Multimed Tools Appl (2016) 75:3517–3536
DOI 10.1007/s11042-015-2462-3

Meaningful (2, $infinity$) secret image sharing scheme based on flipping operations

Duanhao Ou · Wei Sun

Received: 8 July 2014 / Revised: 22 December 2014 / Accepted: 12 January 2015 /
Published online: 28 January 2015

Abstract In this paper, a new method to construct a secret image sharing (SIS) scheme is proposed, where a secret image is shared into several shares by a perfect secure way without any knowledge of cryptography. A basic algorithm implemented by flipping operations with probability for constructing a meaningful (2, 2) SIS scheme is first proposed. Neither codebook tailor-made requirement nor pixel expansion is required in the proposed scheme. Additionally, the meaningful shares by the proposed scheme can be directly generated without any extra data hiding process. During the decrypting procedure, the secret image is visually revealed by performing XOR operations on two meaningful shares. In the following stage, a meaningful (2, $infinity$) SIS scheme is extended underlying the basic algorithm, where the number of shares can be extended anytime. Further, no matter how large the number of the extended shares is, the visual qualities of both the meaningful share and revealed secret image remain unchanged. Finally, sufficient number of formal proofs are provided to validate the correctness of the proposed schemes, whose superiority is also demonstrated by the experimental results.

Keywords Secret image sharing · XOR operation · Flipping operation · Meaningful shares · (2, *infinity*)

D. Ou (✉)
School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
e-mail: ouduanhao@163.com; ouduanh@mail2.sysu.edu.cn

W. Sun (✉)
School of Software, Sun Yat-sen University, Guangzhou 510006, China
e-mail: sunwei@mail.sysu.edu.cn

W. Sun
State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China

1 Introduction

The rapid increase in Internet usage and the continuing improvements in multimedia technologies are responsible for the increasing popularity of network-based digital images transmission. However, transmitting the important images, such as those used by the military or by commercial businesses, over the public network makes them vulnerable to be attacked. The research toward image security for protecting important image had thus been investigated. In general, the traditional image security methods can be classified into two main categories: (1) image encryption methods for secret image protection, and (2) image authentication methods for image integrity protection. An image encryption method, such as the image encryption based on gyrator transform [14], fractional Mellin transform [33] or compressive sensing [19], mainly involves the random phase and a secret key. By this method, a secret image can be processed to generate the encrypted image which is non-recognizable in appearance. Only the legal receiver with the corrected key can decrypt and access the secret image. On the other hand, for the aim of protecting the image integrity, image authentication methods were studied. By these methods, the authentication information of the protected image, such as digital signature [1] or digital watermark [32], is generated and used to detect the tempered areas. However, one common defect of the above-mentioned methods is their policy of centralized storage, in which an entire protected image is accommodated in a single information carrier. If a hacker detects an abnormality in the information carrier in which the protected image resides, she/he may intercept it or simple ruing the entire information carrier. Once the information carrier is destroyed, the protected image is also lost forever. Secret image sharing (SIS) is another image security method which does not suffer from these problems. The SIS scheme is constructed by applying the secret sharing concept, which was introduced independently by Blakley [3] and Shamir [22], on digital images. The SIS scheme is with higher tolerance against data corruption or loss than other image-protection mechanisms, such as image encryption or image steganography. In 1995, Naor and Shamir [20] construct a SIS scheme, called visual cryptography (VC), which involves the notions of perfect cipher and human visual system. In a (k, n) VC scheme, a secret image is encoded into n random-liked images, called shares or shadows. In such a way, the secret image can be visually revealed by stacking any k shares, whereas any $k-1$ or less shares give no clue about the secret. Unlike traditional cryptographic methods such as data encryption standard (DES) scheme and advanced encryption standard (AES) scheme, VC provides fast decryption without any complex computation. Additionally, if the random-liked share includes truly random pixels, VC is regarded unconditional secure and provides unbreakable encryption. However, meaningless appearance of the random-liked shares may impose difficulty for managing the shares. An initial model of VC was implemented by Naor and Shamir [20] in 1995. Based on the pioneer work of Naor and Shamir, many issues on VC have been extensively studied, such as providing meaningful shares [2, 16], improving the contrast [4, 11] and reconstructing black secret pixels perfectly [5, 13]. Despite lots of wonderful results on the above-mentioned VC schemes, some drawbacks still remain as follows:

- Pixel expansion. The size of each share is $m \geq 2$ times as big as that of the secret image. Generally, the variable m is referred to as the pixel expansion factor, which is desired to be as small as possible. The pixel expansion would cause a problem of burdening with the data storage.
- Codebook required. The Naor-Shamir VC schemes always require a codebook to support encoding a secret image, where the codebook is difficult to be designed. For a

(k, n) VC scheme, designing the codebooks for different parameters k or n is not trivial.

– Poor visual quality. Due to the stacking decryption, the visual quality of revealed secret image by VC schemes is usually poor. Moreover, when stacking more shares, the visual quality of the revealed secret image becomes terrible.

To overcome the problems of pixel expansion and codebook required, random grid-based VC schemes (RGVCS) [12, 23, 24] were introduced, where the shares with invariant size can be generated. The initial model of RGVCS was implemented by Kafri and Keren [12]. The size of each share generated by Kafri and Keren is the same as that of the original secret image, which implies no pixel expansion is achieved. Inspired by Kafri and Keren, follow-up researches on RGVCS were further studied, such as investigating different access structure schemes [7, 8, 28], improving visual quality [27, 30] and offering meaningful shares [9, 10]. Unfortunately, due to the stacking decryption, the contrast of the revealed secret image achieves at most $1/2$ in RGVCS. Such low image quality further limits the applications. To address this problem, another secret image sharing (SIS) schemes [17, 18, 25, 26] were investigated, where a secret image is decrypted by XOR operation instead of stacking operation. In such a decryption way, the visual quality of revealed secret image can be further improved and the alignment problem is solved as well. In [25], Tuyls et al. gave some valid constructions for the XOR-based SIS scheme, but the tailor-made codebooks are required. Moveover, their generated shares are meaningless which are hard to identify and may impose difficulty for managing the shares. Liu et al. [18] presented an optimal XOR-based VC scheme for improving the contrast, but the drawbacks such as meaningless share, codebook required and pixel expansion still remain in their scheme. To manage the shares efficiently, XOR-based SIS schemes with offering meaningful shares [21, 29] were investigated. However, the existing meaningful SIS schemes are devised only for (n, n) case, which may limit the applications.

Based on the above-mentioned problems, our work aims to propose a meaningful XOR-based SIS scheme for $(2, infinity)$ case. The definition of $(2, infinity)$ case is first introduced in [6], where the number of shares can be extended anytime. In this paper, the proposed XOR-based SIS scheme is implemented by performing flipping operations on the pre-selected cover images. First, a basic algorithm for constructing a meaningful $(2, 2)$ XOR-based SIS scheme is devised, where the meaningful shares can be directly generated without extra data hiding process. Subsequently, a meaningful $(2, infinity)$ XOR-based SIS scheme is extended underlying the basic algorithm. Further, no matter how large the number of the extended shares is, the visual qualities of both the meaningful shares and revealed secret image always maintain the same as those in the basic $(2, 2)$ algorithm. In general, the main contributions of the proposed SIS scheme are summarized as follows:

1. Neither codebook nor pixel expansion is needed.
2. Shares with meaningful contents are achieved, which makes shares management efficient.
3. Unlike some existing meaningful schemes [9, 10], our scheme can generate meaningful shares without extra data hiding process, which may reduce the computation time of the scheme.
4. Due to the XOR decryption, superior visual qualities of both the share and revealed secret image are achieved.
5. Black secret pixels can be reconstructed perfectly, so that the revealed secret image can be further identified by human visual system.

6. Sufficient number of formal proofs are provided to demonstrate the correctness of the proposed scheme.

The rest of this paper is organized as follows. Related works on secret image sharing are briefly introduced in Section 2. The proposed meaningful SIS schemes, including the basic $(2, 2)$ case and the extended $(2, \ infinity)$ case, are stated in Section 3. Experimental results and discussions are provided to demonstrate the feasibility of the proposed SIS scheme in Section 4, and finally some conclusions are made in Section 5.

2 Related works

In this paper, secret image sharing concept is applied for constructing the proposed SIS scheme. For offering a better comprehension of the proposed scheme, the secret image sharing concept is first introduced in the following. In a traditional (k, n) SIS scheme, a secret image is encoded into n random-liked images, called shares, each of which is then distributed to the related participant. A (k, n) SIS scheme is consider valid if it meets the security and contrast conditions. The security condition indicates that the knowledge of any $k-1$ or fewer shares gives no clue about the secret image, and the contrast condition implies that any k or more shares can reveal the secret image. In 1995, Naor and Shamir [20] first constructed a valid SIS scheme by using two collections of $n \times m$ Boolean matrices B_1 and B_0. Each pixel of the secret image is encoded into n pixels, each of which consists of m sub-pixels. To encode a black (resp.white) secret pixel, the dealer randomly selects one matrix from the Boolean matrices B_1 (resp.B_0), and assigns the row i of the selected matrix to the pixel of share SH_i. With stacking any k or more shares in a way which properly aligns the sub-pixels, the secret image can be disclosed by human visual system. However, no clue about the secret image can be gained if only $k-1$ or fewer shares are collected. An example for constructing a $(2, 2)$ Naor-Shamir's SIS scheme is shown in the following. Two collections of Boolean matrices used in the $(2, 2)$ SIS scheme are designed as bellow:

$$B_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\} \tag{1}$$

$$B_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \tag{2}$$

In the $(2, 2)$ SIS scheme, a secret pixel is encoded into two shared pixels, each of which includes two sub-pixels. Thus, its pixel expansion is 2. When encoding a secret pixel sp, a matrix MT is randomly selected from B_0 if sp is white, and from B_1 if sp is black. Simulation results are shown in Fig. 1 to demonstrate the feasibility of the $(2, 2)$ SIS scheme, where the image of Fig. 1a is taken as a secret image. Two shares generated by the $(2, 2)$ SIS scheme are illustrated in Fig. 1b-c. By observing Fig. 1b-c, it can be found that each generated share is a random-liked image which gives no clue about the secret. However, the stacked result by the two shares can visually reveal the secret image, as shown in Fig. 1d. Although the Naor-Shamir SIS schemes can provide an easy and fast decryption, some problems of poor visual quality, random-liked shares and pixels alignment still remain.

To achieve high visual quality, another XOR-based SIS scheme [25] is introduced, where the secret image is decrypted by XOR operation instead of stacking operation. In addition,

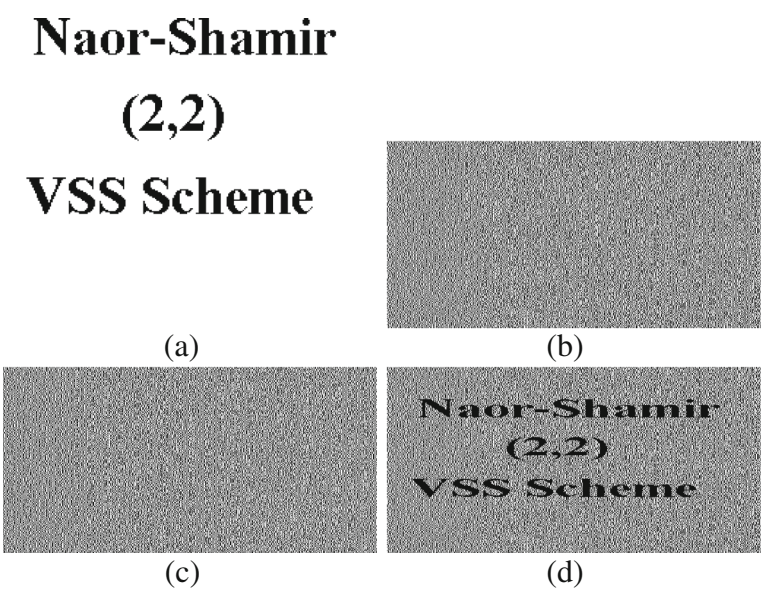


Fig. 1 Simulation results of the (2,2) Naor-Shamir SIS scheme which is constructed by using two collections of the Boolean matrices B_0 and B_1. **a** The secret image, **b** the share 1, **c** the share 2, **d** the stacked result by (c) and (d)

the XOR-based SIS scheme can solve the problem of pixels alignment as well. For handling more applications, a $(2,\ infinity)$ SIS schemes based on XOR decryption is extended. The definition of a $(2, infinity)$ scheme is first given in [6], where the number of shares can be extended anytime. No matter how large the number of the extended shares is, the $(2,\ infinity)$ SIS scheme always meets the security and contrast conditions. For example, when the number of shares is extended from 2 to N, where N denotes an any arbitrarily large positive integer. For the XOR-based $(2,\ infinity)$ SIS scheme, the security condition implies each of N shares gives no clue about the secret image, while the contrast condition indicates the XOR-ed result by any 2 of N shares can visually reveal the secret image. Note that, the decryption procedure of our $(2, N)$ SIS scheme is different from that of the traditional $(2, N)$ SIS scheme. When the share number $k > 2$, all the k shares are generally utilized to decrypt the secret image in the traditional $(2, N)$ SIS scheme. However, in our $(2, N)$ SIS scheme, we just utilize any 2 of these k shares to decrypt the secret image.

In this paper, two logical operations, the NOT operation ("$\overline{(\cdot)}$") and the XOR operation ("$\oplus$"), are needed to construct the proposed SIS schemes. The logical NOT operation is equivalent to the flipping operation which is utilized to share the secret image, and the logical XOR operation is used to decrypt the secret image from the shares. The truth-table of XOR and NOT logical operations for binary scalar inputs is given in Table 1. For binary scalar inputs, the XOR or NOT operation is carried out bit by bit. For binary matrix inputs, the XOR operation of two $H \times W$ matrices, A and B, is defined element-wise. That is, $A \oplus B = [A_{i,j} \oplus B_{i,j}]$, where $i = 1, 2, \cdots, H$, $j = 1, 2, \cdots, W$. Other notations used in this paper are illustrated as follows: digits 1 and 0 are referred to as the white and black pixels, respectively; $R_{\{\oplus,1,2\}}$ denotes the XOR-ed result by shares $\{R_1, R_2\}$, such that $R_{\{\oplus,1,2\}} = R_1 \oplus R_2$.

Table 1 The truth-table of XOR and NOT logical operations for binary scalar inputs

a	b	$a \oplus b$	$\overline{a}$	$\overline{b}$
0	0	0	1	1
0	1	1	1	0
1	0	1	0	1
1	1	0	0	0

In the following, some definitions are given for the further analysis on the proposed SIS schemes.

Definition 1 (Average light transmission [23, 29]). For a certain pixel p in a binary image I with sized $H \times W$, the probability of pixel p being white, denoted by $Prob(p = 1)$, represents the light transmission of pixel p, denoted by $T(p)$, such that $T(p) = Prob(p = 1)$. When p is a white pixel, the light transmission of p is $T(p) = 1$. Whereas, when p is a black pixel, the light transmission of p is $T(p) = 0$. Totally, the average light transmission of image I is defined as

$$T(I) = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} T(I_{i,j})}{H \times W}. \tag{3}$$

Definition 2 (Area representation [23, 29]). Let $A(1)$ (resp. $A(0)$) be the area of all the white (resp. black) pixels in image A where $A = A(1) \cup A(0)$ and $A(1) \cap A(0) = \emptyset$. Therefore, $B[A(1)]$ (resp. $B[A(0)]$) is the corresponding area of all the white (resp. black) pixels in image B.

Definition 3 (Contrast of the XOR-ed result). Given an original secret image S, and any two of n corresponding shares generated by our schemes, denoted by R_i and R_j. To evaluate the visual quality of the XOR-ed result by the two shares R_i and R_j, such that $R_{\{\oplus,i,j\}} = R_i \oplus R_j$, the contrast of the XOR-ed result with respect to the original secret image S is defined as

$$\alpha_{xor} = \frac{T(R_{\{\oplus,i,j\}}[S(1)]) - T(R_{\{\oplus,i,j\}}[S(0)])}{1 + T(R_{\{\oplus,i,j\}}[S(0)])},$$

Remark 1 The contrast is widely accepted to evaluate the visual quality of the revealed binary image. Since secret image in the revealed result would be better identified by human visual system with larger contrast, the contrast is expected to be as large as possible. As documented in [7], if the contrast is bigger than zero, the revealed result can disclose the contents of the secret image, that is called the contrast condition. Especially, when $T(R_{\{\oplus,i,j\}}[S(0)]) = 0$, all the revealed pixels associated to the black secret pixels are definitely black. By the same way, the contrast of the share is as given as Definition 4.

Definition 4 (Contrast of the share). Given an original cover image C, and the corresponding share R_i generated by our schemes. The contrast of the share R_i with respect to the original cover image C is

$$\alpha_{share} = \frac{T(R_i[C(1)]) - T(R_i[C(0)])}{1 + T(R_i[C(0)])}$$

Remark 2 Similarly, the share R_i resembles the cover image C if the contrast of the share meets $\alpha_{share} > 0$, that is called the meaningful condition. On the other hand, if the contrast of the share meets $\alpha_{share} = 0$, such that $T(R_i[C(1)]) = T(R_i[C(0)])$, which implies the share R_i is meaningless and hard to be identified. Generally, the security, contrast and meaningfulness conditions should be met at the same time for a meaningful SIS scheme.

3 The proposed meaningful SIS schemes

To address the problems of poor visual quality and pixels alignment, the SIS schemes constructed by flipping operations are proposed. In addition, to make the shares managements efficient, the proposed SIS schemes can generate meaningful shares without any extra data hiding process. A basic algorithm for constructing a meaningful $(2, 2)$ SIS scheme is first proposed, where a secret image is shared into two meaningful shares by flipping operations with probability. During the decrypting procedure, the secret image can be visually revealed by performing XOR operations on two meaningful shares. Subsequently, a meaningful $(2, infinity)$ SIS scheme is extended underlying the basic algorithm. Meanwhile, sufficient number of formal proofs are also provided to validate the correctness of the proposed schemes.

3.1 The basic $(2, 2)$ SIS scheme

The basic algorithm for constructing a meaningful $(2, 2)$ SIS scheme is formally illustrated as in Algorithm 1.

Algorithm 1 (The basic $(2, 2)$ SIS scheme)

Input: A binary secret image S and a cover image C, both with $H \times W$ pixels, and a probability parameter β $(0 < \beta < \frac{1}{2})$.

Output: two shares R_1 and R_2, each of which is $H \times W$ in size.

1: Firstly, two images R_1 and R_2 are initially set to the cover image C, such that

$$R_1 = C, R_2 = C.$$

Subsequently, the secret image S would be encoded by performing flipping operations on these two images, as described as in the following steps.

2: For each position (i, j) in the secret image S, different flipping strategies are employed on the two corresponding pixels $R_1(i, j), R_2(i, j)$ according to the value of $S(i, j)$.

3: If $S(i, j) = 0$, two pixels $R_1(i, j)$ and $R_2(i, j)$ are together to be flipped with probability β.

4: If $S(i, j) = 1$, each of two pixels $R_1(i, j)$ and $R_2(i, j)$ would be flipped with probability β independently.

5: Repeat Steps $2 - 4$ until all the secret pixels are processed, and output two shares R_1 and R_2, each of which has the same image size as the secret image.

Remark 3 Algorithm 1 is implemented by different flipping strategies, where neither codebook nor pixel expansion is needed. Especially, Algorithm 1 can directly generate meaningful shares without any extra data hiding process, which may reduce the computation time of the scheme. In the following, formal proofs are provided to demonstrate the correctness of Algorithm 1. As formulated by Theorem 1, Algorithm 1 can be proved to be a valid construction for a meaningful $(2, 2)$ SIS scheme. Meanwhile, the contrasts of the revealed secret image and meaningful shares are also analyzed in Theorems 2 and 3, respectively.

Lemma 1 *Given two shares R_1 and R_2 generated by Algorithm 1, each of which gives no clue about the secret image S: $T(R_k[S(0)]) = T(R_k[S(1)])$, where $k = 1, 2$.*

Proof As stated in Algorithm 1, each shared pixel $R_k(i, j)$ is obtained by flipping the related original pixel with the probability β no matter whether the secret pixel $S(i, j)$ is 1 or 0. By Definitions 1 and 2, we have $T(R_k[S(0)]) = T(R_k[S(1)])$ $(k = 1, 2)$. Therefore, every share R_k gives no clue about the secret image S. □

Lemma 2 *Given two shares R_1 and R_2 generated by Algorithm 1, each of which resembles the cover image C: $T(R_k[C(1)]) > T(R_k[C(0)])$, where $k = 1, 2$.*

Proof Since each shared pixel $R_k(i, j)$ is generated by flipping the original cover pixel $C(i, j)$ with probability β, we have

$$Prob(R_k(i, j) = 1|C(i, j) = 1) = 1 - \beta,$$

$$Prob(R_k(i, j) = 1|C(i, j) = 0) = \beta.$$

By Definitions 1 and 2, we obtain $T(R_k[C(1)]) = 1 - \beta$ and $T(R_k[C(0)]) = \beta$. Therefore, $T(R_k[C(1)]) - T(R_k[C(0)]) = 1 - 2\beta$. Since $0 < \beta < \frac{1}{2}$, we have $T(R_k[C(1)]) - T(R_k[C(0)]) > 0$. As a result, $T(R_k[C(1)]) > T(R_k[C(0)])$. Therefore, each share R_k can resemble the cover image C. □

Lemma 3 *Given two shares R_1 and R_2 generated by Algorithm 1, the XOR-ed result by the two shares $R_{\{\oplus,1,2\}} = R_1 \oplus R_2$ visually reveals the secret image S: $T(R_{\{\oplus,1,2\}}[S(1)]) > T(R_{\{\oplus,1,2\}}[S(0)])$, but carries no information about the cover image C: $T(R_{\{\oplus,1,2\}}[C(1)]) = T(R_{\{\oplus,1,2\}}[C(0)])$.*

Proof As stated in Algorithm 1, when $S(i, j)$ is 0, both the two cover pixels are together flipped with probability β. It is observed that the two generated shared pixels $R_1(i, j)$ and $R_2(i, j)$ are always the same no matter the flipping operations are performed or not, hence the XOR-ed result by the two shared pixels are equal to zero. Thus, we have $Prob(R_1(i, j) \oplus R_2(i, j) = 1|S(i, j) = 0) = 0$. By Definitions 1 and 2, we get $T(R_{\{(\oplus,1,2\}}[S(0)]) = 0$. When $S(i, j)$ is 1, the shared pixels $R_1(i, j)$ and $R_2(i, j)$ are individually generated by flipping the corresponding pixel $C(i, j)$ with the probability β; thus, we have

$$Prob(R_1(i, j) \oplus R_2(i, j) = 1|S(i, j) = 1) = 2\beta(1 - \beta).$$

By Definitions 1 and 2, we get $T(R_{\{(\oplus,1,2\}}[S(1)]) = 2\beta(1-\beta)$. Hence, $T(R_{\{(\oplus,1,2\}}[S(1)]) - T(R_{\{(\oplus,1,2\}}[S(0)]) = 2\beta(1 - \beta)$. Since $0 < \beta < \frac{1}{2}$, we have $2\beta(1 - \beta) > 0$. As a result, $T(R_{\{\oplus,1,2\}}[S(1)]) > T(R_{\{\oplus,1,2\}}[S(0)])$. Therefore, the XOR-ed result $R_{\{\oplus,1,2\}}$ visually reveals the secret image S.

On the other hand, we know that the shared pixels $R_1(i, j)$ and $R_2(i, j)$ are generated by flipping the corresponding cover image pixel with probability β. Since

$$Prob(R_1(i, j) \oplus R_2(i, j) = 1|C(i, j) = 1) = 2\beta(1 - \beta)$$

and

$$Prob(R_1(i, j) \oplus R_2(i, j) = 1|C(i, j) = 0) = 2\beta(1 - \beta),$$

we get

$$Prob(R_{\{\oplus,1,2\}} = 1|C(i, j) = 1) = Prob(R_{\{\oplus,1,2\}} = 1|C(i, j) = 0).$$

By Definitions 1 and 2, we get $T(R_{\{\oplus,1,2\}}[C(1)]) = T(R_{\{\oplus,1,2\}}[C(0)])$. As a result, the XOR-ed result $R_{\{\oplus,1,2\}}$ gives no information about the cover image S. □

Theorem 1 *Algorithm 1 is a valid construction of a meaningful* $(2, 2)$ *SIS scheme. It meets the following conditions:*

- *(Security condition) Every share* R_k *gives no clue about the secret image* S*:* $T(R_k[S(0)]) = T(R_k[S(1)])$*, where* $k = 1, 2$.
- *(Meaningfulness condition) Every share* R_k *looks like the cover image* C*:* $T(R_k[C(1)]) > T(R_k[C(0)])$*, where* $k = 1, 2$.
- *(Contrast condition) The XOR-ed result by the two shares* $R_{\{\oplus,1,2\}} = R_1 \oplus R_2$ *visually reveals the secret image* S*:* $T(R_{\{\oplus,1,2\}}[S(1)]) > T(R_{\{\oplus,1,2\}}[S(0)])$*, but gives no information about the cover image* C*:* $T(R_{\{\oplus,1,2\}}[C(1)]) = T(R_{\{\oplus,1,2\}}[C(0)])$.

Proof According to Lemmas 1, 2 and 3, the three conditions are satisfied. Therefore, Algorithm 1 is a valid construction of a meaningful $(2, 2)$ SIS scheme. □

Theorem 2 *Given two shares* R_1 *and* R_2 *generated by Algorithm 1, the contrast of the XOR-ed result by two shares is* $2\beta(1-\beta)$*, and the reconstruction of black secret pixels is perfect:* $T(R_{\{\oplus,1,2\}}[S(0)]) = 0$.

Proof From the proof of Lemma 3, we have $T(R_{\{\oplus,1,2\}}[S(0)]) = 0$ and $T(R_{\{\oplus,1,2\}}[S(1)]) = 2\beta(1-\beta)$. The formula $T(R_{\{\oplus,1,2\}}[S(0)]) = 0$ implies the reconstruction of black secret pixels is perfect. According to Definition 3, the contrast of the XOR-ed result is calculated by

$$\begin{aligned}\alpha_{xor} &= \frac{T(R_{\{\oplus,1,2\}}[S(1)]) - T(R_{\{\oplus,1,2\}}[S(0)])}{1 + T(R_{\{\oplus,1,2\}}[S(0)])} \\ &= [2\beta(1-\beta) - 0] / [1 + 0] \\ &= 2\beta(1-\beta).\end{aligned}$$

□

Theorem 3 *The contrast of the meaningful share* R_k $(k = 1, 2)$ *generated by Algorithm 1 is* $\frac{1-2\beta}{1+\beta}$.

Proof From the proof of Lemma 2, we have $T(R_k[C(1)]) = 1-\beta$ and $T(R_k[C(0)]) = \beta$. According to Definition 4, the contrast of the share R_k is calculated by

$$\begin{aligned}\alpha_{share} &= \frac{T(R_k[C(1)]) - T(R_k[C(0)])}{1 + T(R_k[C(0)])} \\ &= [1 - \beta - \beta] / [1 + \beta] \\ &= \frac{1-2\beta}{1+\beta}.\end{aligned}$$

□

Remark 4 It is convenient to see that as β increases from 0 to $1/2$, α_{xor} goes up but α_{share} goes down. With the adjustable parameters, the application of the proposed SIS schemes becomes flexible. The tradeoff among the visual quality of the revealed secret image and meaningful shares can vary from the application to application by setting different parameters.

3.2 The extended (2, $infinity$) SIS scheme

In this section, a meaningful (2, $infinity$) SIS scheme is extended underlying the basic (2, 2) SIS scheme. The extended (2, $infinity$) scheme inherits all the advantages of the basic (2, 2) SIS scheme, such as no codebook required, no pixel expansion, meaningful shares and superior visual quality. Additionally, the extended (2, $infinity$) scheme obtains some new properties: (1) the shares generated by the basic (2, 2) SIS scheme could be re-used in the extended (2, $infinity$) SIS scheme, (2) the visual qualities of both the new share and revealed secret image maintain exactly the same as those in the basic (2, 2) SIS scheme no matter how large the number of the extended shares is.

As stated in the basic (2, 2) SIS scheme, every pixel of the original cover image is flipped with probability β no matter the corresponding secret pixel is white or black, so that the generated share gives no clue about the secret image. In the following, underlying the basic (2, 2) SIS scheme, we construct new shares to extend the number of shares, where every pixel of the new share is also generated by flipping the cover image pixel with probability β. The extended (*2,infinity*) SIS scheme is formally illustrated as in Algorithm 2.

Algorithm 2 (The extended $(2, infinity)$ SIS scheme)

Input: A binary secret image S and a cover image C used in Algorithm 1, a meaningful share R generated by Algorithm 1 with parameter β, and the number N of new shares, all the input images are $H \times W$ in size.

Output: N new shares $R_1^{new}, \cdots, R_N^{new}$, each of which is with $H \times W$ pixels.

1: For each position (i, j) in the secret image S, Step 2 or 3 is carried out according to the value of $S(i, j)$.

2: If $S(i, j) = 0$, the N new shared pixels in the position (i, j) are constructed by

$$R_1^{new}(i, j) = R(i, j), \cdots, R_N^{new}(i, j) = R(i, j).$$

3: If $S(i, j) = 1$, the N new shared pixels in the position (i, j) are first set to $C(i, j)$, such that

$$R_1^{new}(i, j) = C(i, j), \cdots, R_N^{new}(i, j) = C(i, j).$$

Then, the flipping operations are individually performed on these N pixels with probability β.

4: When all the secret pixels are completely processed, the N new meaningful shares $R_1^{new}, \cdots, R_N^{new}$ can be achieved. Each generated share has the same image size as the secret image.

Similarly, sufficient number of formal proofs are provided to demonstrate the correctness of Algorithm 2. As formulated by Theorem 4, Algorithm 2 can be proved to be a valid construction for a meaningful (2, $infinity$) SIS scheme.

Theorem 4 *Let R_1 and R_2 be the two shares generated by Algorithm 1 with a parameter β ($0 < \beta < \frac{1}{2}$), and $R_1^{new}, \cdots, R_N^{new}$ be the N new shares generated by Algorithm 2, where N denotes an any arbitrarily large positive integer. Algorithm 2 is a valid construction for a meaningful (2, $infinity$) SIS scheme. It should meet the following conditions:*

- *Each of shares $\{R_1, R_2, R_1^{new}, \cdots, R_N^{new}\}$ gives no clue about the secret image S.*
- *Each of shares $\{R_1, R_2, R_1^{new}, \cdots, R_N^{new}\}$ is a meaningful image which can resemble the cover image C.*
- *The XOR-ed result by any two of shares $\{R_1, R_2, R_1^{new}, \cdots, R_N^{new}\}$ visually reveals the secret image S, but carries no information about the cover image C.*

Proof Since the shares R_1 and R_2 are generated by Algorithm 1, it is convenient to see each of these two shares gives no clue about the secret image by the security condition of Theorem 1. As we known, the input share R for Algorithm 2 is generated by Algorithm 1, that is $R \in \{R_1, R_2\}$. As stated in Algorithm 1, every pixel of the share R is generated by performing flipping operation on the corresponding cover image pixel with probability β, which can be denoted by $Prob(R(i, j) = \overline{C(i, j)}) = \beta$.

For each new share R_k^{new} $(k = 1, \cdots, N)$, when $S(i, j) = 0$, the corresponding shared pixel $R_k^{new}(i, j) = R(i, j)$; thus, we have

$$Prob(R_k^{new}(i, j) = \overline{C(i, j)} | S(i, j) = 0) = Prob(R(i, j) = \overline{C(i, j)}) = \beta.$$

On the other hand, when $S(i, j) = 1$, as stated in Step 3 of Algorithm 2, it is clearly obtained

$$Prob(R_k^{new}(i, j) = \overline{C(i, j)} | S(i, j) = 1) = \beta.$$

Therefore, no matter whether the secret pixel $S(i, j)$ is 0 or 1, the probability of performing flipping operation on pixel $C(i, j)$ is always equal to β. As a result, for all shares $\{R_1, R_2, R_1^{new}, \cdots, R_N^{new}\}$, each of them gives no clue about the secret image S.

As formulated by Lemma 2, the shares R_1 and R_2 generated by Algorithm 1 are meaningful. By Theorem 3, the contrast of the share R_k $(k = 1, 2)$ is obtained by computing

$$\alpha_{share} = \frac{1 - 2\beta}{1 + \beta}.$$

Since $0 < \beta < \frac{1}{2}$, we have $\alpha_{share} > 0$. On the other hand, for each new share R_k^{new} $(k = 1, \cdots, N)$, since every pixel $R_k^{new}(i, j)$ is generated by flipping the corresponding cover image pixel $C(i, j)$ with probability β, we have

$$Prob(R_k^{new}(i, j) = 1 | C(i, j) = 1) = 1 - \beta$$

and

$$Prob(R_k^{new}(i, j) = 1 | C(i, j) = 0) = \beta.$$

By Definition 4, the contrast of the new share can be calculated as

$$\alpha_{share}^{new} = \frac{1 - \beta - \beta}{1 + \beta} = \frac{1 - 2\beta}{1 + \beta}.$$

It is clearly seen that $\alpha_{share}^{new} = \alpha_{share} > 0$. Hence, for all shares $\{R_1, R_2, R_1^{new}, \cdots, R_N^{new}\}$, each of them is a meaningful image which resembles the cover image C. Additionally, it can be concluded that all shares have the same contrast $\frac{1-2\beta}{1+\beta}$.

Let R_{x_1} and R_{x_2} be any two shares from $\{R_1, \cdots, R_n, R_1^{new}, \cdots, R_N^{new}\}$. As stated in Algorithms 1 and 2, when $S(i, j) = 0$, the shared pixels $R_{x_1}(i, j)$ and $R_{x_2}(i, j)$ are always the same; thus, we have $Prob(R_{\{\oplus, x_1, x_2\}}(i, j) = 1 | S(i, j) = 0) = 0$. When $S(i, j) = 1$, the shared pixels $R_{x_1}(i, j)$ and $R_{x_2}(i, j)$ are individually generated by flipping the corresponding image pixel $C(i, j)$ with the probability β; thus, we have

$$Prob(R_{\{\oplus, x_1, x_2\}}(i, j) = 1 | S(i, j) = 1) = 2\beta(1 - \beta).$$

By Definitions 1 and 2, we have $T(R_{\{\oplus, x_1, x_2\}}[S(0)]) = 0$ and $T(R_{\{\oplus, x_1, x_2\}}[S(1)]) = 2\beta(1 - \beta)$. According to Definition 3, the contrast of the XOR-ed result $R_{\{\oplus, x_1, x_2\}}$ can be calculated

$$[2\beta(1 - \beta) - 0] / [1 + 0] = 2\beta(1 - \beta).$$

Since $0 < \beta < \frac{1}{2}$, we have $2\beta(1 - \beta) > 0$. As a result, the XOR-ed result $R_{\{\oplus, x_1, x_2\}}$ can disclose the secret image by human visual system.

On the other hand, we know that the shares R_{x_1} and R_{x_2} are generated by flipping the cover image pixel with probability β. Since

$$Prob(R_{\{\oplus,x_1,x_2\}}(i,j) = 1 | C(i,j) = 1) = 2\beta(1-\beta)$$

and

$$Prob(R_{\{\oplus,x_1,x_2\}}(i,j) = 1 | C(i,j) = 0) = 2\beta(1-\beta),$$

we get

$$Prob(R_{\{\oplus,x_1,x_2\}}(i,j) = 1 | C(i,j) = 1) = Prob(R_{\{\oplus,x_1,x_2\}}(i,j) = 1 | C(i,j) = 0).$$

By Definitions 1 and 2, we have $T(R_{\{\oplus,x_1,x_2\}}[C(1)]) = T(R_{\{\oplus,x_1,x_2\}}[C(0)])$. Hence, the XOR-ed result $R_{\{\oplus,x_1,x_2\}}$ does not give any information about the cover image C. □

Remark 5 From the proof of Theorem 4, the contrast of the new share is $\frac{1-2\beta}{1+\beta}$, which is the same as the contrast of the share generated by the basic (2, 2) SIS scheme. Meanwhile, the contrast of the XOR-ed result by the extended $(2, \ infinity)$ SIS scheme is $2\beta(1-\beta)$ which dose not depend on the extended number N. It implies that when the parameters β is set, the contrasts of the shares and the revealed secret image are fixed to some value no matter how large the number of new shares is. Further, the reconstruction of black secret pixels by the proposed schemes is perfect, which makes the secret image well identified by human visual system.

4 Experimental results and discussions

4.1 Feasibility

In this section, several experiments were conducted to demonstrate the feasibility of the proposed schemes. The first experiment is a (2, 2) SIS scheme constructed by Algorithm 1 with parameter β being 0.2, where all the test images are 512×512 in size. Simulation results of the first experiment are illustrated in Fig. 2, where Fig. 2a and b respectively show the secret image and the cover image used in the experiment. As shown in Fig. 2c-d, the generated shares are meaningful images which resemble the cover image. The XOR-ed result by two shares (c) and (d) visually reveals the secret image but carries no information about the cover image, as illustrated as in Fig. 2e. It is observed that the reconstruction of black secret pixels is perfect, which is helpful to further identify the secret image in the XOR-ed result by the naked eyes.

The second experiment conducted by the extended $(2, \ infinity)$ SIS scheme is illustrated in Fig. 3, where the (2, 2) case of Fig. 2 is extended to a (2, 3) case by Algorithm 2. The three meaningful shares of the (2, 3) case are shown in Fig. 3a-c, where shares of Fig. 3a-b directly utilize the two shares generated from the (2, 2) case of Fig. 2, and the new meaningful share of Fig. 3c is generated by Algorithm 2. The XOR-ed results by any two of these three shares are illustrated in Fig. 3d-f, where the secret image is visually revealed. Note that, all the revealed pixels associated to the black secret pixels are always black, that implies the reconstruction of black pixels is perfect.

To further demonstrate the feasibility of the extended $(2, \ infinity)$ SIS scheme, another experiment for a (2, 10) case is conducted by Algorithm 2 with a bigger number N being 8, where the (2, 2) case of Fig. 2 is extended to a (2, 10) case. Five of ten meaningful shares are shown in Fig. 4a-e, where Fig. 4a-b directly re-use the two shares of the (2, 2) case and Fig. 4c-e are the three of eight new shares generated by Algorithm 2. It can be observed

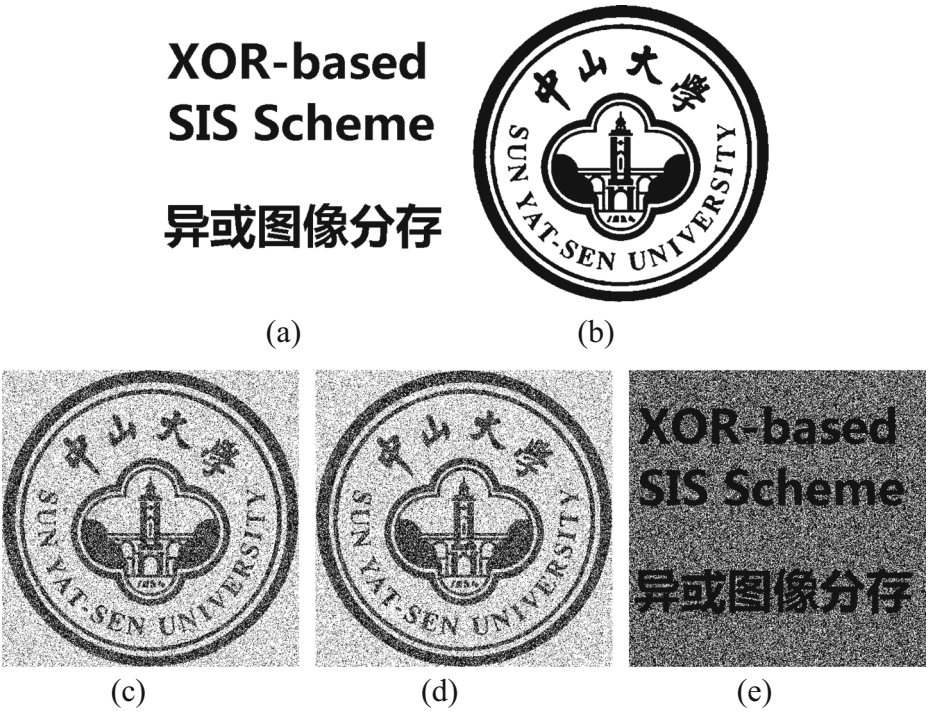


Fig. 2 Experimental results of the basic $(2, 2)$ SIS scheme with $\beta = 0.2$, where all the test images are 512×512 in size. **a** The secret image, **b** the cover image, **c** share R_1, **d** share R_2, **e** $R_1 \oplus R_2$

that the XOR-ed result by any two meaningful shares of Fig. 4a-e visually reveals the secret image with perfect reconstruction of black pixels, as illustrated as in Fig. 4f-o.

4.2 Correctness of the theoretical contrasts

As stated in Section 3, theoretical contrasts of the extended $(2, \ infinity)$ SIS scheme are exactly the same as those of the basic $(2, 2)$ SIS scheme. The theoretical contrasts can be characterized by a general formula with a parameter β, as described as follows:

$$\alpha_{share} = \frac{1 - 2\beta}{1 + \beta} \tag{4}$$

$$\alpha_{xor} = 2\beta(1 - \beta) \tag{5}$$

It is observed that the contrasts of the shares and the revealed secret image do not depend on the extended number of shares. For example, assume that an extended $(2, \ infinity)$ SIS scheme is constructed underlying the $(2, 2)$ SIS scheme with β being 0.25. For the $(2, \ infinity)$ SIS scheme, no matter how large the number of the extended shares is, the contrasts of the share and the revealed secret image are fixed to $\frac{2}{5}$ and $\frac{3}{8}$, respectively.

To examine the correctness of the theoretical contrasts, the experimental contrasts of the revealed secret image and shares are desired to be calculated. Table 2 illustrates the experimental contrasts of the $(2, 2)$ experiment by Algorithm 1, while Tables 3 and 4 respectively illustrate the experimental contrasts of the $(2, 3)$ and $(2, 10)$ experiments, both of which are constructed underlying the $(2, 2)$ experiment by Algorithm 2. From Tables 2–4, for each

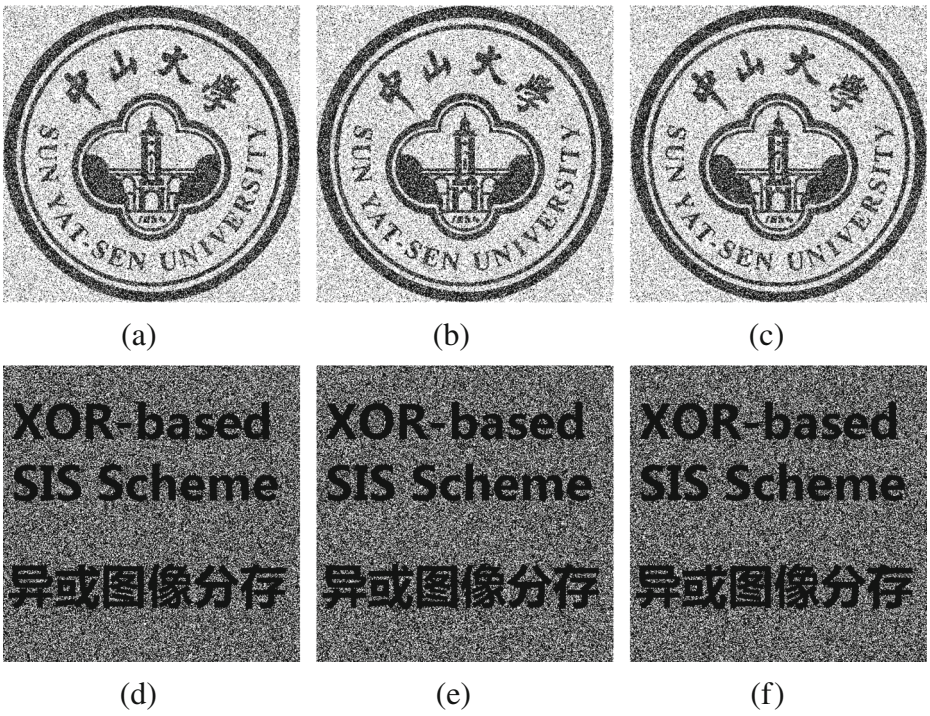


Fig. 3 Experimental results of the extended (2, $infinity$) SIS scheme for a (2, 3) case, which is constructed underlying the (2, 2) case of Fig. 2. **a–b** Two shares of the (2, 2) case by Algorithm 1: R_1 and R_2, **c** a new share R_3 generated by Algorithm 2, **d** $R_1 \oplus R_2$, **e** $R_1 \oplus R_3$, **f** $R_2 \oplus R_3$

single share R_i, we have $T(R_i[S(1)]) \approx T(R_i[S(0)])$ and $T(R_i[C(1)]) > T(R_i[C(0)])$. That implies the share resembles the cover image C but gives no clue about the secret image S. Hence, the security and meaningfulness conditions are met. For the XOR-ed result by any two shares R_x and R_y, denoted by $R_x \oplus R_y$, we can obtain $T((R_x \oplus R_y)[S(1)]) > T((R_x \oplus R_y)[S(0)])$ and $T((R_x \oplus R_y)[C(1)]) \approx T((R_x \oplus R_y)[C(0)])$. That indicates the XOR-ed result by any two shares visually reveals the secret image but carries no information about the cover image, so that the contrast condition is met as well. In addition, we found that $T((R_x \oplus R_y)[S(0)])$ is always equal to 0, that implies that the reconstruction of the black secret pixel is perfect. Further, the correctness of the theoretical contrasts is also substantiated by Tables 2–4, where the experimental contrasts are approximately the same as the theoretical contrasts.

4.3 Comparisons

For the extended (2, $infinity$) SIS scheme, the contrasts of both the share and revealed secret image do not depend on the extended number of shares. Indeed, the visual qualities of the extended (*2, infinty*) SIS scheme are always the same as those of the basic (2, 2) SIS scheme no matter how large the share number is. It is desired to calculate the contrasts of the revealed secret images by the proposed schemes, and compare them with those by other related schemes. In some reported $(2, n)$ SIS schemes [6–8, 29], the stacked result by any two shares can visually reveal the secret image, but the shares generated by these schemes

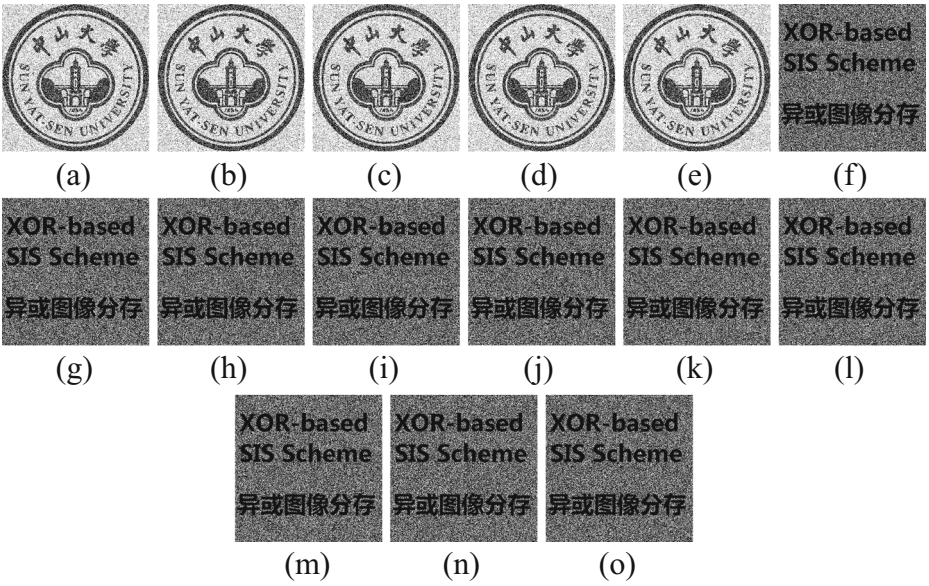


Fig. 4 Experimental results of the (2, $infinity$) SIS scheme for a (2, 10) case, which is constructed underlying the (2, 2) case of Fig. 2. (**a**-**c**) Two shares of the (2, 2) case by Algorithm 1: R_1 and R_2, (**c**-**e**) three of eight new shares by Algorithm 2: R_3, R_4 and R_5, (**f**) $R_1 \oplus R_2$, (**g**) $R_1 \oplus R_3$, (**h**) $R_1 \oplus R_4$, (**i**) $R_1 \oplus R_5$, (**j**) $R_2 \oplus R_3$, (**k**) $R_2 \oplus R_4$, (**l**) $R_2 \oplus R_5$, (**m**) $R_3 \oplus R_4$, (**n**) $R_3 \oplus R_5$, (**o**) $R_4 \oplus R_5$

are meaningless. For the fairness, the parameter β is set to 0.5 for generating meaningless shares by the proposed schemes. Contrast comparisons among the proposed schemes and related SIS schemes [6–8, 29] are provided in Table 5, where all the generated shares are meaningless. It is observed that the largest contrast of the revealed secret image by the proposed schemes is achieved. Specially, the value of $T(S^R[S(0)])$ calculated from the revealed secret image by the proposed schemes is always equal to zero, which indicates that the reconstruction of black secret pixels is perfect. However, the shares generated above are meaningless which may impose difficulty for managing the shares and increase the chance of suspicion on secret image communication. Fortunately, when the adjustable parameter β is satisfied $0 < \beta < 0.5$, the meaningful version of the proposed SIS scheme can be achieved, where the meaningful shares are generated.

It is desired to calculate the computational complexity of XOR decryption for the proposed scheme, and make comparisons of computational complexity among the proposed

Table 2 Experimental contrasts for the (2, 2) experiment of Fig. 2, where the theoretical contrast of the share is 0.5000 obtained by (4), and the theoretical contrast of the revealed secret image is 0.3200 obtained by (5)

Image R	$T(R[S(1)])$	$T(R[S(0)])$	Experimental α_{xor} for revealed secret image	$T(R[C(1)])$	$T(R[C(0)])$	Experimental α_{share} for the share
R_1	0.6047	0.6273	–	0.7988	0.2022	0.4971
R_2	0.6037	0.6273	–	0.7999	0.1992	0.5009
$R_1 \oplus R_2$	0.3209	0	0.3209	0.2652	0.2708	–

Table 3 Experimental contrasts for the (2, 3) experiment of Fig. 3, where the theoretical contrast of the share is 0.5000 obtained by (4), and the theoretical contrast of the revealed secret image is 0.3200 obtained by (5)

Image R	$T(R[S(1)])$	$T(R[S(0)])$	Experimental α_{xor} for revealed secret image	$T(R[C(1)])$	$T(R[C(0)])$	Experimental α_{share} for the share
R_1	0.6047	0.6273	–	0.7998	0.2022	0.4971
R_2	0.6037	0.6273	–	0.7999	0.1992	0.5009
R_3	0.6030	0.6273	–	0.7984	0.2007	0.4978
$R_1 \oplus R_2$	0.3209	0	0.3209	0.2652	0.2708	–
$R_1 \oplus R_3$	0.3220	0	0.3220	0.2653	0.2735	–
$R_2 \oplus R_3$	0.3201	0	0.3201	0.2652	0.2686	–

Table 4 Experimental contrasts for the (2, 10) experiment of Fig. 4, where the theoretical contrast of the share is 0.5000 obtained by (4), and the theoretical contrast of the revealed secret image is 0.3200 obtained by (5)

Image R	$T(R[S(0)])$	$T(R[S(1)])$	Experimental α_{xor} for revealed secret image	$T(R[C(0)])$	$T(R[C(1)])$	Experimental α_{share} for the share
R_1	0.6047	0.6273	–	0.7998	0.2022	0.4971
R_2	0.6037	0.6273	–	0.7999	0.1992	0.5009
R_3	0.6033	0.6273	–	0.7986	0.2009	0.4978
R_4	0.6051	0.6273	–	0.8013	0.2001	0.5010
R_5	0.6052	0.6273	–	0.8005	0.2019	0.4979
$R_1 \oplus R_2$	0.3209	0	0.3209	0.2652	0.2708	–
$R_1 \oplus R_3$	0.3208	0	0.3208	0.2646	0.2716	–
$R_1 \oplus R_4$	0.3198	0	0.3198	0.2638	0.2708	–
$R_1 \oplus R_5$	0.3204	0	0.3204	0.2635	0.2731	–
$R_2 \oplus R_3$	0.3203	0	0.3203	0.2647	0.2704	–
$R_2 \oplus R_4$	0.3171	0	0.3171	0.2616	0.2685	–
$R_2 \oplus R_5$	0.3192	0	0.3192	0.2632	0.2707	–
$R_3 \oplus R_4$	0.3210	0	0.3210	0.2651	0.2713	–
$R_3 \oplus R_5$	0.3216	0	0.3216	0.2656	0.2717	–
$R_4 \oplus R_5$	0.3184	0	0.3184	0.2623	0.2705	–

Table 5 Contrast comparisons among the proposed schemes with $\beta = 0.5$ and related SIS schemes

Schemes	$T(S^R[S(1)])$	$T(S^R[S(0)])$	α for revealed secret image
Our (2, 2) scheme	$\frac{1}{2}$	0	$\frac{1}{2}$
Our (2, $infinity$) scheme	$\frac{1}{2}$	0	$\frac{1}{2}$
Wu and Sun's (2, n) scheme [29]	$\sqrt{2}-1$	$3-2\sqrt{2}>0$	$\frac{\sqrt{2}-1}{2} < \frac{1}{2}$
Chen and Lin's (2, $infinity$) scheme [6]	$\sqrt{2}-1$	$3-2\sqrt{2}>0$	$\frac{\sqrt{2}-1}{2} < \frac{1}{2}$
Chen and Tsao's (2, n) scheme [7]	$\frac{1}{4}+\frac{1}{2n(n-1)}$	$\frac{1}{4}-\frac{1}{2n(n-1)}>0$	$\frac{4}{5n(n-1)-2} < \frac{1}{2}$
Chen and Tsao's (2, n) scheme [8]	$\frac{1}{2}$	$\frac{1}{4}>0$	$\frac{1}{5} < \frac{1}{2}$

Table 6 Comparisons of computational complexity for the decryption among the proposed scheme and other related SIS schemes, where k is the number of shares

Schemes	Computational complexity
The proposed scheme	$O(1)$
[29]	$O(1)$
[6]	$O(1)$
[7]	$O(1)$
[18]	$O(k)$
[8]	$O(1)$
[25]	$O(k)$
[20]	$O(1)$
[31]	$O(k \log^2 k)$
[15]	$O(k \log^2 k)$

scheme and other related SIS schemes [6–8, 15, 18, 20, 25, 29, 31], as shown as in Table 6. In the traditional $(2, n)$ SIS schemes [18, 25], when the involved share number k is larger than 2, all the k shares are usually used to decrypt the secret image. Since the computational complexity of XOR decryption is proportional to the share number, its computational complexity can be stated as $O(k)$. However, in the proposed scheme, we just utilized any 2 of these k shares to decrypt the secret image, so that its computational complexity is $O(1)$ which is approximately the same as that of the OR-based VC schemes [6–8, 20, 29]. Further, as compared to the computational complexity $O(k \log^2 k)$ of Shamir-based SIS schemes [15, 31], the computational complexity of the proposed scheme requires less time.

Feature comparisons among the proposed SIS schemes and related SIS schemes are demonstrated in Table 7. Major advantages of the proposed SIS schemes are given as follows:

1. The shares are with meaningful contents, which makes the shares management efficient.
2. The XOR-ed result by any two shares visually reveals the secret image but carries no information about the cover image.
3. The reconstruction of black secret pixels is perfect, which makes the secret image well identified by human visual system.

Table 7 Feature comparisons among our scheme and other related SIS schemes

Schemes	Features						
	Meaningful shares	Decryption	Perfect black	Visual quality	Pixel Expansion	Code book required	Type of VCS
ours	Yes	XOR	Yes	High	No	No	$(2, infinity)$
[29]	No	OR	No	Low	No	No	$(2, n)$
[6]	No	OR	No	Low	No	No	$(2, n)$,$(2, infinity)$
[7]	No	OR	No	Low	No	No	(k, n)
[18]	No	XOR	No	High	Yes	Yes	$(2, n)$
[8]	No	OR	No	Low	No	No	$(2, n)$, (n, n)
[25]	No	XOR	No	High	Yes	Yes	(k, n)
[20]	No	OR	No	Low	Yes	Yes	(k, n)

4. Superior visual quality is achieved as compared to some reported OR-based SIS schemes.
5. Merits such as no codebook required and no pixel expansion are maintained.

5 Conclusion

This paper is aimed at giving a new method to devise meaningful SIS schemes by flipping operations. The devised SIS schemes include the basic $(2, 2)$ SIS scheme and the extended $(2, infinity)$ SIS scheme. The proposed SIS schemes have advantages of no pixel expansion and no codebook required. In addition, shares with meaningful contents can be directly generated without any extra data hiding process, and superior visual qualities of both the share and revealed secret image are achieved by the proposed schemes. In the decrypting procedure of the extended $(2, infinity)$ SIS scheme, when more than two shares are provided, we just need any two of them to decrypt the secret image by XOR operations. Meanwhile, sufficient number of formal proofs are provided to validate the correctness of the proposed SIS schemes. The contrasts of both the share and revealed secret image can be characterized by a general formula with a parameter β, where the contrast of the share is $\frac{1-2\beta}{1+\beta}$ and the contrast of the revealed secret image is $2\beta(1-\beta)$. Further, the application of the proposed SIS schemes is flexible, because that the tradeoff among the visual quality of the share and revealed secret image can vary from the application to application by setting different parameters.

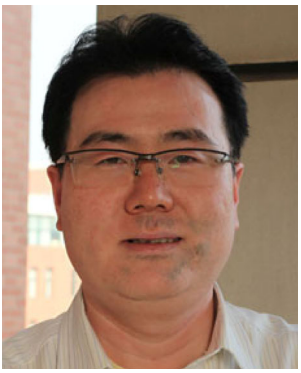
Acknowledgments This work was in part supported by 973 Program (Grant No. 2011CB302400) and Natural Science Foundation of Guangdong Province, China (Grant No. S2013010013728).

References

1. Ababneh S, Ansari R, Khokhar A (2009) Iterative compensation schemes for multimedia content authentication. J Vis Commun Image Represent 20(5):303–311
2. Ateniese G, Blundo C, Santis AD, Stinson DR (2001) Extended capabilities for visual cryptography. Theor Comput Sci 250(1):143–161
3. Blakley G (1979) Safeguarding cryptographic keys. In: Proceedings of AFIPS 1979, national computer conference, vol 48, pp 313–317
4. Blundo C, D'Arco P, De Santis A, Stinson DR (2003) Contrast optimal threshold visual cryptography schemes. SIAM J Discret Math 16(2):224–261
5. Blundo C, De Bonis A, De Santis A (2001) Improved schemes for visual cryptography. Designs. Codes Crypt 24(3):255–278
6. Chen SK, Lin SJ (2012) Optimal (2, n) and (2, infinity) visual secret sharing by generalized random grids. J Vis Commun Image Represent 23(4):677–684
7. Chen T, Tsao K (2011) Threshold visual secret sharing by random grids. J Syst Softw 84(7):1197–1208
8. Chen TH, Tsao KH (2009) Visual secret sharing by random grids revisited. Pattern Recogn 42(9):2203–2217
9. Chen TH, Tsao KH (2011) User-friendly random-grid-based visual secret sharing. IEEE Trans Circ Syst for Video Technol 21(11):1693–1703
10. Guo T, Liu F, Wu C (2013) K out of k extended visual cryptography scheme by random grids. Signal Process 94:90–101
11. Hofmeister T, Krause M, Simon HU (2000) Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theor Comput Sci 240(2):471–485
12. Kafri O, Keren E (1987) Encryption of pictures and shapes by random grids. Opt Lett 12(6):377–379
13. Koga H, Ueda E (2006) Basic properties of the (t, n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels. Des Codes Crypt 40(1):81–102

14. Li H (2009) Image encryption based on gyrator transform and two-step phase-shifting interferometry. Opt Lasers Eng 47(1):45–50
15. Lin C, Tsai W (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(3):405–414
16. Liu F, Wu C (2011) Embedded extended visual cryptography schemes. IEEE Trans Inf Forensic Secur 6(2):307–322
17. Liu F, Wu C, Lin X (2010) Step construction of visual cryptography schemes. IEEE Trans Inf Forensic Secur 5(1):27–38
18. Liu F, Wu CK (2010) Optimal xor based (2, n)-visual cryptography schemes. IACR Cryptol ePrint Arch 2010:545
19. Lu P, Xu Z, Lu X, Liu X (2013) Digital image information encryption based on compressive sensing and double random-phase encoding technique. Optik-Int J for Light and Electron Opt 124(16):2514–2518
20. Naor M, Shamir A (1995) Visual cryptography . In: Advances in Cryptology EUROCRYPT'94. Springer, Berlin Heidelberg New York, pp 1–12
21. Ou D, Sun W, Wu X (2015) Non-expansible xor-based visual cryptography scheme with meaningful shares. Signal Process 108(0):604–621
22. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
23. Shyu SJ (2007) Image encryption by random grids. Pattern Recogn 40(3):1014–1031
24. Shyu SJ (2009) Image encryption by multiple random grids. Pattern Recogn 42(7):1582–1596
25. Tuyls P, Hollmann HD, Van Lint JH, Tolhuizen L (2005) Xor-based visual cryptography schemes. Designs. Codes Crypt 37(1):169–186
26. Wang D, Zhang L, Ma N, Li X (2007) Two secret sharing schemes based on boolean operations. Pattern Recogn 40(10):2776–2785
27. Wu X, Liu T, Sun W (2013) Improving the visual quality of random grid-based visual secret sharing via error diffusion. Journal of Visual Communication and Image Representation 24:552–556
28. Wu X, Sun W (2012) Visual secret sharing for general access structures by random grids. IET Inf Secur 6(4):299–309
29. Wu X, Sun W (2013) Generalized random grid and its applications in visual cryptography. IEEE Trans Inf Forensic Secur 8(9):1541–1553
30. Yan X, Wang S, El-Latif AAA, Niu X (2014) Random grids-based visual secret sharing with improved visual quality via error diffusion. In: Multimedia tools application, pp 1–18
31. Yang C, Chen T, Yu KH, Wang C (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80(7):1070–1076
32. Zhang X, Qian Z, Ren Y, Feng G (2011) Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Trans Inf Forensic Secur 6(4):1223–1232
33. Zhou N, Wang Y, Gong L (2011) Novel optical image encryption scheme based on fractional mellin transform. Opt Commun 284(13):3234–3242

Duanhao Ou received his BSc in computer science from South China Agricultural University, Guangzhou, P.R., China, in 2009. He is currently a PhD candidate in the School of Information and Science at Sun Yat-Sen University. His research interests are steganography, secret sharing and image processing.



Wei Sun received his Ph.D. in Computer Science from Sun Yat-sen University in 2004. He is currently a professor in the School of Software at Sun Yat-sen University. His research interests are multimedia security and computer graphics.