Mathematical Biosciences and Engineering

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

MBE, 17(4): 2950–2966
DOI: 10.3934/mbe.2020166
Received: 26 December 2019
Accepted: 04 March 2020
Published: 31 March 2020

Research article

Image inpainting-based behavior image secret sharing

Xuehu Yan*, Xuan Zhou, Yuliang Lu, Jingju Liu and Guozheng Yang

National University of Defense Technology, Hefei 230037, China

* **Correspondence:** Email: publictiger@126.com; Tel: 8655188602882; Fax: 8655188602882881.

Abstract: The polynomial-based image secret sharing (ISS) scheme encodes a secret image into n shadows assigned to n participants. The secret image with high resolution is decoded by Lagrange interpolation when collecting any k or more shadows. Thus, ISS is used in applications such as distributive storage in the cloud, digital watermarking, block chain, and access control. Meaningful shadows are significant in ISS because meaningful shadows decrease the suspicion of image encryption and increase the efficiency of shadow management. Generally, previously meaningful ISS schemes were achieved through embedding the shadows into cover images using information hiding techniques and suffer from large pixel expansion and complex decoding procedure. Digital image processing, such as inpainting (texture synthesis), is a standard technique in multimedia applications. It will be highly significant if ISS can be performed in the processing of a normal digital image processing technique. Generally, the encoding method of an ISS scheme entails the use of a mathematical function that is sensitive to any slight change in the ISS output; therefore, the development of a method for performing the ISS procedure and simultaneously achieving image processing behavior is a key challenge. In this paper, we exploit the behavior ISS (BISS) and realize an image inpainting-based BISS scheme for the (k, n) threshold. Using screening operations, a secret image is encoded into the pixels of cover images by polynomial-based ISS in the processing of inpainting shadows to obtain meaningful shadows similar to the input cover images. In addition, the secret image can be losslessly decoded by Lagrange interpolation when collecting any k or more shadows. Experiments are given to confirm the efficiency of the scheme.

Keywords: image secret sharing; behavior image secret sharing; image inpainting; polynomial; color image; meaningful shadows

1. Introduction

Digital images have a special feature that distinguishes them from general digital data (even though they are a specific form of such data), whereby each binary (grayscale) pixel is represented by a 1 bit

(8 bits); thus, SIS can be easily applied to secret sharing.

The image secret sharing (ISS) scheme encodes a secret image into n shadows assigned to n participants. The secret image is decoded when collecting any k or more shadows. Thus, ISS has been applied to distributed storage in the cloud, digital watermarking, block chain, and access control [1–4].

The basic principles of widely studied high-resolution ISS techniques include visual cryptography (VC), *a.k.a.* visual secret sharing (VSS) [4, 5], and polynomials [6–12].

In VC, for a (k, n)-threshold [11,13–17], the encoded n shadows are usually printed onto transparent films and then assigned to associated n participants. VC has the merit that the secret is decoded without any cryptographic computations by superposing any k or more shadows and using only the human naked eye. Unfortunately, the conventional VC schemes generally have the weaknesses of poor image quality and pixel expansion.

To decode the secret image with high resolution, the first polynomial-based secret sharing scheme for a (k, n) threshold introduced by Shamir [6] entailed the construction of a random $(k-1)$-degree polynomial to obtain n shadows. When any k or more shadows are collected, the secret is decoded with high resolution by Lagrange interpolation. Inspired by Shamir's work, many enhanced polynomial-based ISS schemes [18–21] with additional properties have been introduced. The advantage of polynomial-based ISS is that the decoded secret image is obtained with high resolution and no pixel expansion. However, this technique has the drawbacks that the decoded secret image is generally slightly distorted and the shadows appear as noise (meaningless).

Meaningful shadows are significant in ISS because they decrease the suspicion of image encryption and increase the efficiency of shadow management. More importantly, meaningful shadows can be used to search in the encrypted domain based on image recognition, which is a reasonable approach for distributed storage and cloud computing.

However, most polynomial-based ISS schemes with meaningful shadows [19,22,23] utilize existing information hiding techniques other than ISS, which embed the shadows into n cover images in order to output meaningful steganographic images (shadows). However, this kind of method entails pixel expansion and has a high computational decoding complexity. In addition, meaningfulness is achieved based on information hiding rather than ISS.

Digital image processing, such as inpainting (texture synthesis) [24–26], is a normal behavior in multimedia applications. Therefore, performing ISS in the processing of normal digital image processing behavior will be a significant advance. Recently, Yan et al. [26] proposed a partial ISS scheme for a (k, n)-threshold based on linear congruence and image inpainting. This scheme can recover the full secret image including the secret target part when collecting any k or more shadow images. However, it has some artifacts or secret leakage on the shadow and inputs the same cover image.

The encoding method of an ISS scheme generally entails the use of a mathematical function that is sensitive to any slight change in the ISS output; therefore, how to perform the ISS procedure and simultaneously achieve the image processing behavior is a key challenge, which is the motivation of this paper.

In this paper, we exploit the behavior ISS (BISS) and realize an image inpainting-based BISS scheme for the (k, n) threshold. Figure 1 illustrates the motivation of this paper, where BISS means that digital image processing behavior is utilized to achieve ISS.

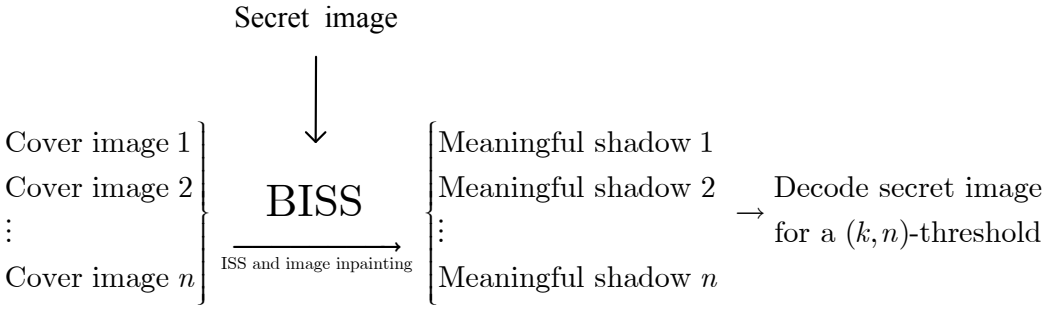


Figure 1. The motivation of this paper.

In the realized inpainting-based [24, 25] BISS scheme for the (k, n) threshold, using screening operations, a secret image is encoded into the pixels of cover images by polynomial-based ISS in the processing of inpainting shadows to obtain the meaningful shadows that are similar to the input cover images. In addition, the secret image can be losslessly decoded by Lagrange interpolation when collecting any k or more shadows. Experiments are given to validate the efficiency of the scheme.

The outline of the rest of the paper is as follows. Section 2 focuses on some basic preliminaries for the realized scheme. In Section 3, the realized scheme is described in detail. Section 4 is devoted to experiments. Finally, Section 5 concludes the paper.

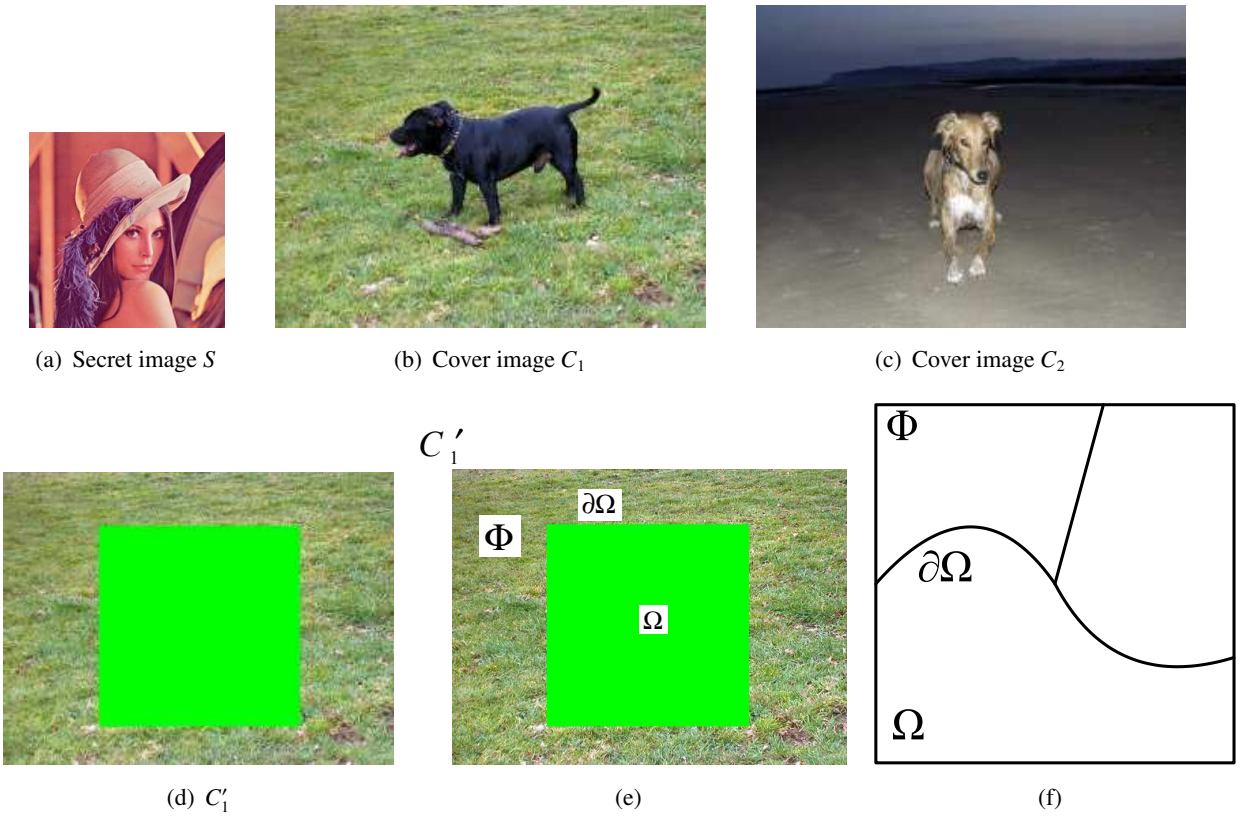
2. Preliminaries

In this section, we give the BISS motivation description and some preliminaries as the basis for the realized method. The original secret image S is shared among the total of n shadows, while the reconstructed secret image S' is reconstructed from t ($k \le t \le n, t \in \mathrm{Z}^+$) shadows.

2.1. Motivation description

As shown in Figure 2, for the given secret image in Figure 2(a), denoted by S, Figure 2(b),(c) show two input cover images C_1 and C_2, Figure 2(d) is obtained by manually selecting and removing the target part (of the same size as S) with the color green from the original cover image C_1, the notations of different regions and their edges are shown in Figure 2(e), and the general notations are given in Figure 2(f). The region Ω denotes the target part with the same size as S, part Φ means the untouched part, and $\partial\Omega$ is the edge of the 2 parts. The shadow-covered secret after sharing is denoted by $SC_i, i = 1, 2, \cdots, n$ for the (k, n) threshold.

A BISS problem can be described as follows: For the selected target part Ω and the associated cover images $C_1, C_2, \cdots, C_n$, a BISS scheme outputs n meaningful shadows $SC_i, i = 1, 2, \cdots, n$, assigned to n associated participants, and each shadow has an appearance similar to a cover image. When any k or more shadows are collected, the secret image can be decoded. However, even if infinite computational power is available, no part of the secret image will be decoded when less than k shadows are collected.



(a) Secret image S (b) Cover image C_1 (c) Cover image C_2

(d) C_1' (e) (f)

Figure 2. An example of the BISS problem description. (a) Secret image S; (b),(c) same input cover image C_i; (d) C_1' obtained by manually selecting and removing the target part with the color green from the original cover image C_1; (e) notations in this example; (f) general notations.

2.2. Polynomial-based image secret sharing

The current processing pixel value of the grayscale secret image is denoted by s, and then, to encode s into n pixels for n corresponding shadows by using the polynomial-based ISS scheme [6], the steps will be repeated until all of the secret pixels have been processed.

Step 1: Construct a $k-1$ degree polynomial as follows.

$$g(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P \tag{2.1}$$

where $a_0 = s$, a_i is random in $[0, P-1]$ for $i = 1, 2, \cdots k-1$ and $P = 251$.

Step 2: Calculate

$$sc_1 = g(1), \cdots, sc_i = g(i), \cdots, sc_n = g(n) \tag{2.2}$$

In the decoding phase of polynomial-based ISS, for any given k pairs among the total n pairs $\{(i, sc_i)\}_{i=1}^{n}$, where i is the ith participant's order label, using Lagrange interpolation, we can solve for the coefficients of $g(x)$ and finally calculate $s = g(0)$. By contrast, the secret image S will not be decoded with any less than k shadows.

Figure 3 gives an example by directly applying the polynomial-based ISS method for the $(2, 2)$ threshold to BISS, where the same input secret image and cover images as those for Figure 2 are used. We find that the target part can be decoded with high resolution (with slight loss), while the corresponding target parts of the shadows are noise-like, decreasing the efficiency of shadow management and increasing the suspicion of encryption.

Polynomial-based sharing idea will be selected in our scheme as the basic ISS method. In the realized scheme, polynomial-based ISS will be enhanced to be lossless and meaningful in the processing of inpainting shadows. .

(a) Shadow SC_1 (b) Shadow SC_2 (c) Decoded secret image S'

Figure 3. Experimental results of directly applying the polynomial-based ISS method for the $(2, 2)$ threshold to BISS. (a),(b) Two shadows SC_1 and SC_2; (c) cropped secret image S' decoded from SC_1 and SC_2.

2.3. Image inpainting

Image inpainting refers to the process of reconstructing the lost or damaged part of an image. Its essence is the process of recovering the complete information according to the lost incomplete information. The inpainting features used for an image are generally discussed as follows.

1) Image inpainting technology is to analyze images according to the rules of human vision, which mainly depends on the research of image model and the cognitive rules of human vision.

2) How to fill the target part is mainly determined by the overall situation of the image. The purpose of image inpainting is to maintain the harmony and unity of the whole original image.

3) The original structure around the target part should be extended to the inside of the target part.

4) The target part can be divided into several areas by the extension of the surrounding structure, and each area is filled with a color or patch similar to the surrounding boundary.

5) Repaint the details inside the target part, that is, match the texture.

6) The basic idea of image inpainting method based on texture synthesis is to select appropriate patch samples from known untouched part, synthesize or copy them to the defect area, and ensure **the similarity and continuity of texture and structure** at the same time. At this point, the process of matching, searching and filling, and the determination of patch priority are the most important.

Among the many image inpainting techniques developed and reported in the literature, the widely used and investigated approach of Criminisi et al. [24, 25] will be adopted in our scheme. We will describe the image inpainting approach of Criminisi et al. in detail. The key feature in the design of this method is the selection of the patch priority order during region filling. The patch with the highest priority is filled preferentially. The priorities will be updated after each filling until the whole target is completely inpainted in the same manner. The main inpainting process is as follows.

1) Select the target part Ω to be inpainted, and $\Phi = C - \Omega$, where C denotes the whole image.

2) Use the image texture feature to determine the size of the template window, denoted by Ψ_p , where any $p \in \partial\Omega$ represents the center of the template window, and the size of the window must be larger than the largest texture element.

3) Calculate patch priorities according to Eq (2.3), i.e., the product of the data term and the confidence term.

$$W(p) = C(p)D(p) \tag{2.3}$$

where $C(p)$ and $D(p)$ represent **the data term and the confidence term**, respectively, and are defined as

$$D(p) = \frac{\left|\nabla S_p^{\perp} \cdot n_p\right|}{a} \tag{2.4}$$

$$C(p) = \frac{\sum\limits_{q \in \psi_p \cap \bar{\Omega}} C(q)}{\left|\psi_p\right|} \tag{2.5}$$

where $\left|\psi_p\right|$ denotes the area of ψ_p and a is a normalization factor. At point p, $\nabla S_p^{\perp}$ and n_p are the isophote direction and the normal vector direction, respectively.

The data term expresses the difference between the normal vector direction and the isophote direction. The confidence term measures the amount of reliable information in the template window. In other words, when the difference between the normal vector direction and the isophote direction is smaller and the template window contains more information, the priority of the patch will be higher.

4) Find $\hat{p}$ by using Eq (2.6) and, in the source image, the block $\psi_{\hat{q}} \in \Phi$ with the highest matching by using the template window as specified by Eq (2.7), where the sum of squared Differences (SSD) is

adopted as the evaluation standard. Finally, the patch of the current window is replaced by the highest matching block.

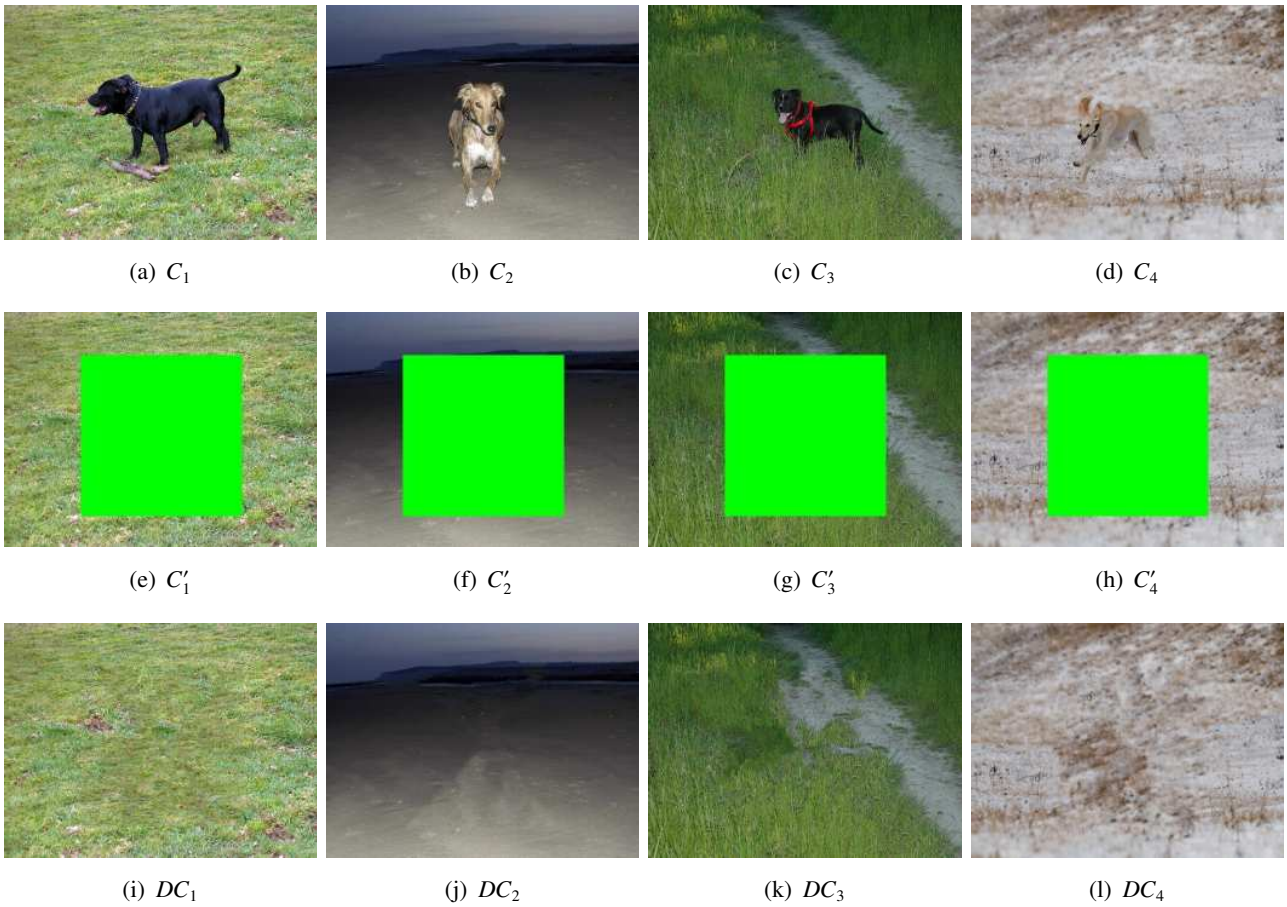
$$\hat{p} = \arg \max_{p \in \partial\Omega} W(p) \tag{2.6}$$

$$\hat{q} = \arg \min_{q \in \Phi} d(\psi_{\hat{p}}, \psi_q) \tag{2.7}$$

5) For any $q \in \psi_{\hat{p}} \cap \Omega$, after each filling process, renew the confidence terms $C(q) = C(\hat{p})$.

6) Repeat steps 3–5 until the image is completely inpainted.

As examples, the inpainted images obtained using the approach of Criminisi et al. are shown in Figure 4. Some other visually plausible images are obtained, and therefore, image inpainting will be used in the realized scheme to achieve meaningful shadows.



(a) C_1 (b) C_2 (c) C_3 (d) C_4

(e) C_1' (f) C_2' (g) C_3' (h) C_4'

(i) DC_1 (j) DC_2 (k) DC_3 (l) DC_4

Figure 4. Examples of the inpainted images obtained using the approach of Criminisi et al. (a–d) Cover images; (e–h) C_i' obtained by manually selecting and removing the target part with the color green from the cover image C_i; (i–l) directly inpainted images.

3. The realized BISS scheme

In this section, we will realize an image inpainting-based BISS scheme for the (k, n) threshold. We will encode the original secret image S and the selected target part Ω of the cover image, resulting in n output meaningful shadows $SC_1, SC_2, \cdots SC_n$. Prior to describing the realized scheme in detail, we first describe the selection of the patch priority order in region filling.

3.1. Filling order selection

In ISS, n shadows will be output in the inpainting processing. According to Eq (2.6), as shown in Figure 5, each shadow will have its own current filling order, *a.k.a.* $\hat{p}_i$. The n orders will be different for the n shadows, but the order should be unique in ISS to avoid shape distortion in order to successfully decode the secret.

Thus, we have to determine the filling order for different shadows from possible n candidate orders. Our design is to select the filling order $\hat{p_{i^*}}$ with the highest patch priority in order to achieve better image quality of the shadows, i.e., $i^* = \arg\max_{i\in[1,n]} W_i(\hat{p}_i)$ and $\hat{p}_i = \hat{p_{i^*}}$, $i = 1, 2, \cdots n$.

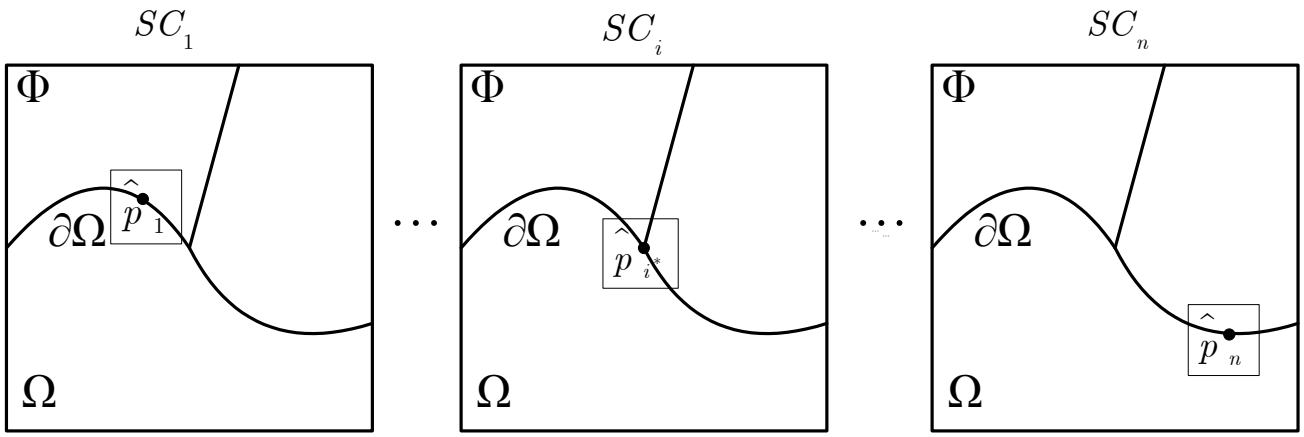


Figure 5. Filling order selection strategy.

3.2. The realized method

Our generation steps are described in Algorithm 1.

In Algorithm 1, we note the following:

1) In Step 2, each shadow has its own filling order (highest priority), i.e., $\hat{p}_i$. To inpaint synchronously, in Step 3 from the n candidate orders, the highest priority is selected as the the adopted order for inpainting all of the n shadows.

2) Δ is used to control the image quality between the shadows and the directly inpainted images. To satisfy $f(x_i) < P - 1$ and $\left|f(x_i) - C'_{i,pl}(h, w)\right| \leq \Delta$, all the possible values of $a_1, a_2, \cdots, a_{k-1}$ will decrease to $N_A = 256^{k-1} \times \left(\frac{2\Delta}{256}\right)^n$, and, thus $\Delta = \frac{\sqrt[n]{N_A \times 256^{n+1-k}}}{2}$.

3) In Step 8, each color image can be decomposed to three planes, and each plane is similar to a grayscale image.

Algorithm 1. The realized BISS scheme for the (k, n) threshold.

Input: The threshold parameters (k, n), a color secret image S with size $H \times W$, and n color cover images $C_1, C_2, \cdots C_n$.

Output: n color shadows $SC_1, SC_2, \cdots SC_n$.

Step 1: Remove the target part Ω_i with the same size as S, to obtain C_i', for $i = 1, 2, \cdots n$. Let C_i' be the input uninpainted image. Use the method in section 2.3 to determine the size of the template window, denoted by Ψ_{p^*}.

Step 2: For each shadow, find $\hat{p}_i$ using Eq (2.6).

Step 3: Find $i^* = \arg\max_{i\in[1,n]} W_i(\hat{p}_i)$, and set $\hat{p}_i = \hat{p_{i^*}}$, $i = 1, 2, \cdots n$.

Step 4: For each cover image, according to $\hat{p}_i$ and Eq (2.7), search for the most matching block to gain $\psi_{\hat{q}_i}$, and then, replace the patch of the current window by the most matching block, for $i = 1, 2, \cdots n$.

Step 5: For each position $(h, w) \in \{(h, w)|H_1 \le h \le H_2, W_1 \le w \le W_2\}$, where (H_1, W_1) and (H_2, W_2) denote the coordinates of the current processing template window, repeat Steps 6–9.

Step 6: Let N_A represent the number of available random values in the sharing phase, and initialize $N_A = 2$.

Step 7: Compute $\Delta = \frac{\sqrt[n]{N_A \times 256^{n+1-k}}}{2}$, where Δ denotes an image quality threshold.

Step 8: Decompose all the color images to three (R, G, B) grayscale planes. For each plane, repeat Step 9.

Step 9: Construct the following $k-1$ degree polynomial.

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod P \tag{3.1}$$

where $a_0 = S(h, w)$, a_i is random in $[0, P]$, and $P = 257$, for $i = 1, 2, \cdots k-1$.

Let $C'_{i,pl}(h, w)$ denote the plth plane of the ith shadow, for $i = 1, 2, \cdots n$ and $pl = R, G, B$.

Screen all of the possible values of $a_1, a_2, \cdots, a_{k-1}$, and compute $f(x_i)$. Check if $f(x_i) < P - 1$ and $\left|f(x_i) - C'_{i,pl}(h, w)\right| \le \Delta$, for $i = 1, 2, \cdots n$, then, calculate $C'_{i,plane}(h, w) = f(x_i)$ and go to the next plane or position; otherwise, $N_A = N_A + 1$, and go to Step 7.

Step 10: Renew the confidence terms after each filling process $C'(q_i) = C'(\hat{p}_i)$m for any $q_i \in \psi_{\hat{p}_i} \cap \Omega$, $i = 1, 2, \cdots n$.

Step 11: Repeat Steps 2–5 until each cover image is completely inpainted.

Step 12: Output n shadows $C'_1, C'_2, \cdots C'_n$.

4) After the patch of the current window is replaced by the most matching block in Step 4, the secret block of the current window is encoded into n corresponding blocks with close values based on polynomial-based ISS sharing to replace the patch of the current window in Steps 8-9. Then, the modified patches of the current window will be the basis for the subsequent inpainting processing. Although the ISS sharing processing may introduce slight noise or error into the shadows, the already inpainted block with slight noise will be the input of the next inpainting round. Based on the current input, the order with the highest priority and the most matching block will also be selected. Finally, meaningful shadows will be obtained in a visually plausible way.

5) In Step 9, because grayscale $a_1, a_2, \cdots, a_{k-1}$ are random and all the possible values of $a_1, a_2, \cdots, a_{k-1}$ are screened to satisfy $\left|f(x_i) - C'_{i,pl}(h,w)\right| \leq \Delta$, for $i = 1, 2, \cdots n$, by setting $C'_{i,plane}(h,w) = f(x_i)$, the values of the shadow pixels are close to those of the cover image pixels such that meaningful shadows can be obtained.

6) A prime number $P = 257$ is selected in Step 9, and by using screening operations on $a_1, a_2, \cdots, a_{k-1}$, $f(x_i) < P - 1$ will be satisfied to achieve the value of the shadow pixel in the range of $[0, 255]$ and lossless decoding.

7) If $f(x_i) < P - 1$ and $\left|f(x_i) - C'_{i,pl}(h,w)\right| \leq \Delta$ are not satisfied after screening all the possible values of $a_1, a_2, \cdots, a_{k-1}$, N_A is increased to increase the value of Δ, and thus, the conditions can be more easily satisfied. Generally, $N_A \leq 16$ is satisfactory.

8) x_i, such as 1,33,67 and 101, will be specified in our experiments in order to achieve better image quality and security.

9) Since every position has three color channels (planes), in Step 9, after the current plane is finished, we go to the next plane or position.

The secret decoding of the realized scheme is the same as polynomial-based ISS based on color decomposition, *a.k.a* Lagrange interpolation when any k or more shadows are collected.

4. Experimental results and analyses

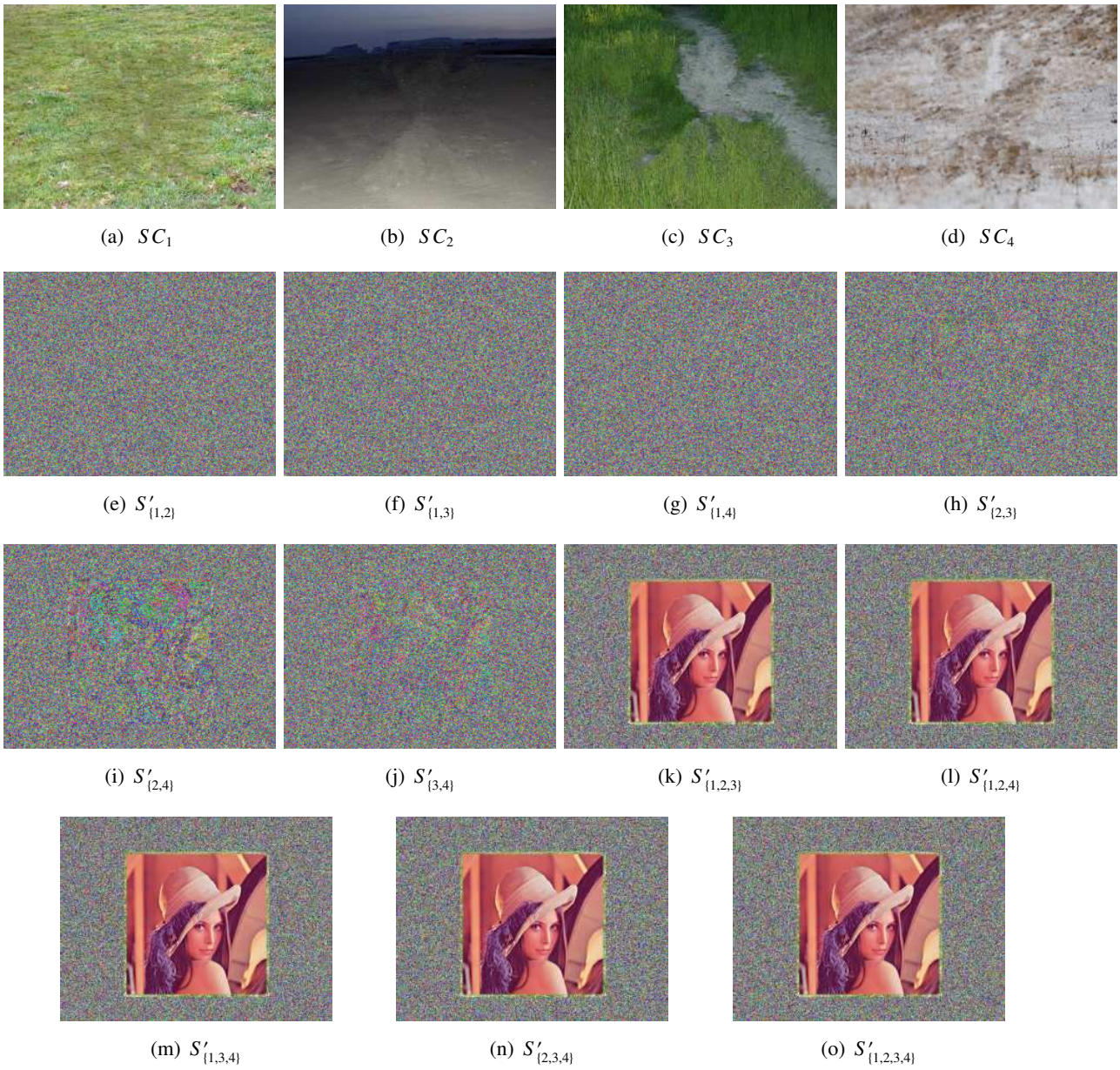
In this section, experiments and analyses are performed to evaluate the effectiveness of the realized method. In the experiments, the secret image in Figure 2(a) with the size of 256×256 and the cover images in Figure 4(a–d) with the size of 500×375 will be employed.

4.1. Image illustration

The simulation results obtained by the realized BISS scheme for case $(3, 4)$ are shown in Figure 6, where Figure 6(a–d) present the encoded four shadows SC_1, SC_2, SC_3, and SC_4 and the decoded results obtained by Lagrange interpolation with any two or more shadows are illustrated in Figure 6(e–o). Here, $S'_{\{1,2\}}$ denotes the secret image decoded with SC_1 and SC_2. The shadows in Figure 6 corresponding to the target part are meaningful, and they look reasonable to the human eyes. When any three or more shadows are collected, lossless secret images are obtained. However, no information on the secret image is decoded when fewer than three shadows are collected.

Additionally, the $(2, 2)$ threshold simulation results are shown in Figure 7, and it is observed that the results are similar to the results of the simulations described above.

Based on the above-described results, we know the following.



(a) SC_1 (b) SC_2 (c) SC_3 (d) SC_4

(e) $S'_{\{1,2\}}$ (f) $S'_{\{1,3\}}$ (g) $S'_{\{1,4\}}$ (h) $S'_{\{2,3\}}$

(i) $S'_{\{2,4\}}$ (j) $S'_{\{3,4\}}$ (k) $S'_{\{1,2,3\}}$ (l) $S'_{\{1,2,4\}}$

(m) $S'_{\{1,3,4\}}$ (n) $S'_{\{2,3,4\}}$ (o) $S'_{\{1,2,3,4\}}$

Figure 6. Experimental result for the realized scheme for the threshold $(3, 4)$.

(a) SC_1 (b) SC_2 (c) $S'_{\{1,2\}}$

Figure 7. Experimental result for the realized scheme for the threshold $(2, 2)$.

1) Each shadow is meaningful and looks reasonable to the human eyes. Each shadow separately looks similar to a natural cover image.

2) An arbitrary secret image is successfully inpainted into the visually plausible shadows.

3) We cannot decoding the secret when $t < k$ shadows are collected; when $t = k$ or more shadows are collected, the secret image is decoded losslessly.

4) A BISS for the (k, n) threshold is achieved.

4.2. Image quality

The image quality is evaluated using the peak signal-to-noise-ratio (*PSNR*) given in Eq (4.1) and the structural similarity index measure (SSIM) [27] given in Eq (4.3). The same secret image shown in Figure 2(a) and the cover images shown in Figure 4(a–c) are used to perform the experiments.

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})\text{dB} \tag{4.1}$$

where

$$MSE = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}[S'(h,w) - S(h,w)]^2 \tag{4.2}$$

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \tag{4.3}$$

where

$l(x,y) = \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1}$

$c(x,y) = \frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2}$

$s(x,y) = \frac{2\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3}$

$\mu_x, \mu_y, \sigma_x, \sigma_y, and\ \sigma_{xy}$ mean the local means, standard deviations, and cross-covariance for images x and y. In this paper, we assume $C_3 = \frac{C_2}{2}, \alpha = \beta = \gamma = 1$.

For the secret target area and (k, n) ($2 \le k \le n, 2 \le n \le 4$) threshold, the PSNR and SSIM between SC_i and DC_i for the target area, for $i = 1, 2, \cdots, n$, are given in Table 1. From Table 1, when n is fixed, a larger value of k leads to better image quality of the shadow since a larger value of k results in a lower value of Δ; when k is fixed, a larger value of n leads to a worse image quality of the shadow.

Table 1. Average PSNR and SSIM between SC_i and DC_i for the target area.

Threshold (k,n)	PSNR	SSIM
(2,2)	19.1913	0.3336
(2,3)	15.1980	0.2759
(3,3)	19.2590	0.4092
(3,4)	17.8137	0.2973
(4,4)	17.8643	0.2995

4.3. Embedding capacity

We intend to introduce and discuss the embedding capacity of the presented scheme as follows.

Definition 1 (Embedding capacity)**.** *When n cover images with a size of $H_C \times W_C$, denoted by $C_1, C_2, \cdots C_n$, are input, a secret image, represented by S, with a size of $H_S \times W_S$ is encoded into n shadows, denoted by $SC_1, SC_2, \cdots SC_n$, with a size of $H_{SC} \times W_{SC}$, the embedding capacity, denoted by EC, can be employed to evaluate the average embedding rate per shadow bit, as in Eq (4.4).*

$$EC = \frac{L_S \times H_S \times W_S}{n \times L_{SC} \times H_{SC} \times W_{SC}} \tag{4.4}$$

where L_x, H_x, and W_x denote the color level, image height, and image weight of x, respectively. For a binary image, $L_x = 1$, $L_x = 8$ for a grayscale image and $L_x = 24$ for a RGB color image.

We further explain and analyze Definition 1 as follows.

- In Eq (4.4), the denominators include the total bits in all shadows; the numerator indicates the total bits embedded in the output shadows.
- A larger pixel expansion will lead to lower EC based on Eq (4.4) because of the larger $W_{SC} \times H_{SC}$.
- $L_{SC} = 24$ and $L_S = 24$ in the presented scheme. Thus, $EC = \frac{H_S \times W_S}{n \times H_{SC} \times W_{SC}}$ in the presented scheme.

According to Eq (4.4), the embedding capacity of Figure 7 and Figure 6 is 0.175 and 0.087, respectively.

4.4. Comparisons with related schemes

We compare our BISS with the schemes of Yan et al. [26] and Ding et al. [9], where the same secret image as in Figure 2(a) and the $(3, 3)$ threshold are used. These are chosen for comparison because the scheme of Yan et al. also utilizes image inpainting to achieve partial image secret sharing and the scheme of Ding et al. relies on pixel expansion based on a polynomial for the (k, n) threshold.

Yan et al. [26] proposed a partial ISS scheme for the (k, n)-threshold based on linear congruence and image inpainting. Their scheme can recover the full secret image including the secret target part when collecting any k or more shadow images. We use the same parameters as Yan et al. [26] to perform the comparisons shown in Figures 8 and 9, where $k = 3, n = 3$. Figure 9 illustrates the experimental results obtained using the scheme of Yan et al. [26]. Figure 8 illustrates the experimental results obtained using our scheme. According to Figures 8 and 9, both the scheme of Yan et al. and our scheme output meaningful shadows based on image inpainting and decode the secret image losslessly. However, the differences between the scheme of Yan et al. and our scheme are as follows.

1) There are some artifacts or secret leakage on the shadow of Yan et al.'s scheme due to the sharing principle of linear congruence, while our scheme has no artifact due to the polynomial sharing principle.

2) When any $t < k$ shadows are collected, Yan et al.'s scheme exhibits secret leakage, while our scheme has no secret leakage because of its different sharing principles.

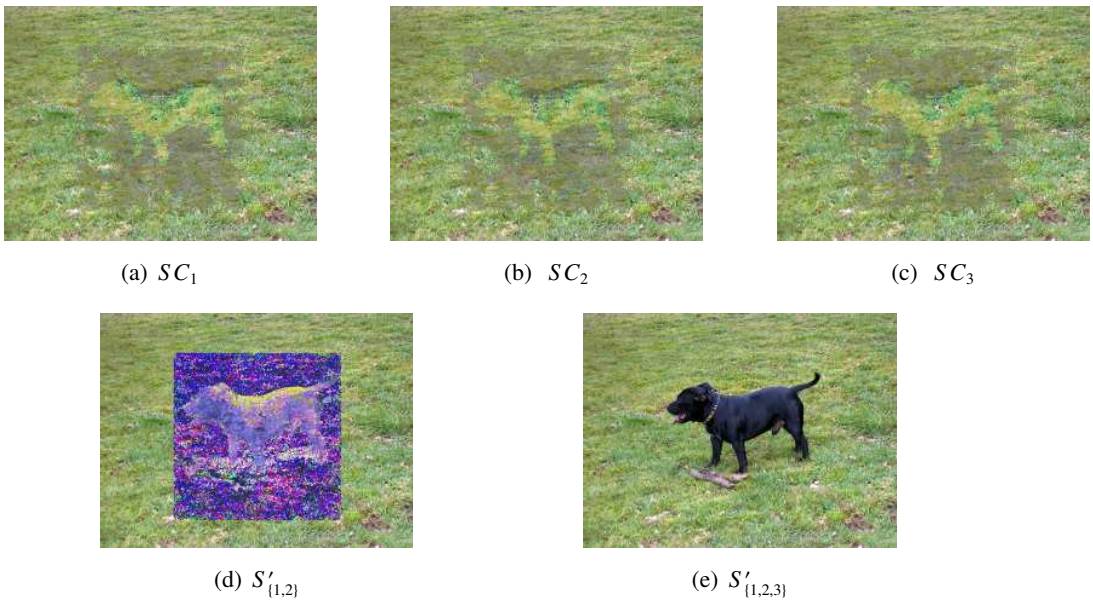
3) We can input three different cover images, while Yan et al.'s scheme inputs the same one, so our scheme is more convenient for managing the shadows than theirs.

4) Their secret can only be a part of the cover image, while in our scheme, the secret can be any input secret image; hence, our method is more general than theirs.

(a) SC_1 (b) SC_2 (c) SC_3

(d) $S'_{\{1,2\}}$ (e) $S'_{\{1,2,3\}}$

Figure 8. Experimental result of the realized BISS scheme for the threshold $(3, 3)$.

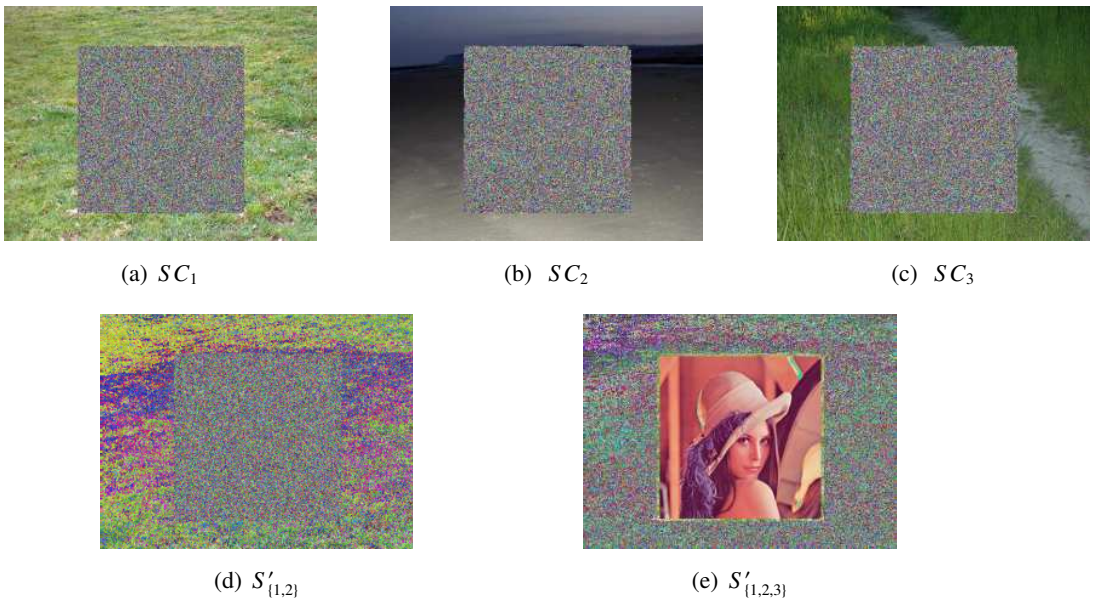


(a) SC_1 (b) SC_2 (c) SC_3

(d) $S'_{\{1,2\}}$ (e) $S'_{\{1,2,3\}}$

Figure 9. Experimental results of the scheme of Yan et al. [26] for the (k, n) threshold, where $k = 3, n = 3$.

The experimental results of the scheme of applying the traditional polynomial-based ISS method for the (k, n) threshold [9] are shown in Figure 10. According to Figures 8 and 10, the differences between the results are quite obvious. More importantly, our scheme can decode the secret image losslessly, while the scheme of Ding et al. is slightly lossy because 251 is adopted as the prime.



(a) SC_1 (b) SC_2 (c) SC_3

(d) $S'_{\{1,2\}}$ (e) $S'_{\{1,2,3\}}$

Figure 10. Experimental results of the scheme of applying the traditional polynomial-based ISS method for the (k, n) threshold [9], where $k = 3, n = 3$.

4.5. Extensions

The realized scheme may be extended to improve the performance of the realized scheme in the following way.

Cheating is a serious issue in related ISS schemes. In [28], an ISS scheme for a (k, n) threshold with a separate shadow authentication ability is proposed based on ISS itself rather than information hiding through applying visual secret sharing (VSS) to polynomial-based ISS by using a screening operation.

We may apply the idea to the presented algorithm to deal with the cheating issue at the price of reducing image quality. More specifically, in step 9 of the realized scheme, in order to achieve separate shadow authentication, we may increase an additional condition, i.e., the most significant bit (MSB) of the value of each shadow pixel is equal to the corresponding bit of a binary authentication image; in other words, step 4 of the Algorithm 1 in [28] is added into step 9 of the realized scheme. We note that, since more conditions should be satisfied in this way, the shadow quality will be reduced.

5. Conclusion

This paper considered a method for outputting meaningful ISS by image secret sharing (ISS) rather than information hiding. An image inpainting-based behavior ISS (BISS) scheme for the (k, n) threshold is realized. Experiments confirm the efficiency of the scheme. The PSNR of the shadow is close to 20, achieving acceptable shadow image quality. Comparisons with related schemes

show the advantages of the realized scheme. Our future work will focus on applying follow-up improved image inpainting methods, improving the image quality, cheating prevention and realizing secret image recovery in the case of lossy shadows.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Numbers: 61602491, 61501148) and the Key Program of the National University of Defense Technology (Grant Number: ZK-17-02-07).

Conflict of Interest

We have no conflicts of interest to declare.

References

1. X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, H. Liu, Exploiting the homomorphic property of visual cryptography, *Int. J. Digital Crime Forensics*, **9** (2017), 45–56.
2. A. Belazi, A. A. A. El-Latif, A simple yet efficient s-box method based on chaotic sine map, *Optik*, **130** (2017), 1438–1444.
3. Y. Cheng, Z. Fu, B. Yu, Improved visual secret sharing scheme for qr code applications, *IEEE Trans. Inf. Forensics Secur.*, **13** (2018), 2393–2403.
4. G. Wang, F. Liu, W. Q. Yan, Basic visual cryptography using braille, *Int. J. Digital Crime Forensics*, **8** (2016), 85–93.
5. M. Naor, A. Shamir, *Visual cryptography*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Springer, Perugia, Italy, 1995, 1–12.
6. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.
7. X. Yan, L. Liu, Y. Lu, Q. Gong, Security analysis and classification of image secret sharing, *J. Inf. Secur. Appl.*, **47** (2019), 208 – 216,
8. X. Yan, J. Li, Y. Lu, L. Liu, G. Yang, H. Chen, *Relations between secret sharing and secret image sharing*, Security with Intelligent Computing and Big-data Services Springer International Publishing, Cham, 2020, 79–93.
9. W. Ding, K. Liu, X. Yan, H. Wang, L. Liu, Q. Gong, An image secret sharing method based on matrix theory, *Symmetry*, **10** (2018), 530.
10. Z. Zhou, G. R. Arce, G. Di Crescenzo, Halftone visual cryptography, *IEEE Trans. Image Process.*, **15** (2006), 2441–2453.
11. Z. Wang, G. R. Arce, G. Di Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Secur.*, **4** (2009), 383–396.
12. F. Liu, C. Wu, Embedded extended visual cryptography schemes, *IEEE Trans. Inf. Forensics Secur.*, **6** (2011), 307–322.

13. J. Weir, W. Yan, *A comprehensive study of visual cryptography*, Transactions on Data Hiding and Multimedia Security V, Springer, Berlin, Heidelberg, 2010, 70–105.
14. X. Yan, Y. Lu, L. Liu, General meaningful shadow construction in secret image sharing, *IEEE Access*, **6** (2018), 45246–45255.
15. T. Guo, J. Jiao, F. Liu, W. Wang, On the pixel expansion of visual cryptography scheme, *Int. J. Digital Crime Forensics*, **9** (2017), 38–44.
16. X. Yan, X. Liu, C. N. Yang, An enhanced threshold visual secret sharing based on random grids, *J. Real-Time Image Process.*, **14** (2018), 61–73.
17. X. Yan, S. Wang, X. Niu, C. N. Yang, Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality, *Digital Signal Process.*, **38** (2015), 53–65.
18. C. C. Thien, J. C. Lin, Secret image sharing, *Comput. Graphics*, **26** (2002), 765–770.
19. C. N. Yang, C. B. Ciou, Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability, *Image Vision Comput.*, **28** (2010), 1600–1610.
20. L. Bao, S. Yi, Y. Zhou, Combination of sharing matrix and image encryption for lossless (k, n) -secret image sharing, *IEEE Trans. Image Process.*, **26** (2017), 5618–5631.
21. Y. Liu, C. Yang, Y. Wang, L. Zhu, W. Ji, Cheating identifiable secret sharing scheme using symmetric bivariate polynomial, *Inf. Sci.*, **453** (2018), 21–29.
22. P. Li, P. J. Ma, X. H. Su and C. N. Yang, Improvements of a two-in-one image secret sharing scheme based on gray mixing model, *J. Visual Communi. Image Representation*, **23** (2012), 441–453.
23. P. Li, C. 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.
24. A. Criminisi, P. Perez, K. Toyama, Region filling and object removal by exemplar-based image inpainting, *IEEE Trans. Image Process.*, **13** (2004), 1200–1212.
25. W. Shen, X. Song, X. Niu, Hiding traces of image inpainting, *Res. J. Appl. Sci. Eng. Technol.*, **4** (2012), 4962–4968.
26. X. Yan, Y. Lu, L. Liu, S. Wang, Partial secret image sharing for (k,n) threshold based on image inpainting, *J. Visual Commun. Image Representation*, **50** (2018), 135–144,
27. Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: From error visibility to structural similarity, *IEEE Trans. Image Process.*, **13** (2004), 600–612.
28. X. Yan, Q. Gong, L. Li, G. Yang, Y. Lu, J. Liu, Secret image sharing with separate shadow authentication ability, *Signal Process. Image Commun.*, **82** (2020), 115721.

AIMS Press