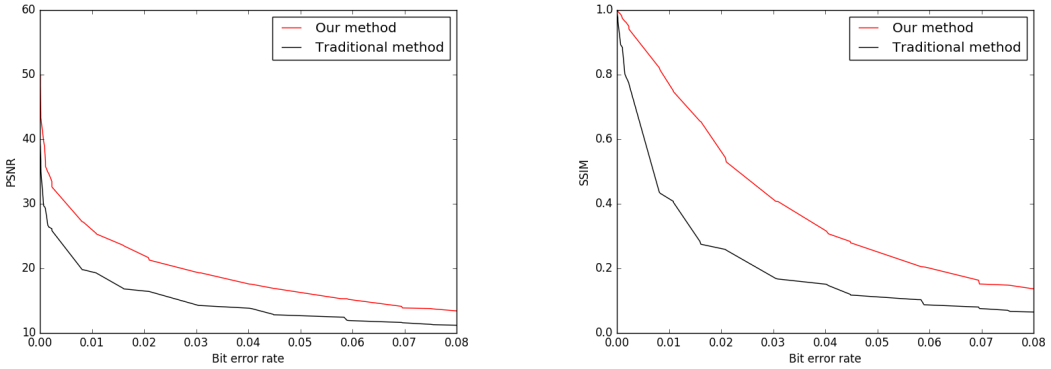


FIGURE 10. Experimental results of the proposed (3, 3)-threshold with Gaussian noise added to all shadow images. (a)-(c) The noisy shadow images added with Gaussian noise; (d) different pixels between noisy shadow image SC_1' and initial shadow image SC_1; (e) recovery result by using our scheme, $PSNR = 19.5585$, $SSIM = 0.4324$; (f) recovery result with traditional method, $PSNR = 13.7882$, $SSIM = 0.1496$.



(a) PSNR (b) SSIM

FIGURE 11. Comparison between our scheme and the traditional scheme with Gaussian noise. 11(a)PSNR; 11(b)SSIM.

and Figure. 13(f) displays the recovery results by using our scheme with four shadow images. Figure. 13(i) represents the image by using our scheme with all five shadow images, and Figure. 13(h,j) shows the reconstructed images with the traditional method.

In Fig 14, the comparison between our scheme and a traditional scheme with JPEG compression is exhibited.

4) SUMMARY

Through the experiments, several points can be reflected as follows:

1) RPSIS is secure because it meets the basic condition of (k, n)-threshold secret image sharing and no shadow images will leak texture, pattern or other information about the secret image.
2) RPSIS is proven to be robust. It performs well in resisting LSB flipping noise and Gaussian noise. It can also mitigate the impact on the recovery of JPEG-compressed shadow images to a certain extent.
3) As for the (k, n)-threshold scheme, the quality of the recovered image from k shadow images is better than that from k ones.

D. DISCUSSION

1) SECURITY

From Figure. 4 and Figure. 5, the pixel distribution of shadow images is random and uniform, and it can be inferred that the proposed RPSIS scheme is secure. However, as a common test image, "Lena" contains various details, smooth areas, shadows and textures, and it cannot fully reflect the security of secret image sharing methods. In Figure. 15, a special image is adopted to observe the security of shadow images of RPSIS. It shows that even when processing an extreme image, the pixel values in shadow images are also uniformly and randomly distributed, and less than k shadow images cannot reveal the secret image.

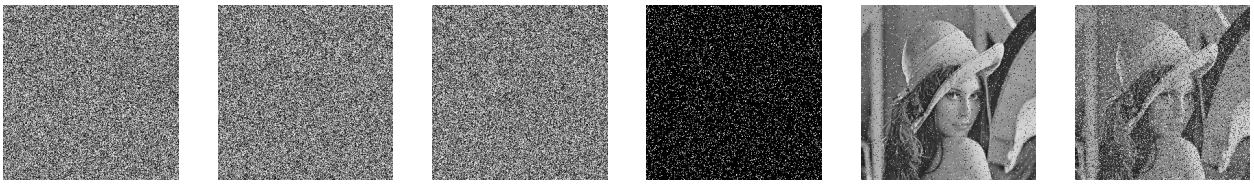
2) PARAMETERS

During the share generating process, different parameters can lead to different results.

Serials: Through our experiments, it is found that not all combinations of serials can generate the qualified shadow images. In fact, this is another scientific problem that needs to be solved. According to experiments, two different ways of selecting serial numbers can be taken into consideration: one is a continuous set of prime numbers, like $(11, 13, 17, 19, \ldots)$, and the other is a set of prime numbers with relatively large differences, like $(11, 29, 67, 101, \ldots)$. Figure. 16 shows the recovery effects under different noise densities, where $(11, 29, 67)$ and $(11, 13, 17)$ are adopted when generating shadow images.

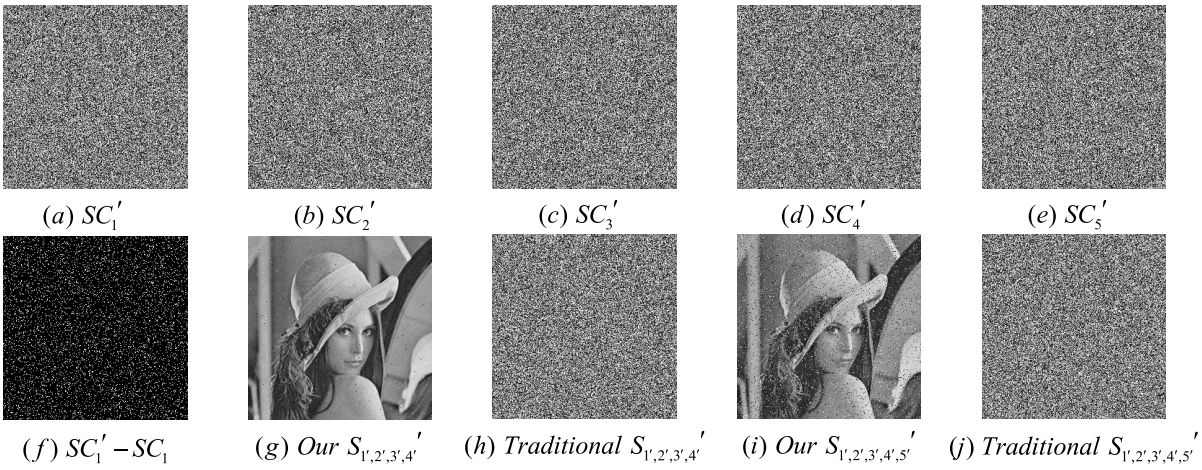
From the experimental results shown in Figure. 16, it can be inferred that the continuous set of prime numbers may lead to a better recovery effect.

ECC: In Algorithm 1 Step 1, the choice of WL and HL affects the decision of ECCs, which leads to various



(a) SC_1' (b) SC_2' (c) SC_3' (d) $SC_1 - SC_1'$ (e) Our $S_{1',2',3'}'$ (f) Traditional $S_{1',2',3'}'$

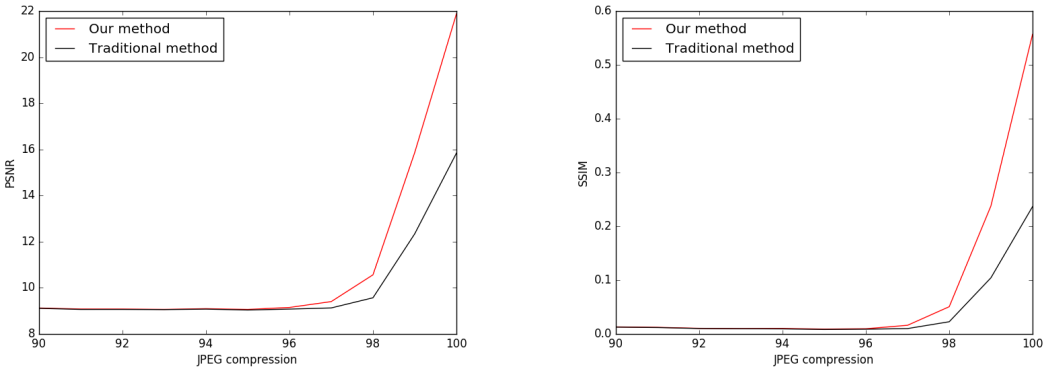
FIGURE 12. Experimental results of the proposed (3, 3)-threshold with JPEG compression noise added to all shadow images. (a)-(c) The JPEG-compressed shadow images with a quality of 100; (d) different pixels between noisy shadow image SC_1' and initial shadow image SC_1; (e) recovery results using our scheme, $PSNR = 21.8809$, $SSIM = 0.5568$; (f) recovery results with the traditional method, $PSNR = 15.8418$, $SSIM = 0.2366$.



(a) SC_1' (b) SC_2' (c) SC_3' (d) SC_4' (e) SC_5'

(f) $SC_1' - SC_1$ (g) Our $S_{1',2',3',4'}'$ (h) Traditional $S_{1',2',3',4'}'$ (i) Our $S_{1',2',3',4',5'}'$ (j) Traditional $S_{1',2',3',4',5'}'$

FIGURE 13. Experimental results of the proposed (4, 5)-threshold with JPEG compression noise added to all shadow images. (a)-(e) The JPEG-compressed shadow images with quality of 100; (f) different pixels between noisy shadow image SC_1' and initial shadow image SC_1; (g) recovery result from (a)-(d) with our proposed RPSIS scheme, $PSNR = 29.6084$, $SSIM = 0.8076$; (h) recovery result from (a)-(d) with the traditional method, $PSNR = 9.0703$, $SSIM = 0.0089$; (i) recovery result from (a)-(e) with our proposed RPSIS scheme, $PSNR = 19.3007$, $SSIM = 0.3974$; (j) recovery result from (a)-(e) with the traditional method, $PSNR = 9.0775$, $SSIM = 0.0100$.



(a) PSNR (b) SSIM

FIGURE 14. Comparison between our scheme and a traditional scheme with JPEG compression. 16(a)PSNR; 16(b)SSIM.

error-correction abilities, and the applicable conditions cannot be generalized simply.

In our algorithm, the high half bits planes are used to check the low ones of the last block, and the selection of $ECC(k_0, n_0, t_0)$ can better meet the following condition: $k_0 = 2n_0$. If $k_0 > 2n_0$, the encoded data bits are shorter; if $k_0 < 2n_0$, the error correction ability will be reduced. Based on the above considerations, we have two proper ECC options for grayscale images: $ECC(32, 16, 3)$ and $ECC(8, 4, 1)$.

For bit error noise, on the one hand, $ECC(8, 4, 1)$ can correct all LSB flipping errors even if the density of noise is 100%; however, $ECC(32, 16, 3)$ cannot achieve this effect. On the other hand, $ECC(8, 4, 1)$ is powerless against multi-bit pixel errors, while $ECC(32, 16, 3)$ performs better to some degree.

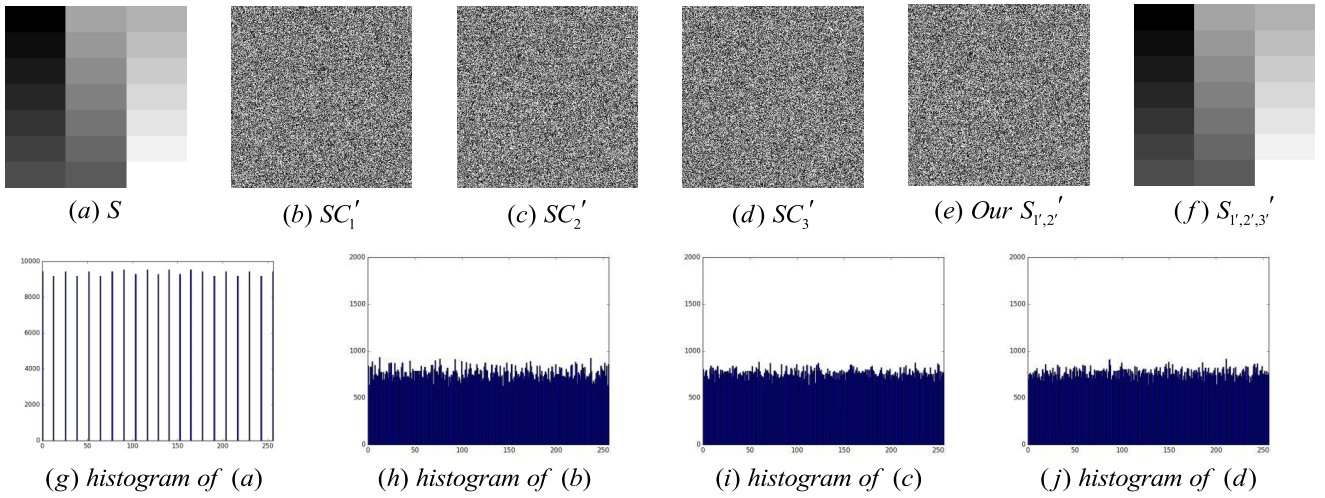
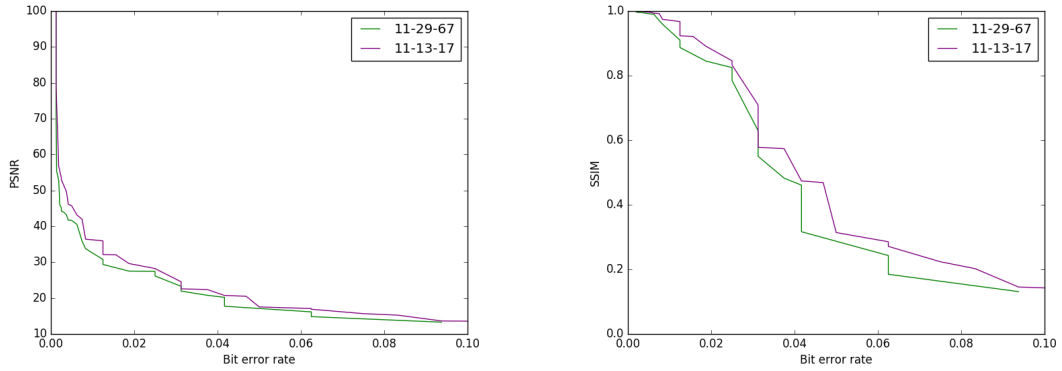


FIGURE 15. The shadow images, histograms and recovery results of special image without noise. (a)Extreme secret image; (b)-(d)shadow images; (e)recovery results from (b)-(c); (f)recovery results from (b)-(d); (g)-(h)histograms of (a)-(d).



(a) PSNR (b) SSIM

FIGURE 16. Comparison between different serials, a continuous set of prime numbers, and a set of prime numbers with relatively large differences. 16(a)PSNR; 16(b)SSIM.

Figure. 17 displays the different effects with $ECC(32, 16, 3)$ and $ECC(8, 4, 1)$ for JPEG compression. From the results, it can be found that $ECC(8, 4, 1)$ performs gently, and $ECC(32, 16, 3)$ performs better when the JPEG-compression parameter is quite high.

According to the experimental results, if the amount of noise is large but the effect on each pixel value is not obvious, $ECC(8, 4, 1)$ can be adopted. If it is the other way around, it is better to select $ECC(32, 16, 3)$.

TABLE 1. The characteristics of our scheme and other related works.

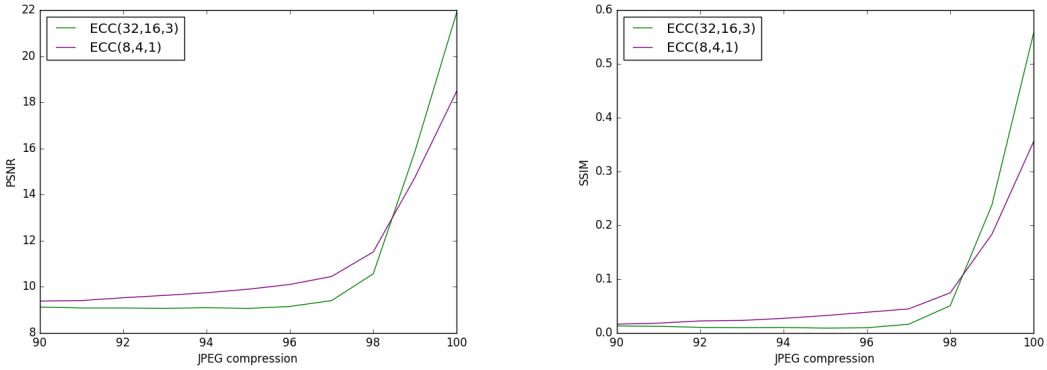
Scheme	Sharing Target	Robustness	Lossless Recovery	Pixel Expansion
Our scheme	Grayscale or color image	Yes	Yes	No
[19]	Grayscale or color image	Yes	Yes	Yes
[20]	Color image	Yes	Yes	Yes
[21]	Data	Yes	Yes	Yes
[22]	Data	Yes	Yes	Yes
[23]	Data	Yes	Yes	Yes
[25]	Grayscale image	Yes	No	No
[32]	Grayscale or color image	No	Yes	No

E. COMPARISON WITH OTHER WORKS

In this section, we will compare our recovery quality with that of other works. First, our scheme will be compared with related work from robustness, lossless recovery and pixel expansion. These three aspects cannot be always realized at the same time. Table. 1 displays the results. In Table. 1, lossless recovery means that the secret information can be recovered completely and without loss and noise, and pixel expansion is compared with the secret information.

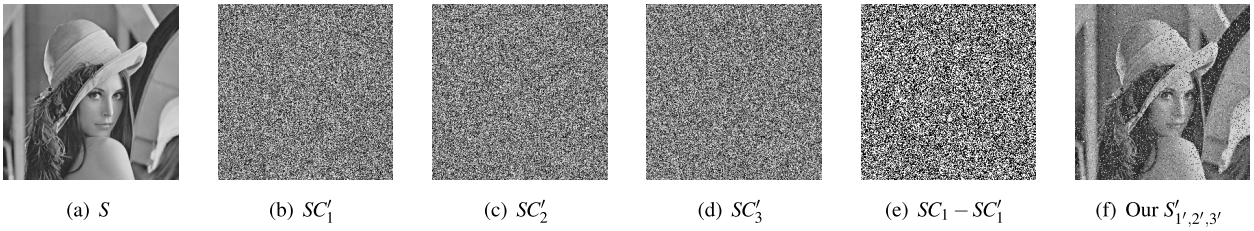
From Table. 1, it can be inferred that our scheme takes the characteristics of these three aspects into account.

To evaluate the ability of robustness of our scheme, our scheme is compared with the related works in the case of adding noise to the shadow images.



(a) PSNR (b) SSIM

FIGURE 17. Comparison of different ECCs for JPEG compression on shadow images. 17(a)PSNR; 17(b)SSIM.



(a) S (b) SC'_1 (c) SC'_2 (d) SC'_3 (e) $SC_1 - SC'_1$ (f) Our $S'_{1',2',3'}$

(g) S (h) SC'_1 (i) SC'_2 (j) SC'_3 (k) $SC_1 - SC'_1$ (l) Gong's $S'_{1',2',3'}$

FIGURE 18. Comparison between our scheme and Gong's scheme with LSB flipping noise. Figure. 18(a) and Figure. 18(g) are the secret image; Figure. 18(b) - Figure. 18(d) are the shadow images of our scheme added with LSB flipping noise, density $d = 0.5$; Figure. 18(h) - Figure. 18(j) are the shadow images of Gong's method added with LSB flipping noise, density $d = 0.5$; Figure. 18(e) and Figure. 18(k) show the differences between noisy shadow images and original images, respectively; Figure. 18(f) is the recovered secret image of our method, $PSNR = 15.5094$, $SSIM = 0.2165$, and Figure. 18(l) is the recovered secret image of Gong's method, $PSNR = 9.0233$, $SSIM = 0.0114$.

(a) BER=10^{-2} (b) BER=10^{-3} (c) BER=10^{-4} (d) BER=10^{-5}

FIGURE 19. The recovered images of Wang's method when shadow images are added with different levels of Gaussian noise. 19(a)BER = 10^{-2}, PSNR=13.12; 19(b)BER = 10^{-3}, PSNR=22.67; 19(c)BER = 10^{-4},PSNR=30.96;19(d)BER = 10^{-5},PSNR=32.62.

1) COMPARISON WITH GONG's WORK

In Gong's work [32], the polynomial-based secret image sharing is generated in the field of $GF(2^8)$, which perfectly corresponds one-to-one to 256 pixel values so that the scheme can realize perfect lossless recovery. In Figure. 18, the comparison of our scheme RPSIS and Gong's method is shown. Figure. 18(a) - Figure. 18(f) are the sharing and recovered images generated with our method RPSIS, Figure. 18(g) - Figure. 18(l) are the sharing and recovered images generated with Gong's method. From Figure. 18, when the shadow images are added with the same LSB flipping noise, our scheme can resist the noise, and the recovered

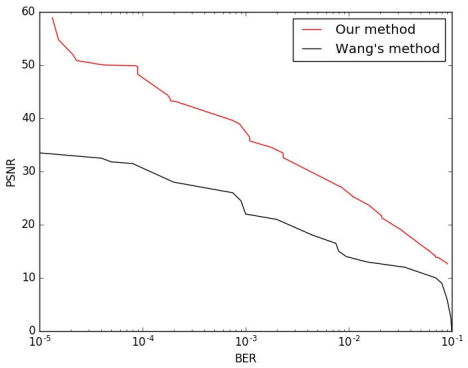


FIGURE 20. **The comparison with Wang's method to determine the visual quality of a recovered image with shadow images added with Gaussian noise.**

image can be distinguished, but the content of the recovered image with Gong's method cannot be recognized.

2) COMPARISON WITH WANG's WORK

In Wang's work [25], the proposed scheme called CS-PSIS can resist bit errors to some extent. Compressed sensing (CS) is a technology of signal sampling, which is the process of data compression during the sampling process. CS-PSIS utilizes CS and a novel scalar quantization to extract important information and discard unimportant information in the original secret image, and after these steps, information is compressed. Then, the quantized measurements are divided into n shadows, and identification numbers are also contained in the shadows through an extended DH protocol. In other words, CS-PSIS focuses on compressing significant information, and robustness is an additional function. On the contrary, our RPSIS mainly focuses on robustness to resist errors in shadow images.

Figure. 19 shows the recovered images of Wang's method when shadow images are added with different levels of Gaussian noise.

Figure. 20 illustrates the recovery effects of the two schemes. Gaussian noise is added to shadow images, and bit-error-rate (BER) is utilized to measure noise level. When shadow images are added the same level of BER, the recovery quality of our method is higher, and the range of correcting error is wider than Wang's. Furthermore, [25] shows the results of shadow images added with Gaussian noise and does not refer to other kinds of noise.

VI. CONCLUSION

In this paper, we propose a novel robust secret image sharing based on polynomial (RPSIS). It utilizes random elements during the share generating process to generate a checksum of part of the other shares to resist the potential errors in storage, transmission or even those caused by malicious destruction. Different from other existing schemes, RPSIS can not only be robust to several typical kinds of noise but also keep shadow images the same size as the initial secret image. RPSIS is theoretically and experimentally proven to be secure and robust to LSB noise, Gaussian noise, JPEG-compression noise, *etc*. We also discuss the parameters that may affect recovery quality, such as serial numbers and ECCs, and give proper selections. Last but not least, there are still some improvements to be made on our work. First, the capability of error correction can be further improved; second, the present scheme is more aimed at bit-error noise, and a new scheme for addictive noise can be designed; third, the optical serial numbers are continuous prime numbers, and the exact theoretical foundation is worth researching.

ACKNOWLEDGMENT

The authors would like to thank the Editor and anonymous reviewers for their valuable comments.

REFERENCES

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS*, 1979, p. 313.
[3] P. Li, C.-N. Yang, and Z. Zhou, "Essential secret image sharing scheme with the same size of shadows," *Digit. Signal Process.*, vol. 50, pp. 51–60, Mar. 2016.
[4] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1994, pp. 1–12.
[5] P.-Y. Lin, R.-Z. Wang, Y.-J. Chang, and W.-P. Fang, "Prevention of cheating in visual cryptography by using coherent patterns," *Inf. Sci.*, vol. 301, pp. 61–74, Apr. 2015.
[6] C.-N. Yang, C.-H. Chen, and S.-R. Cai, "Enhanced Boolean-based multi secret image sharing scheme," *J. Syst. Softw.*, vol. 116, pp. 22–34, Jun. 2016.
[7] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognit.*, vol. 43, no. 1, pp. 397–404, Jan. 2010.
[8] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," *Inf. Sci.*, vol. 180, no. 15, pp. 2889–2894, Aug. 2010.
[9] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Secret image sharing for (k, k) threshold based on Chinese remainder theorem and image characteristics," in *Image and Video Technology*, M. Paul, C. Hitoshi, and Q. Huang, Eds. Cham, Switzerland: Springer, 2018, pp. 174–181.
[10] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Inf. Sci.*, vol. 473, pp. 13–30, Jan. 2019.
[11] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3848–3858, 2020.
[12] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Trans. Multimedia*, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.
[13] Z. Chen, X. Hou, X. Qian, and C. Gong, "Efficient and robust image coding and transmission based on scrambled block compressive sensing," *IEEE Trans. Multimedia*, vol. 20, no. 7, pp. 1610–1621, Jul. 2018.
[14] X. Yan, Y. Lu, and L. Liu, "General meaningful shadow construction in secret image sharing," *IEEE Access*, vol. 6, pp. 45246–45255, 2018.
[15] A. Gutub, N. Al-Juaid, and E. Khan, "Counting-based secret sharing technique for multimedia applications," *Multimedia Tools Appl.*, vol. 78, no. 5, pp. 5591–5619, Mar. 2019.
[16] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority," in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC)*, 1989, pp. 73–85.
[17] C. Blundo and A. De Santis, "Lower bounds for robust secret sharing schemes," *Inf. Process. Lett.*, vol. 63, no. 6, pp. 317–321, Sep. 1997.
[18] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Inf. Sci.*, vol. 453, pp. 21–29, Jul. 2018.

[19] A. Espejel-Trujillo, M. Nakano-Miyatake, J. Olivares-Mercado, and H. Perez-Meana, "A cheating-prevention mechanism for hierarchical secret-image-sharing using robust watermarking," *Multimedia Tools Appl.*, vol. 75, no. 13, pp. 7855–7873, Jul. 2016.
[20] M. Ghebleh and A. Kanso, "A novel secret image sharing scheme using large primes," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11903–11923, May 2018.
[21] R. Cramer, I. B. Damgård, N. Döttling, S. Fehr, and G. Spini, "Linear secret sharing schemes from error correcting codes and universal hash functions," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 313–336.
[22] M. Cheraghchi, "Nearly optimal robust secret sharing," *Des., Codes Cryptogr.*, vol. 87, no. 8, pp. 1777–1796, Aug. 2019.
[23] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-Solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, Sep. 1981.
[24] V. Rishiwal, M. Yadav, and K. V. Arya, "A robust secret image sharing scheme," in *Proc. 1st Int. Conf. Emerg. Trends Eng. Technol.*, Jul. 2008, pp. 11–14.
[25] P. Wang, X. He, Y. Zhang, W. Wen, and M. Li, "A robust and secure image sharing scheme with personal identity information embedded," *Comput. Secur.*, vol. 85, pp. 107–121, Aug. 2019.
[26] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.
[27] C.-N. Yang, K.-H. Yu, and R. Lukac, "User-friendly image sharing in multimedia database using polynomials with different primes," in *Proc. Int. Conf. Multimedia Modeling*. Berlin, Germany: Springer, 2007, pp. 443–452.
[28] L. Liu, Y. Lu, and X. Yan, "Polynomial-based extended secret image sharing scheme with reversible and unexpanded covers," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1265–1287, Jan. 2019.
[29] Q. Gong, Y. Wang, X. Yan, and L. Liu, "Efficient and lossless polynomial-based secret image sharing for color images," *IEEE Access*, vol. 7, pp. 113216–113222, 2019.
[30] P. Li, C.-N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 41–50, Jan. 2018.
[31] S. Lin and D. J. Costello, *Error Control Coding*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.
[32] Q. Gong, X. Yan, Y. Wang, and L. Liu, "Polynomial-based secret image sharing in the galois field of $gf(2^8)$," in *Proc. China Inf. Hiding Workshop*, Sep. 2019, pp. 681–688.

YUYUAN SUN was born in China, in 1996. She received the B.Sc. degree (Hons.) in computer application and the M.Sc. degree in cyberspace security from the National University of Defense Technology, Hefei, China, in 2018 and 2020, respectively. She is currently pursuing the Ph.D. degree with the National University of Defense Technology. Her research interests include multimedia security and computer application.

YULIANG LU was born in China, in 1964. He received the B.Sc. (Hons.) and M.Sc. degrees in computer application from Southeast University, China, in 1985 and 1988, respectively. He is currently a Professor with the National University of Defense Technology, Hefei, China. His research interests include computer application and information processing.

XUEHU YAN was born in China, in February 1984. He received the B.Sc. degree (Hons.) in information and calculate science, the M.Sc. degree in computational mathematics, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, China, in 2006, 2008, and 2015, respectively. He is currently an Associate Professor with the National University of Defense Technology, Hefei, China. His research interests include visual cryptography, secret image sharing, information hiding, cryptography, and multimedia security. He has published more than 100 articles in these areas. He was a co-recipient of an International Workshop of Digital Crime and Forensics (IWDCF) 2016 Best Paper Award for the paper Exploiting the Homomorphic Property of Visual Cryptography. Since 2017, he has been an Associate Editor of the *International Journal of Digital Crime and Forensics*.

LINTAO LIU was born in China, in December 1989. He received the B.Sc. degree (Hons.) in computer application, the M.Sc. and Ph.D. degrees in information security from the National University of Defense Technology, Hefei, China, in 2012, 2015, and 2019, respectively. He is currently an Associate Professor with the National University of Defense Technology. His research interests include cryptography, multimedia security, and biometrics.

LONGLONG LI was born in China, in January 1995. He received the B.Sc. degree (Hons.) in automation from the University of Science and Technology of China, China, in 2017, and the M.Sc. degree in cyberspace security from the National University of Defense Technology, Hefei, China, in 2019, where he is currently pursuing the Ph.D. degree. His research interests include secret image sharing and steganalysis.