Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/mbe

MBE, 19(11): 11544–11562.
DOI: 10.3934/mbe.2022538
Received: 29 April 2022
Revised: 13 July 2022
Accepted: 03 August 2022
Published: 11 August 2022

Research article

Meaningful secret image sharing for JPEG images with arbitrary quality factors

Yue Jiang[1,2,*], **Xuehu Yan**[1,2], **Jia Chen**[1,2], **Jingwen Cheng**[1,2] **and Jianguo Zhang**[3]

[1] National University of Defense Technology, Hefei 230037, China

[2] Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

[3] INFOINNO Information Scurity Evaluation CO.,LTD, Hefei 230022, China

* **Correspondence:** Email: jiangyue17@nudt.edu.cn; Tel: +86055164937111; Fax: +86055164937111.

Abstract: JPEG is the most common format for storing and transmitting photographic images on social network platforms. JPEG image is widely used in people's life because of their low storage space and high visual quality. Secret image sharing (SIS) technology is important to protect image data. Traditional SIS schemes generally focus on spatial images, however there is little research on frequency domain images. In addition, the current tiny research on SIS for JPEG images only focuses on JPEG images with a compression quality factor (QF) of 100. To overcome the limitation of JPEG images in SIS, we propose a meaningful SIS for JPEG images to operate the quantized DCT coefficients of JPEG images. The random elements utilization model is applied to achieve meaningful shadow images. Our proposed scheme has a better quality of the shadow images and the recovered secret image. Experiment results and comparisons indicate the effectiveness of the scheme. The scheme can be used for JPEG images with any compression QF. Besides, the scheme has good characteristics, such as (k, n) threshold, extended shadow images.

Keywords: secret image sharing; JPEG images; quality factor; random elements utilization model; meaningful shadows

1. Introduction

Taking Russia's control method of nuclear weapons in the 1990s as an example, Russia designed a similar ”two out of three” access mechanism with the president, the defense secretary, and the defense official. Any two of the three participants jointly authorize nuclear weapons, while no single participant can use nuclear weapons. A secret sharing scheme can solve this kind of access control problem. This example is a typical $(2, 3)$ threshold secret sharing scheme.

Blakley [1] and Shamir [2] first proposed the concept of secret sharing in 1979. The basic idea of secret sharing is to encrypt secret information into multiple shadow images or shares and distribute them to multiple participants. Only a subset of authorized participants can decrypt the secret, while nonauthorized subsets cannot. In the secret sharing scheme composed of multiple participants, the secret is divided into multiple shadow images and distributed to the corresponding participants. A secret sharing algorithm generally includes two stages: share or generate and recover.

The original secret sharing scheme only focused on the bitstream without considering the specific meaning of these bits. With the increasing emphasis on multimedia security, the relationship between multimedia and encryption is becoming closer and closer. As one of the most important digital media carriers, image-sharing technology is becoming more and more popular. Secret image sharing(SIS) originates from secret sharing, which extends the object of secret sharing to digital images. Secret image sharing is a technology that links secret sharing and images.

Inspired by Shamir's work, Thien and Lin [3] first used Shamir's polynomial-based secret sharing to process digital images in 2002. Thien and Lin embed secret pixels in all $k-1$ polynomial coefficients and encrypt the secret image into a shadow image whose size is $1/k$ times that of the original image. This scheme reduces the size of noise like shadow images and is more suitable for fast transmission in the distributed storage environment. After Thien and Lin, polynomial based secret image sharing methods with more properties have been proposed, such as general access structure [4], extended shadow images [5,6], lossless recovery [7–9], multi secret sharing [10,11], two in one recovery [12,13], authentication function [14], no pixel expansion [15–17], etc.

Traditional SIS schemes generate noise like shadow images, which are challenging to manage and easily arouse the suspicion of attackers in network channel transmission. More and more researchers begin to consider making secret image sharing schemes generate understandable and meaningful shadow images, that is, extended secret image sharing (ESIS) schemes with understandable shadow images. The initial ESIS scheme is a combination of SIS and steganography. Generally, the method used encodes the noise-like shadow images generated by SIS into the cover images [18–20]. Lin and Chan [18] generate shadow images based on polynomial SIS and embed the shadow images into the lowest bit of the cover image. He et al. [19] used LOCOI compression to reduce the statistical correlation of adjacent pixels, generated the shadow image based on polynomial SIS, and embedded the shadow image into the cover image by steganography. The disadvantage of this method is that the generated shadow image looks like an image, the capacity of the secret image is small, and the information needs to be extracted before decryption. Different from the above schemes, the author's team also designed the SIS scheme [5] for comprehensible shadow images by using the random number screening mechanism. The general idea is to randomly screen the polynomial coefficients until it is obtained that the first δ bit of the shadow pixel is equal to the first δ bit of the cover image. On the basis of the Shamir polynomial, P is required. Unlike most other secret image sharing schemes that set $P = 251$, the author's team set $P = 257$, limiting all values to $[0, 256]$. Even if the shadow value is $[251, 255]$, the pixel value within the range can be recovered normally, which improves the quality of the shadow image to a certain extent, especially for extreme images.

At present, most secret image sharing schemes deal with spatial images (such as BMP format images), while there are very few secret sharing schemes for the compressed domain. JPEG image is the most popular digital image format on the Internet. The field of JPEG image steganography is developing in full swing [21–25], but there is little research on secret image sharing of JPEG images. The author's team has made a preliminary exploration of JPEG secret image sharing. Sun of the author's team first proposed a secret image sharing scheme for JPEG images. Sun's scheme [26] has the following disadvantages: the translation value of the DCT coefficient is 1024, $P = 2053$, which makes the complexity of sharing algorithm very high; When selecting the sharing area, the scheme is 8 in the upper left corner 8×8 or 4×4, and for the quantized coefficients, most of the signals are concentrated in the middle and low-frequency components in the upper left corner, and their arrangement is more in line with the zigzag arrangement while selecting a square block will cause a waste of resources; The most significant disadvantage of the scheme is that sun's scheme [26] only aims at the color JPEG image with $QF = 100$, and the sharing effect is good. The values of the quantization table with $QF = 100$ are all 1. Before quantization, the DCT coefficient is equal to the DCT coefficient after quantization, and there is no loss caused by rounding.

The existing SIS scheme for JPEG images only performs well for JPEG images with $QF = 100$. In contrast, the shadow image quality generated for JPEG images with other QF is poor. Besides, the algorithm complexity is very high.

Our motivation is to propose a (k, n) threshold SIS meaningful secret image sharing scheme for JPEG images with arbitrary quality factors to overcome the above problems. To overcome the problem of the high algorithm complexity of the existing JPEG secret image sharing scheme, we made improvements. We calculate the minimum prime number P according to the specific secret image and cover images, reduce p to the minimum value, reduce the screening space of random numbers, and reduce the complexity of the algorithm in the secret image sharing based on polynomial. This paper selects the first 4, 9, or 16 bits after the zigzag arrangement of DCT coefficients when selecting the sharing area, which is more in line with the arrangement law of DCT coefficients after quantization and avoids the waste of computing resources. The most crucial point is that the existing technology only works well for JPEG images with $QF = 100$, and the technology has significant limitations and cannot be popularized and applied. The compression factor of JPEG images targeted in this application can be any value between 0–100. A secret image sharing scheme for JPEG images with arbitrary compression factors is proposed, and shadow images with high image quality and restored secret images are obtained.

The following sections are organized as follows. Section 2 introduces the encoding process of JPEG images, polynomial-based SIS, and random elements utilization model. The proposed (k, n) threshold SIS meaningful secret image sharing scheme for JPEG images with arbitrary quality factors is presented in Section 3. Section 5.1 illustrates the details of the experiments and comparisons. And Section 6 is the conclusion.

2. Preliminaries

2.1. JPEG images

To study the SIS scheme for JPEG images, we must start with JPEG image coding. Here we introduce the process of JPEG coding.

The first process of JPEG image coding is preprocessing, including color space transformation, downsampling, and block segmentation. JPEG image coding first converts the color space of the spatial image into $Y^{'}cbcr$ color space. $Y^{'}$ component represents the brightness of pixels, and cb and cr components represent chromaticity (divided into blue and red components). Then, the image is effectively compressed by reducing cb and cr components (called ”downsampling”). The gray image is discussed later, which does not consider the process of color conversion and downsampling, but only the rest of the compression process. The image is segmented to 8×8, which is processed separately in the following compression process.

Next are the core steps of JPEG image coding: value translation, discrete cosine transform (DCT), quantization, and entropy coding. Value translation is to move the spatial pixel value from the positive range to the range centered on zero before calculating the DCT of the 8×8 block. For gray-scale images, each pixel in the original spatial block is $[0, 255]$, the translation value is 128, and the range of spatial pixel block after translation is $[-128, 127]$. $\boldsymbol{S}$ represents the spatial pixel matrix, and $\boldsymbol{M}$ represents the matrix after value translation, then the formula of value translation is shown in Eq (2.1).

$$\boldsymbol{M = S - 128} \tag{2.1}$$

DCT transform gathers most signals in one corner of the result. The element in the top left corner is the DC coefficient, which is quite large compared with other values. The remaining 63 coefficients are AC coefficients. DCT transform can concentrate the low-frequency component in the upper left corner and the high-frequency component in the lower right corner. The primary information is concentrated in the medium and low-frequency components. Let $\boldsymbol{M}$ be the 8×8 spatial matrix for DCT transformation, then the matrix representation of DCT transformation is shown in Eq (2.2). $\boldsymbol{F}$ represents the matrix after DCT transformation. The DC component in the upper left corner of $\boldsymbol{F}$ saves a large value, and the AC component is close to 0.

$$\boldsymbol{F = T \cdot M \cdot T^T} \tag{2.2}$$

Where $\boldsymbol{T}$ is the discrete cosine transform matrix and $\boldsymbol{T^T}$ is the transpose matrix of $\boldsymbol{T}$. The discrete cosine transform matrix $\boldsymbol{T}$ is shown in Eq (2.3).

$$\boldsymbol{T} = \sqrt{\frac{2}{N}} \begin{bmatrix} \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & \cdots & \sqrt{\frac{1}{2}} \\ cos\frac{\pi}{2N} & cos\frac{3\pi}{2N} & \cdots & cos\frac{(2N-1)\pi}{2N} \\ \vdots & \vdots & \vdots & \vdots \\ cos\frac{(N-1)\pi}{2N} & cos\frac{3(N-1)\pi}{2N} & \cdots & cos\frac{(2N-1)(2N-1)\pi}{2N} \end{bmatrix} \tag{2.3}$$

Human eyes are good at seeing slight differences in brightness in large areas but not at distinguishing high-frequency brightness changes. Reducing the amount of information in high-frequency components can effectively compress pictures. Quantization is to divide each DCT coefficient by the corresponding constant in the quantization table. The quantization table $\boldsymbol{QM}$ used in actual quantization is calculated by the standard quantization matrix and the specified quality factor (QF) (The calculation method is shown in Eq (2.4)). The elements in the quantization table control the compression ratio, and larger values produce more extensive compression. Then round to the nearest whole number. Many high-frequency components are rounded to zero, while many other components become small positive or negative numbers. The rounding operation is the only lossy operation in the whole compression process.

$$QM(u,v) = \begin{cases} max\left(\left\lfloor\left(2 - \frac{QF}{50}\right) Q_0(u,v) + 0.5\right\rfloor, 1\right), & 50 \leq QF \leq 100 \\ \left\lfloor \frac{50}{QF} Q_0(u,v) + 0.5\right\rfloor, & 0 < QF < 50 \end{cases} \tag{2.4}$$

$Q_0(u,v)$ represents the quantization step at the position (u,v) in the standard quantization table.

Finally, the quantized value is entropy coded. Entropy coding is a lossless coding that differentially encodes the quantized DC coefficients. The quantized AC coefficients are arranged in a zigzag, then the data is compressed by 0 run-length coding, and finally, the compressed JPEG image code stream is obtained by Huffman coding.

JPEG image decoding is the inverse of the encoding process. The core steps include entropy decoding, inverse quantization, inverse discrete cosine transform (IDCT), and value translation. Firstly, the JPEG entropy is decoded to obtain the quantized DCT coefficient, then multiplied by the DCT coefficient from the quantization table before quantization. The inverse discrete cosine transform is performed and rounded, and finally, each element of the DCT coefficient is added with 128 to obtain the decompressed spatial image.

2.2. Polynomial-based SIS

The scheme proposed in this paper is to share some DCT coefficients of JPEG images as secret information based on polynomial-based SIS. This section introduces polynomial-based SIS.

In 1979, Shamir [2] and Blakley [1] independently proposed a secret sharing scheme based on polynomials, then Thien and Lin [3] applied polynomial-based secret sharing to SIS for the first time in 2002. In (k,n) threshold polynomial-based SIS, any k or more shares can recover the secret, while any $k-1$ or fewer shares couldn't reconstruct the secret. Equation (2.5) shows the definition of the polynomial, where a_0 is the secret, and the remaining $k-1$ coefficients are randomly chosen from the field of $GF(P)$. Lagrange interpolation is used in the recovery phase to reconstruct the secret, as shown in Eq (2.6).

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod P \tag{2.5}$$

$$f(x) = \sum_{i=1}^{k} f(x_i) \prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{(x - x_j)}{(x_i - x_j)} \tag{2.6}$$

Using polynomial-based SIS for JPEG images is different from the spatial domain. The quantized DCT coefficients of JPEG images have negative numbers, which can not be dealt with in the traditional polynomial-based SIS schemes. It is necessary to translate the quantized DCT coefficients to the positive range. In addition, the modulus P in the polynomial is generally taken as 257 for grayscale images because the pixel value range is [0–255]. However, in the polynomial-based SIS scheme for JPEG images, the quantized DCT coefficients range from -1024 to 1023. Therefore, the P value needs to select the appropriate prime number according to the situation.

2.3. Random elements utilization model

We will use the random elements utilization model to generate meaningful shadow images in the following. Here we introduce the random elements utilization model.

According to the principle of polynomial-based SIS, coefficients a_t $(1 \leq t \leq k-1)$ are selected randomly to obtain shared values, and different coefficients a_t can get different shared values. Coefficients a_t can be regarded as random elements to obtain a specific shared value in the sharing process.

To get meaningful shadow images, we establish random elements utilizing model as Eq (2.7). Where $f_i(s, a_1, \cdots, a_{k-1})$ is the i–th shared value of secret s with random elements $a_t, t = 1, 2 \cdots k-1$, and c_i represents the corresponding value in the cover image. $B_\delta\left(f_i\left(s, a_1, \cdots, a_{k-1}\right) - c_i\right)$ denotes that there are δ similar bits between $f_i(s, a_1, \cdots, a_{k-1})$ and c_i, from high to low bit plane.

$$\begin{aligned} &\sum_{i=1}^{n} \left|B_\delta\left(f_i\left(s, a_1, \cdots, a_{k-1}\right) - c_i\right)\right| \bmod p = 0 \\ &s \cdot t \begin{cases} a_t \in Z \\ a_t \in [0, p), t = 1, 2 \cdots k-1 \\ \delta \in [1, 8] \end{cases} \end{aligned} \tag{2.7}$$

In the sharing process, meaningful shadow images can be obtained if the above model conditions can be met. Moreover, the larger the value of δ is, the more similar the shadow image is to the cover image. The branch and bound method or Monte Carlo method can solve the above model.

3. The proposed scheme

This section proposes a (k, n) threshold meaningful SIS scheme for JPEG images, including sharing and recovery processes. The object of the operation is the quantized DCT coefficients of JPEG images in the process of compression coding.

In the sharing phase, given a secret JPEG image and chosen n cover JPEG images, the proposed scheme is to operate on the DCT coefficients of the JEPG image in the process of compression coding. Firstly, a secret JPEG image and n cover JPEG images are entropy decoded to obtain the corresponding quantized DCT coefficients, and the quantized DCT coefficients are divided into 8×8 blocks. Then, each block is zigzag arranged, and the first *num* bits of the data after the zigzag arrangement are extracted as the secret to be shared. The sharing process of the proposed scheme is shown in Figure 1, the schematic diagram of processing DCT coefficients is shown in Figure 2, and the specific algorithm is shown in Algorithm 1.

In the recovery phase, we first obtain the quantized DCT coefficients by entropy decoding k or more than k shares and divide them into blocks of 8×8. Then zigzag arranges each block and extracts the first *num* bit of the data after zigzag arrangement as a candidate recovery object. Next, all DCT coefficients are translated to the positive range according to $|min|$ determined in the sharing process. The secret *num* bits of each block are recovered by Lagrange interpolation and translated inversely. Then add $64 - num$ zeros in each DCT block. Finally, entropy encoded the DCT blocks to obtain the recovered JPEG image. The recovery process of the proposed scheme is shown in Figure 3.

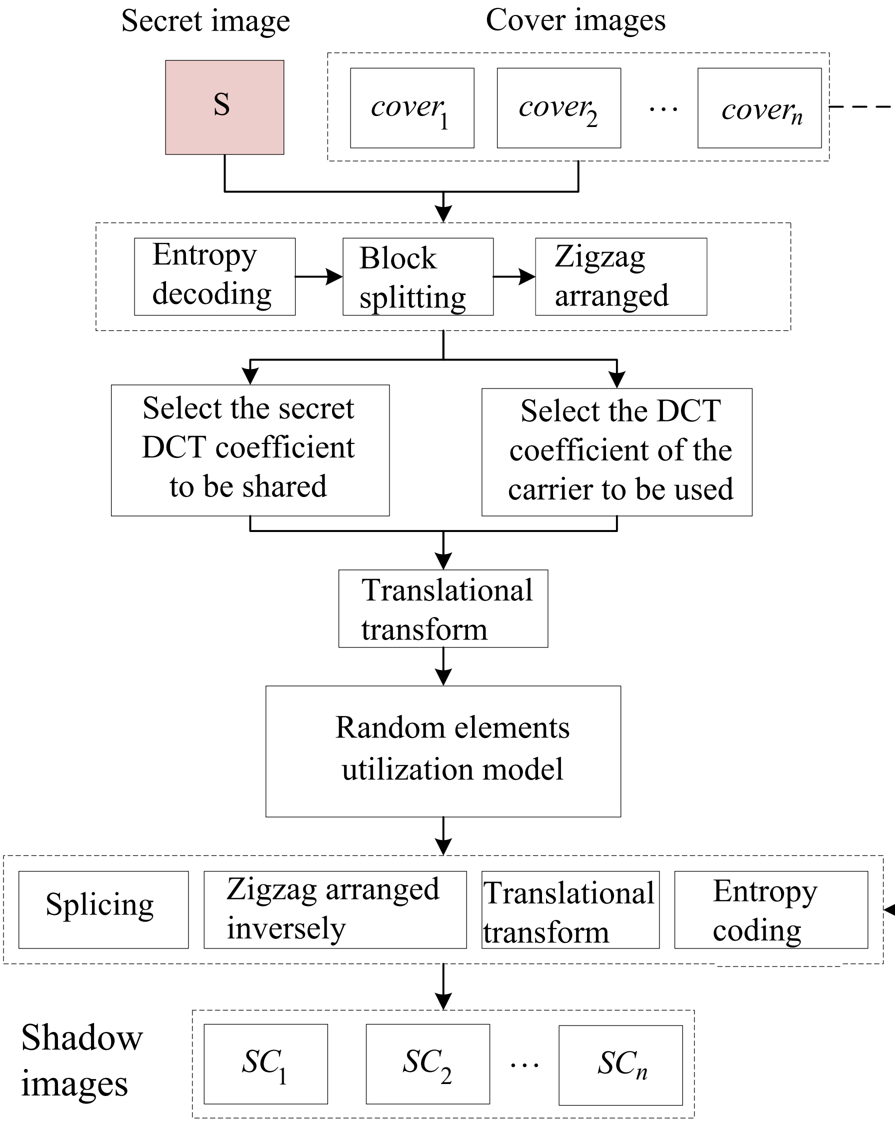


Figure 1. The sharing process of the proposed SIS for JPEG images.

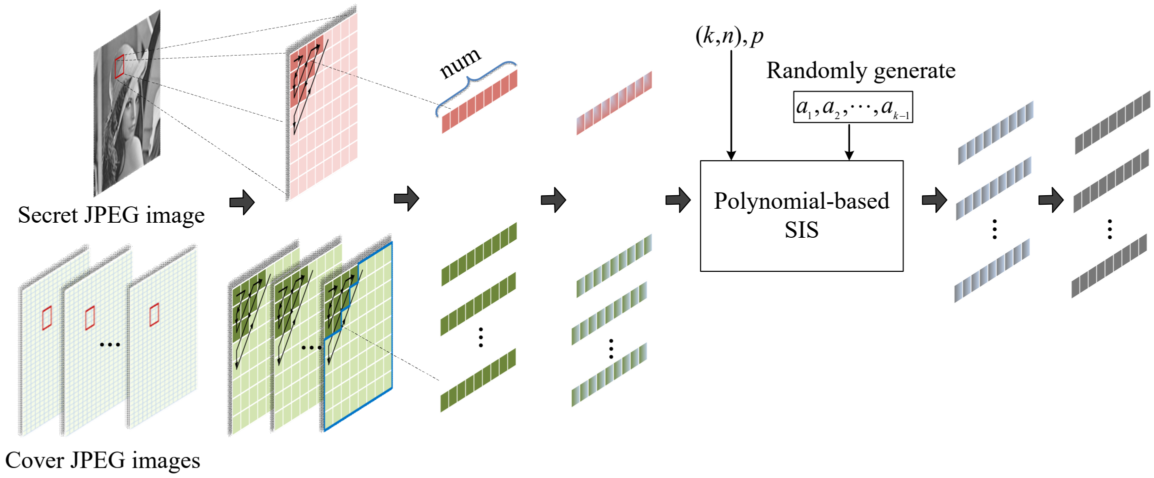


Figure 2. the schematic diagram of processing DCT coefficients.

```
Algorithm 1 The sharing process of the proposed SIS scheme for JPEG image.
Input: A secret JPEG image $S$ with the size of $M \times M$; $n$ cover JPEG images $cover_1, cover_2, \cdots, cover_n$; the threshold parameters $(k, n)$; the number of shared coefficients in each block $num$; the number of similar bits in DCT coefficient between the shares and the cover images $\delta$.
Output: $n$ shadow JPEG images $SC_1, SC_2, \cdots, SC_n$.

Step 1. Obtain the quantized DCT coefficient matrix of the secret JPEG image and the cover JPEG images by entropy decoding $S$ and $cover_1, cover_2, \cdots, cover_n$.
Step 2. Divide the quantized DCT coefficient matrix into 8 × 8 blocks, and each DCT block is represented as $s\_DCTblock_i, cover_1\_DCTblock_i, \cdots, cover_n\_DCTblock_i$.
Step 3. Zigzag arrange each DCT block of each image, and the list of the first $num$ bits extracted is expressed as $S\_DCTblocklist_i, cover_1\_DCTblocklist_i, \cdots, cover_n\_DCTblocklist_i$ , respectively.
Step 4. Find the minimum value $min$ in all lists. If $min \leq 0$, the translation value is $|min|$; Otherwise, the translation value is 0.
Step 5. Obtain the lists after translation $S\_DCTblocklistT_i, cover_1\_DCTblocklistT_i, \cdots$, $cover_n\_DCTblocklistT_i$, according to the translation value.
Step 6. Determine the prime number $P$, according to the values of all lists.
Step 7. Input $(k, n)$, $S\_DCTblocklistT_i, cover_1\_DCTblocklistT_i, \cdots, cover_n\_DCTblocklistT_i$, $P$ and $\delta$ into the random element utilization model to get the $n$ lists of shared value.
Step 8. Splice $num$ bits in each list of shared value and $64 - num$ bits in corresponding cover image DCT list to get $n$ DCT lists of the shares.
Step 9. Obtain the actual value DCT lists of the shares by subtracting $|min|$.
Step 10. Zigzag arrange each DCT lists of the shares inversely, and entropy coding them.
Step 11. Output $n$ shadow images $SC_1, SC_2, \cdots, SC_n$.
```

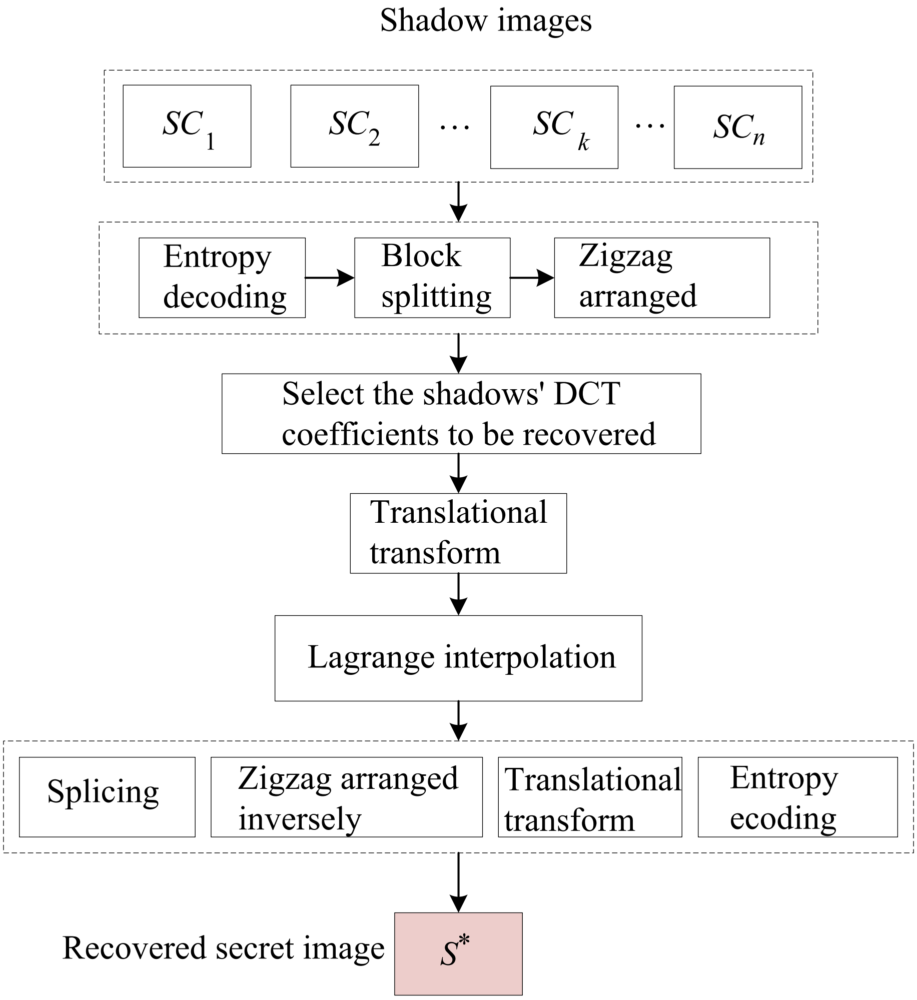


Figure 3. The recovery process of the proposed SIS for JPEG images.

4. Performance analysis

4.1. Security analysis

Because the proposed (k, n) threshold meaningful SIS scheme for JPEG images is constructed based on Shamir's traditional polynomial-based secret sharing, it retains the unconditional security of traditional polynomial-based secret sharing.

Theorem 1. *When k or less than k shadows are collected, the secret DCT coefficients can't be recovered.*

Proof. According to the polynomial secret sharing principle, the secret value is obtained by calculating a $k-1$-degree polynomial expression with a k unknown variable. If k or less than k shadows participate in the recovery, there are be k values that satisfy the Lagrange interpolation expression. Therefore, the secret DCT coefficients can not be recovered when k or less than k shadows are collected.

4.2. Visual quality analysis

For the proposed scheme, the parameters affecting the quality of the shadows and the recovered secret image are expressed as a quintuple (k, n, δ, num, QF). Where (k, n) represents the threshold parameter, and δ denotes the number of similar bits in the DCT coefficient between the shares and the cover images, *num* represents the number of shared coefficients in each block, *QF* is the compression factor of the secret JPEG image.

In the proposed scheme, the secret recovery image is lossy. There are two reasons as follows:

- The secret image is distorted in the sharing process. The DCT block of each secret JPEG image only shares the first *num* bit data after the zigzag arrangement, not all DCT coefficients. For the convenience of calculation, *num* is usually a square number. In addition, the quantized DCT coefficient matrix signal is concentrated in the upper left part, so *num* is preferably less than 32. Therefore, *num* is generally set to 4, 9, or 16.
- The secret image is distorted in the recovery process. There are 64 bits in each DCT block, while *num* bits can be recovered, and the remaining 64 − *num* DCT coefficients are filled with zeros.

Based on the above analysis, we discuss the following three situations:

1) When (k, n, δ, QF) is set as non-constant, the smaller the *num* is, the fewer DCT coefficients are shared, and the more DCT coefficients of the cover image are retained. The higher the similarity between the shadow image and the cover image is. However, the smaller the *num* is, the more zeros will be filled, so the lower the quality of the restored secret image.

2) When (k, n, num, QF) is fixed, the higher the δ is, the higher the quality of the shadow image is. Because there are more similar bits in DCT coefficient between the shares and the cover images, the δ is limited by the (k, n) threshold to generate meaningful shadow images. When the prime number is set to P, there are $(P-1)^{k-1}$ possible shadow value sequences for the DCT coefficients currently processed. The relationship between (k, n, P, δ) should satisfy Eq (4.1).

$$\left(2^{\delta}\right)^{n} \leq (P-1)^{k-1} \tag{4.1}$$

3) When (num, P, QF) is non-constant, the PSNR of the restored secret image is the same no matter how (k, n, δ) changes. The number of DCT coefficients of each block shared determines the amount of secret information carried by the shadow image carries. The amount of secret information in the recovered secret image is also constant.

5. Experimental results and analysis

To verify the effectiveness of the proposed scheme, we implemented some experiments. The performance results will be exhibited in Subsection 5.1. The experimental images in the section are chosen from BOSSbase1.0.5 [27]. Grayscale images with 256 × 256 are randomly selected and converted into JPEG images with compression factors of 40, 50, 60, 70, 75, and 80. The function of *read*() and *write*() in the JPEGIO package is used to simulate entropy decoding and entropy coding. In addition, the proposed scheme is compared with Yan *et al.*'s scheme in Subsection 5.2.

5.1. Experimental results

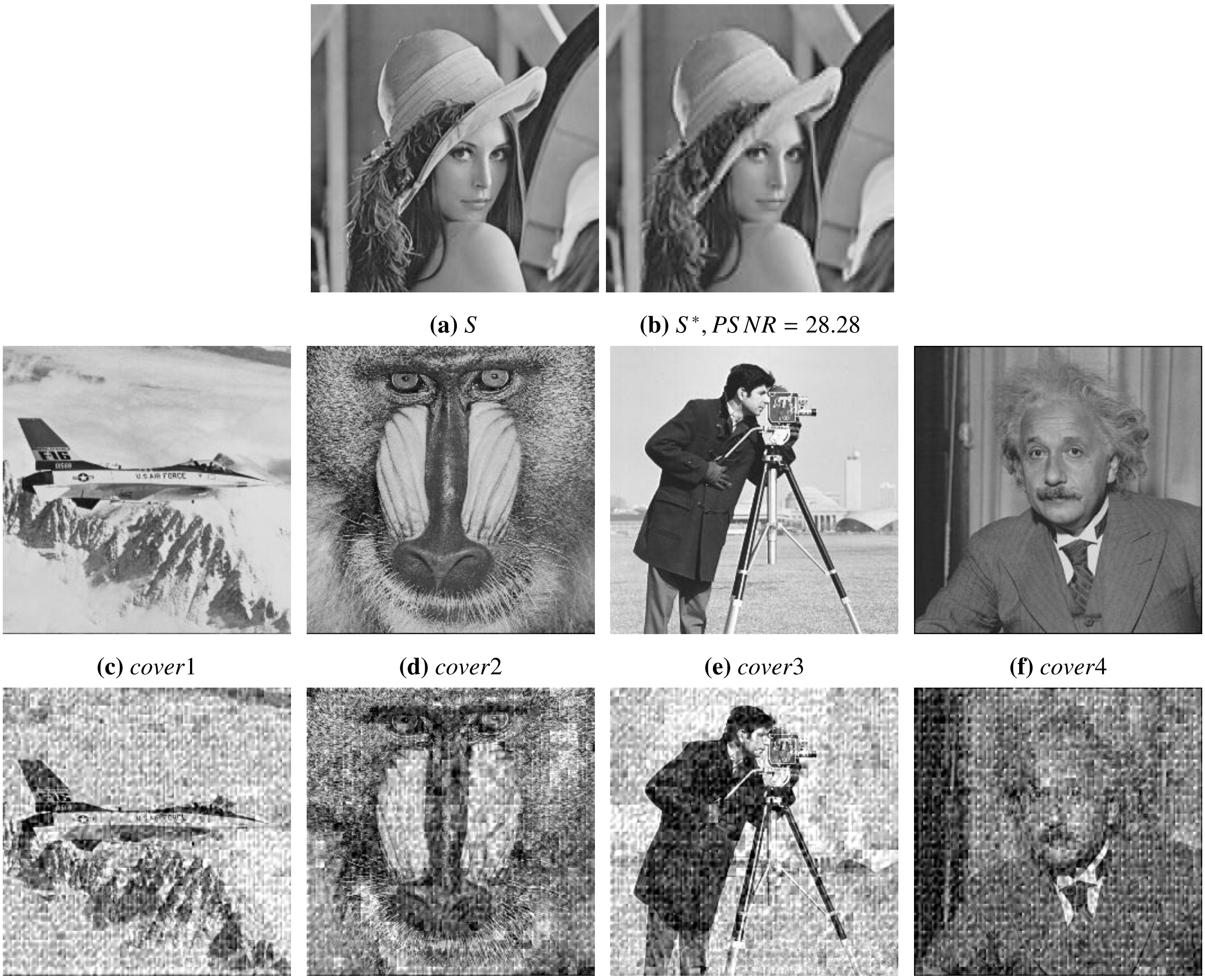
To show the effect of the proposed scheme more comprehensively, we carried out experiments from the following two aspects in this subsection. First, different thresholds should be taken into consideration. Besides, the quintuple (k, n, δ, num, QF) may also influence the performance of the experiments.

Figure 4 illustrates the results of $(3, 4)$-threshold meaningful SIS scheme for JPEG images, where $\delta = 3$, $num = 9$, $id = [11, 13, 19, 21]$ (id is actually the value of x in the polynomial, which refers to x_i in Eq (2.6)), $QF = 75$. The secret grayscale JPEG image with the size of 256 × 256 and $QF = 75$ is shown in Figure 4a. Figure 4c–f show the four grayscale JPEG images with the size 256 × 256 as the input cover images. Four shadow JPEG images changed from cover images are shown in Figure 4g–j. Figure 4b shows the recovered secret JPEG image.

Figure 5 exhibits the results of $(3, 3)$-threshold meaningful SIS scheme for JPEG image, where $\delta = 4$, $num = 9$, $id = [11, 13, 19]$, $QF = 75$. Figure 5a is a secret grayscale JPEG image with the size of 256×256 and $QF = 75$. Figure 5b–d show the three grayscale JPEG images with the size 256×256 as the input cover images. Figure 5e–g show three shadow JPEG images. The recovered secret JPEG image is displayed in Figure 5h.

Figure 5 shows our $(2, 2)$-threshold scheme, where $\delta = 3$, $num = 9$, $id = [11, 13]$, $QF = 75$. Figure 6a displays the secret grayscale JPEG image of 256 × 256 and $QF = 75$. Figure 6b,c show the grayscale JPEG cover images with the size 256 × 256. Figure 6d,e show two JPEG shadow images. The recovered secret JPEG image is shown in Figure 6f.

Table 1 shows visual quality of shadow images under different parameter selections. The variation trend of PSNR of shadow images and recovered secret image with parameters *num* and *QF* are shown in Figures 7 and 8, respectively.

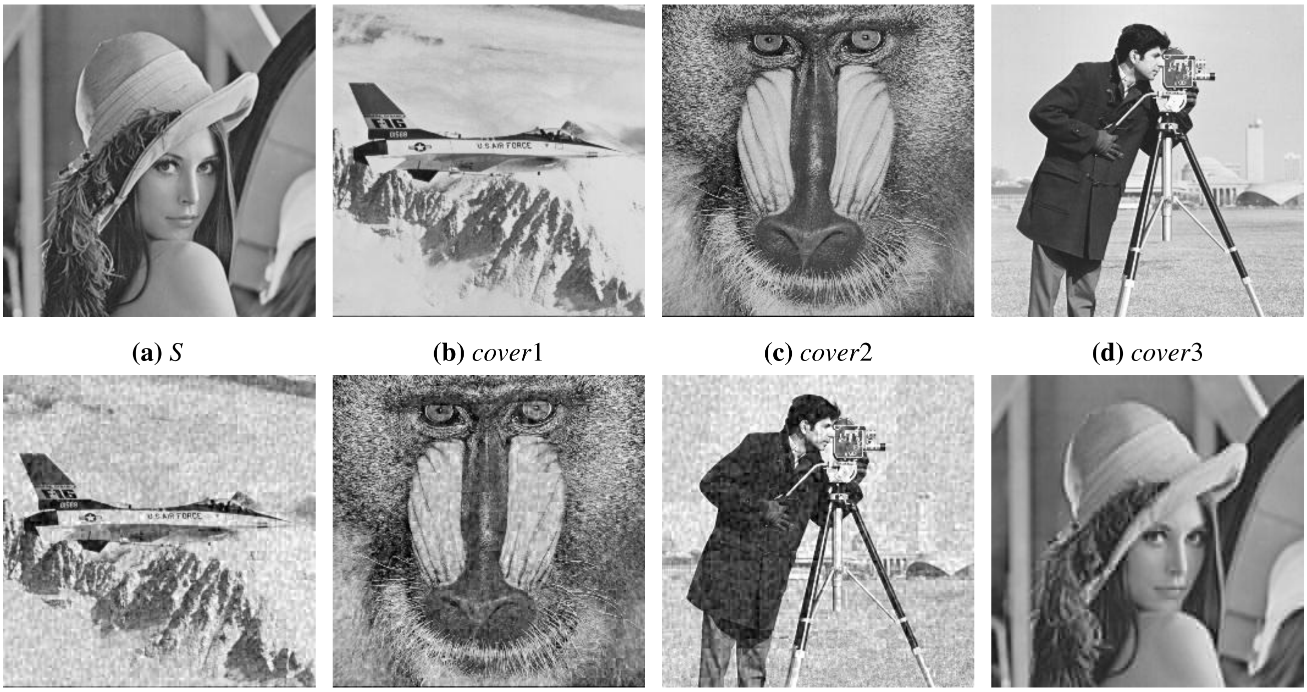


(a) S **(b)** $S^*, PSNR = 28.28$

(c) $cover1$ **(d)** $cover2$ **(e)** $cover3$ **(f)** $cover4$

(g) $SC1, PSNR = 18.10$ **(h)** $SC2, PSNR = 17.53$ **(i)** $SC3, PSNR = 18.12$ **(j)** $SC4, PSNR = 17.55$

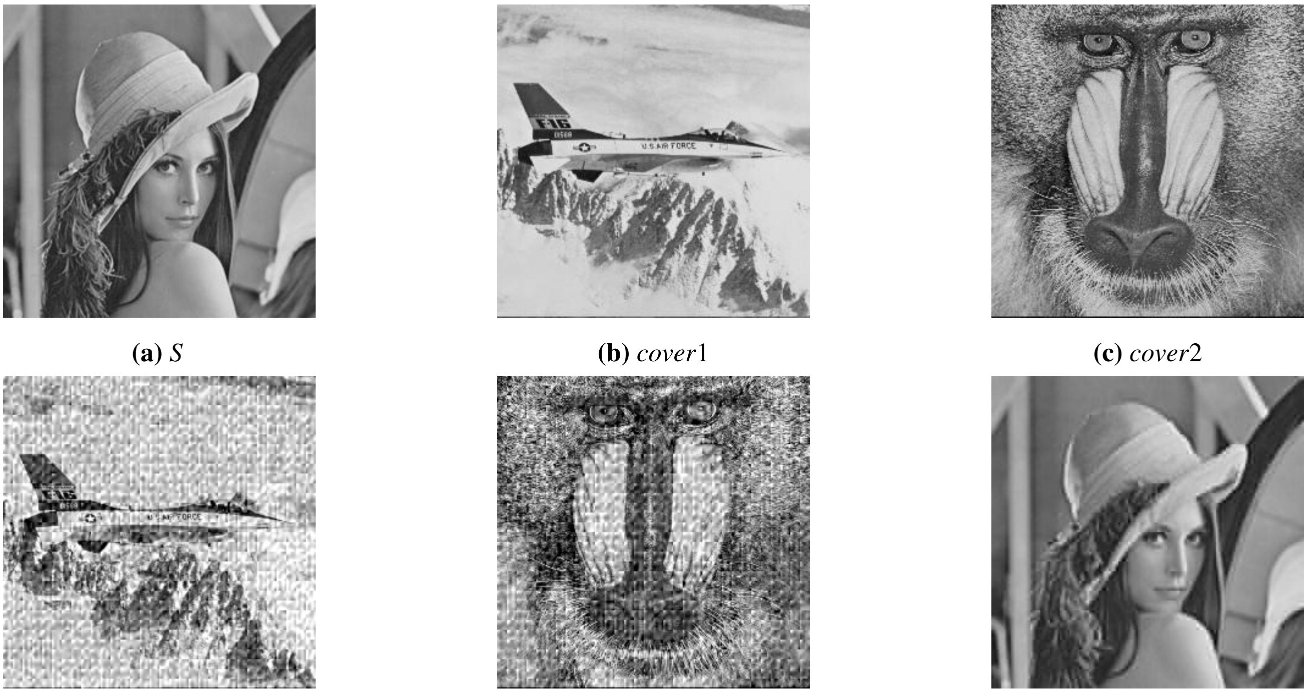
Figure 4. Results of $(3, 4)$-threshold SIS scheme for JPEG images with meaningful shares, $\delta = 3$, $num = 9$, $id = [11, 13, 19, 21]$, $QF = 75$.



(a) S **(b)** $cover1$ **(c)** $cover2$ **(d)** $cover3$

(e) $SC1, PSNR = 24.78$ **(f)** $SC2, PSNR = 24.13$ **(g)** $SC3, PSNR = 24.92$ **(h)** $S^*, PSNR = 28.28$

Figure 5. Results of $(3, 3)$-threshold SIS scheme for JPEG images with meaningful shares, $\delta = 4$, $num = 9$, $id = [11, 13, 19]$, $QF = 75$.



(a) S **(b)** $cover1$ **(c)** $cover2$

(d) $SC1, PSNR = 18.59$ **(e)** $SC2, PSNR = 18.13$ **(f)** $S^*, PSNR = 28.28$

Figure 6. Results of $(2, 2)$-threshold SIS scheme for JPEG images with meaningful shares, $\delta = 3$, $num = 9$, $id = [11, 13]$, $QF = 75$.

Table 1. Visual quality of shadow image under different parameter selection.

(k, n)	$(3, 4)$			$(3, 3)$			$(2, 2)$		
δ	3			4			3		
num	4	9	16	4	9	16	4	9	16
Quality	$PSNR$	$PSNR$	$PSNR$	$PSNR$	$PSNR$	$PSNR$	$PSNR$	$PSNR$	$PSNR$
$SC1$	20.84	18.10	14.21	27.66	24.78	20.59	21.52	18.59	14.68
$SC2$	19.86	17.53	13.70	27.50	24.13	20.16	21.30	18.13	14.52
$SC3$	20.21	18.12	14.43	27.90	24.92	20.47			
$SC4$	20.42	17.55	13.32						
S^*	24.37	28.28	30.48	24.37	28.28	30.48	24.37	28.28	30.48

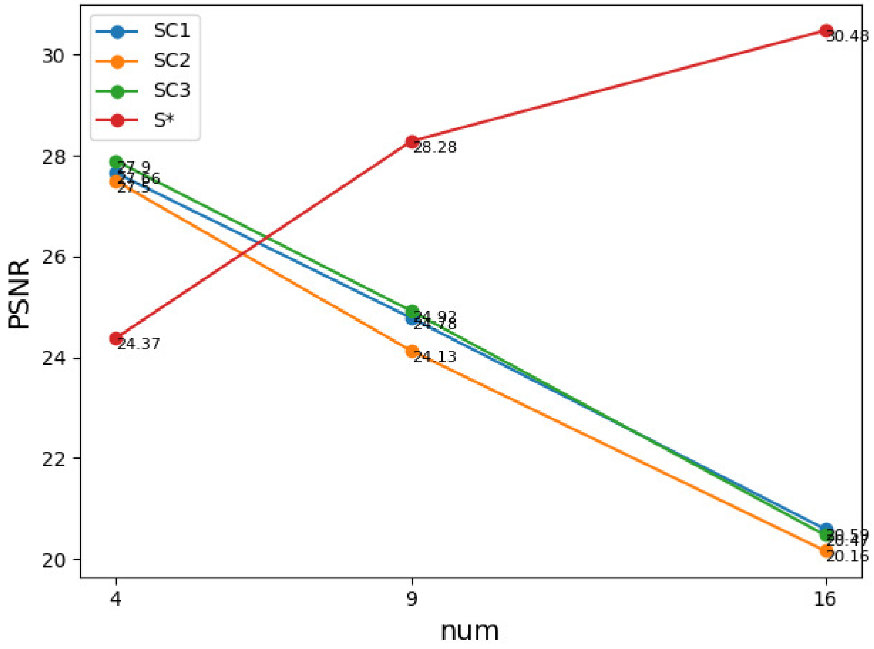


Figure 7. When (k, n, δ, QF) is fixed to $(3, 3, 4, 75)$, the PSNR of shadow images and recovered secret image changes with *num*.

From Figures 4–8 and Table 1, we can draw the following conclusions:

1) Our proposed SIS scheme for JPEG images is effective, and the shadow images are meaningful.

2) The factors affecting the visual quality of shadow images and recovered secret image are consistent with the performance analysis in Subsection 4.2.

3) When (k, n, δ) is fixed, the larger the *num* is, the lower the PSNR of the shadow images are, and the higher the recovered secret image's quality.

4) When *num* is the same, the PSNR of the recovered secret image remains unchanged.

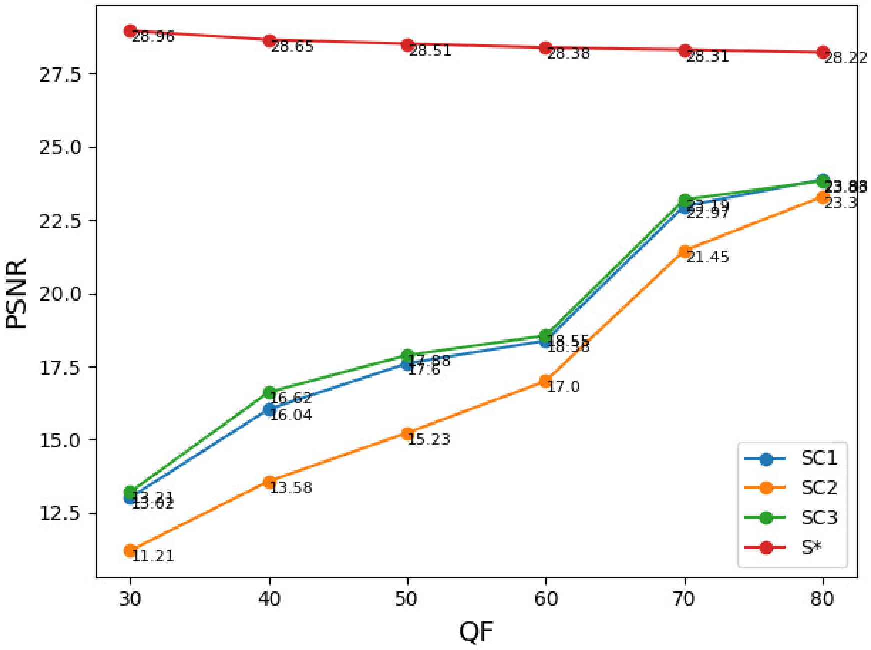


Figure 8. When (k, n, δ, num) is fixed to $(3, 3, 4, 9)$, the PSNR of shadow images and recovered secret image changes with QF.

5) With the increase of QF, the visual quality of the shadow images is better, while the recovered secret image's quality decreases slightly.

5.2. Comparison with Yan et al.'s works

In a sense, the work proposed in this paper can be regarded as a robust secret image sharing scheme for spatial images against JPEG compression, as shown in Figure 9. Our $(3, 3)$ threshold JPEG oriented secret image sharing scheme can be regarded as follows: the spatial image ”S.bmp” is first compressed into ”S.jpg” by the channel with $QF = 75$; ”S.jpg” generates ”SC1.jpg”, ”SC2.jpg” and ”SC3.jpg” after the SIS for JPEG images generation algorithm proposed in this paper. These three images are equivalent to ”SC1.bmp”, ”SC2.bmp” and ”SC3.bmp” through channel compression with $QF = 75$. During restoration, ”SC1.jpg”, ”SC2.jpg”, ”SC3.jpg” restore the secret image through the restoration algorithm of the scheme proposed in this paper to obtain ”S*.jpg” and finally compresses it to the airspace to obtain ”S*.bmp”. This restoration process is equivalent to restoring the secret image from the decompressed spatial image ”SC1.bmp”, ”SC2.bmp” and ”SC3.bmp” to obtain ”S*.bmp”. The whole process corresponds to the scheme proposed by Yan et al. (As shown in Figure 10).

Therefore, here we compare our scheme with Yan et al.'s work [28]. Yan et al. implemented a robust secret image sharing scheme with (k, n) threshold without pixel expansion based on the Chinese Remainder Theorem and error-correcting codes. The scheme uses the method of random screening mechanism to integrate the process of shadow image generation with the process of generating error correction code and generating error correction code while generating shadow so that the generated shadow image itself has internal error correction ability. Considering that the general noise or attack will affect the lower bits of the shadow pixel, such as the lower four bits, the scheme forms an error

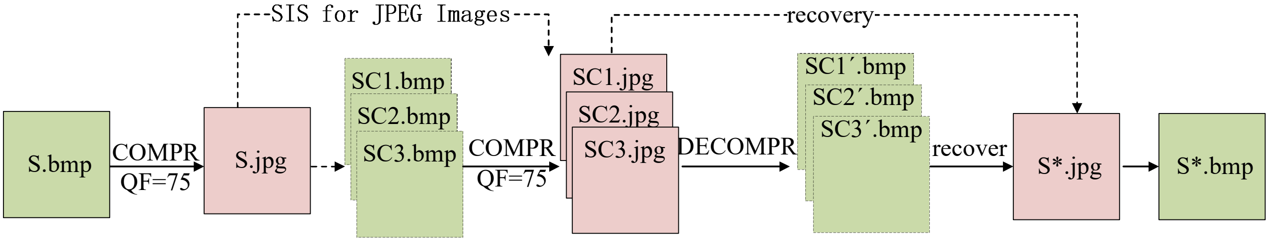


Figure 9. Extended $(3, 3)$ threshold SIS for JPEG images.

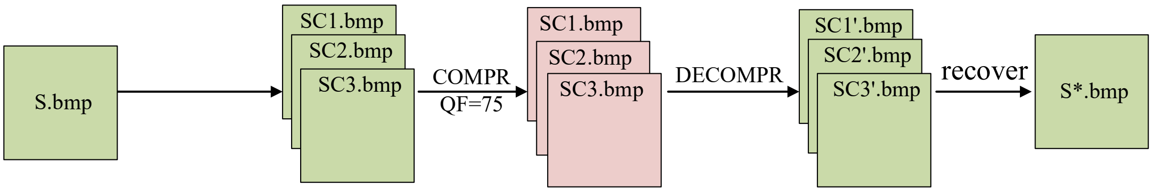
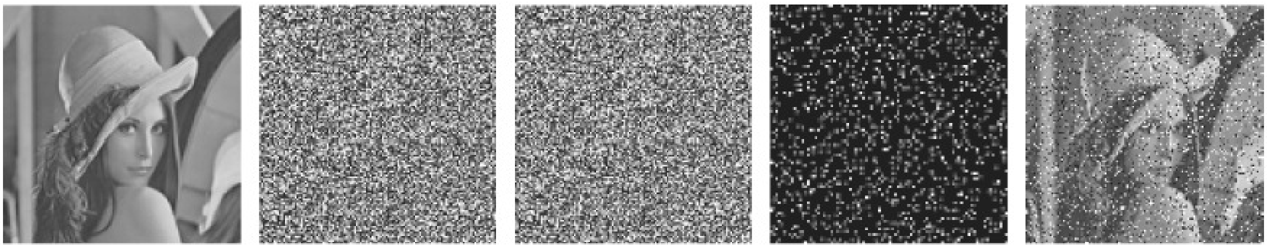


Figure 10. $(3, 3)$ threshold robust SIS by Yan et al..

correction relationship between the lower four bits of the previous pixel and the upper four bits of the next adjacent pixel in the process of generating the shadow, so when the lower four bits of the second pixel are wrong, The high four bits of the previous pixel can correct its error (provided that the noise or attack has little impact on the high four bits, and the high four bits are relatively stable and will not change). In this way, the pixels of the shadow image are generated in turn. And a cascading error correction relationship is formed between the pixels. A slight disadvantage is that the error of the lower four bits of the last pixel cannot be corrected. The scheme realizes the (k, n) threshold and is robust to JPEG compression.

Figure 11 shows the results of the robust $(3, 3)$ threshold SIS scheme proposed by Yan *et al.*, where $m1 = 253$, $m2 = 254$, $m3 = 255$, $HL = 8$, $QF = 100$. Figure 11(a) is the secret image. One shadow image generated is shown in Figure 11(b). The image of the shadow image after JPEG compression with $QF = 100$ is shown in Figure 11(c). Figure 11(d) displays the difference between the shadow image and the compressed image. The recovered secret image is shown in Figure 11(e).This paper proposes the (k, n)-threshold SIS scheme for JPEG images with meaningful shares. The proposed scheme can be regarded as a robust SIS scheme for spatial images against JPEG compression. As shown in Figure 5, the PSNR of the recovered secret image in our proposed with $QF = 75$ is higher than that in Yan *et al.*'s scheme with $QF = 100$. So the proposed SIS scheme for JPEG images has better robustness to JPEG compression. In addition, compared with the Yan *et al.*'s scheme, the shadow image in our scheme is meaningful and can be applied to JPEG images of any QF.

The scheme of Yan et al. [28] is not powerfully robust to JPEG compression because its scheme is designed on the premise that the attack has little impact on the higher bits of the pixel (relatively stable and will not change). This assumption is more consistent with Gaussian noise's impact on the pixel than the impact of JPEG compression on the image. JPEG compression will affect all pixels of the shadow image; When the pixel values before and after compression do not change, there is a specific error correction capability between adjacent pixels. If one of them changes, the error correction capability will be destroyed.



(a) S (b) SC_1 (c) SC'_1 (d) $SC_1 - SC'_1$ (e) $S'_{1'2'3'}, 14.44, 0.2936$

Figure 11. Results of the robust $(3, 3)$ threshold SIS scheme proposed by Yan *et al.*, $m1 = 253$, $m2 = 254$, $m3 = 255$, $HL = 8$, $QF = 100$.

6. Conclusions

This paper proposed a (k, n) threshold meaningful SIS scheme for JPEG images, which can apply to JPEG images of any QF. Starting with the study of JPEG image encoding and decoding, this paper realizes the SIS scheme for JPEG images. Besides, we analyze the reasons for the loss of recovered secret images. We further analyze the impact of the parameters (k, n, δ, num, QF) on the quality of shadow images and recovered secret image. The experimental results indicate the effectiveness of the scheme. The scheme has good characteristics, such as (k, n) threshold and extended shadow images. It can effectively share JPEG images with arbitrary compression factors. In future work, we will focus on a robust SIS scheme against JPEG recompression.

Acknowledgments

This research is funded by the National Natural Science Foundation of China (Grant Number: 61602491).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. G. Blakley, Safeguarding cryptographic keys, *Proc. Afips Natl. Comput. Conf.*, **48** (1979), 313. https://doi.org/10.1109/AFIPS.1979.98

2. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613. https://doi.org/10.1145/359168.359176

3. C. Thien, J. Lin, Secret image sharing, *Comput. Graphics*, **26** (2002), 767–770. https://doi.org/10.1016/S0097-8493(02)00131-0

4. J. B. Feng, H. C. Wu, C. S. Tsai, Y. P. Chu, A new multi-secret images sharing scheme using largrange's interpolation, *J. Syst. Software*, **76** (2005), 326–339. https://doi.org/10.1016/j.jss.2004.07.250

5. T. Liu, L. Lu, H. Yan, Polynomial-based extended secret image sharing scheme with reversible and unexpanded covers, *Multimedia Tools Appl.*, **78** (2018), 1–23. https://doi.org/10.1007/s11042-018-6202-3

6. H. Yan, L. Lu, T. Liu, General meaningful shadow construction in secret image sharing, *IEEE Access*, **6** (2018), 45246–45255. https://doi.org/10.1109/ACCESS.2018.2865421

7. X. Liu, S. Wang, Z. Sang, Z. Zhang, A novel lossless recovery algorithm for basic matrix-based VSS , *Multimedia Tools Appl.*, **77** (2018), 16461–16476. https://doi.org/10.1007/s11042-017-5215-7

8. N. Yang, S. Chen, H. Yu, C. Wang, Improvements of image sharing with steganography and authentication, *J. Syst. Software*, **80** (2006), 1070–1076. https://doi.org/10.1016/j.jss.2006.11.022

9. T. Liu, L. Lu, M. Ding, T. Xuan, A Lossless polynomial-based secret image sharing scheme utilizing the filtering operation, *Secur. Intell. Comput. Big-data Serv.*, **895** (2020), 129–139. https://doi.org/10.1007/978-3-030-16946-6_11

10. P. Li, J. Ma, H. Su, N. Yang, Improvements of a two-in-one image secret sharing scheme based on gray mixing model, *J. Visual Commun. Image Represent.*, **23** (2012), 441–453. https://doi.org/10.1016/j.jvcir.2012.01.003

11. J. Weir, Q. Yan, Sharing multiple secrets using visual cryptography, *IEEE Int. Symp. Circuits Syst.*, 2009. https://doi.org/10.1109/ISCAS.2009.5117797

12. P. Li, N. Yang, Q. Kong, A novel two-in-one image secret sharing scheme based on perfect black visual cryptography, *J. Real-Time Image Process.*, **14** (2018), 41–50. https://doi.org/10.1007/s11554-016-0621-z

13. X. Liu, S. Wang, Z. Sang, Z. Zhang, A novel mapping-based lossless recovery algorithm for vss, *J. Real-Time Image Process.*, **14** (2016), 51–60. https://doi.org/10.1007/s11554-016-0644-5

14. Y. Jiang, Q. Qi, L. Lu, X. Zhou, Secret image sharing with dealer-participatory and non-dealer-participatory mutual shadow authentication capabilities, *Mathematice*, **8** (2020), 234. https://doi.org/10.3390/math8020234

15. H. Yan, X. Liu, N. Yang, An enhanced threshold visual secret sharing based on random grids, *J. Real-Time Image Process.*, **14** (2015), 61–73. https://doi.org/10.1007/s11554-015-0540-4

16. N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognit. Lett.*, **25** (2004), 481–494. https://doi.org/10.1016/j.patrec.2003.12.011

17. Z. Wang, H. Su, Secret image sharing with smaller shadow images, *Pattern Recognit. Lett.*, **27** (2006), 551–555. https://doi.org/10.1016/j.patrec.2005.09.021

18. Y. Lin, H. Chan, Invertible secret image sharing with steganography, *Pattern Recognit. Lett.*, **31** (2010), 1887–1893. https://doi.org/10.1016/j.patrec.2010.01.019

19. F. Liu, K. Wu, Embedded extended visual cryptography schemes, *IEEE Trans. Inf. Forensics Secur.*, **2** (2011), 307–322. https://doi.org/10.1109/TIFS.2011.2116782

20. H. He, Q. Lan, H. Tang, A secure image sharing scheme with high quality stego-images based on steganography, *Multimedia Tools Appl.*, **76** (2017), 7677–7698. https://doi.org/10.1007/s11042-016-3429-8

21. J. Chen, H. Zhou, B. Zhou, Defining cost functions for adaptive jpeg steganography at the microscale, *IEEE Trans. Inf. Forensics Secur.*, **14** (2019), 1052–1066. https://doi.org/10.1109/TIFS.2018.2869353

22. Y. Tao, S. Li, P. Zhang, C. Wang, Towards Robust Image Steganography, *IEEE Trans. Circuits Syst. Video Technol.*, **29** (2021), 594–600. https://doi.org/10.1109/TCSVT.2018.2881118

23. Z. Zhao, X. Guan, H. Zhang, F. Zhao, Improving the robustness of adaptive steganographic algorithms based on transport channel matching, *IEEE Trans. Inf. Forensics Secur.*, **14** (2019), 1843–1856. https://doi.org/10.1109/TIFS.2018.2885438

24. Y. Wang, M. Zhang, X. Li, H. Yu, Non-additive cost functions for jpeg steganography based on block boundary maintenance, *IEEE Trans. Inf. Forensics Secur.*, **16** (2021), 1117–1130. https://doi.org/10.1109/TIFS.2020.3029908

25. T. Taburet, P. Bas, W. Sawaya, J. Fridrich, Natural steganography in jpeg domain with a linear development pipeline, *IEEE Trans. Inf. Forensics Secur.*, **16** (2020), 173–186. https://doi.org/10.1109/TIFS.2020.3007354

26. Y. Sun, *Research on Key Technologies of Robust and Meaningful Secret Image Sharing*, Master's thesis, National University of Defense Technology in Hefei, 2020. In press.

27. P. Bas, T. Filler, P. Tomas, "Break our steganographic system": the ins and outs of organizing BOSS, in *Information Hiding, International Workshop on Information Hiding*, (2011), 59–70. https://doi.org/10.1007/978-3-642-24178-9_5

28. H. Yan, T. Liu, L. Li, L. Lu, Robust secret image sharing resistant to noise in shares, *ACM Trans. Multimedia Comput., Commun., Appl.*, **24** (2021), 1–22. https://doi.org/10.1145/3419750

AIMS Press