Signal Processing 91 (2011) 90–97

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Efficient multi-secret image sharing based on Boolean operations

Tzung-Her Chen *, Chang-Sian Wu

Department of Computer Science and Information Engineering, National Chiayi University, 300 University Rd., Chia-Yi City, Taiwan 600, ROC

ARTICLE INFO

Article history:
Received 10 December 2009
Received in revised form
24 March 2010
Accepted 10 June 2010
Available online 25 June 2010

Keywords:
Multiple secret sharing
Image sharing
Image hiding
Visual secret sharing
Visual cryptography

ABSTRACT

(n,n) visual secret sharing (VSS), first proposed by Naor and Shamir (1995) [4], is used to encode (encrypt) a secret image into n meaningless share images to be superimposed later to decode (decrypt) the original secret by human visual system after collecting all n secret images. In recent years, VSS-based image sharing (encryption) and image hiding schemes, two of a variety of applications based on VSS, have drawn much attention. In this paper, an efficient (n+1,n+1) multi-secret image sharing scheme based on Boolean-based VSS is proposed to not only keep the secret images confidential but also increase the capacity of sharing multiple secrets. The Boolean-based VSS technology, used to encode the secret images, generates n random matrices; then the n secret images are subsequently encoded into the n+1 meaningless share images. It is worthwhile to note that n secret images can be hidden by means of sharing only n+1 share images in the proposed scheme instead of 2n share images. Thus, the present scheme thus benefits from (1) reducing the demand of image transmission bandwidth, (2) easing the management overhead of meaningless share images, and (3) involving neither significant extra computational cost nor distortion for reconstructed secret images. The experimental results show the performance in terms of feasibility and image sharing capacity. Applied into image hiding schemes, the proposed scheme can enhance the hiding capacity.

1. Introduction

Unlike traditional cryptosystems and chaos-based cryptosystems [1–3,23], which provide only computational security by the assumption that breaking the cryptosystem is computationally infeasible, visual secret sharing (VSS), so-called visual cryptography, aims at providing a perfect-security cryptosystem in which the decryption operation involves no computational cost instead of by the human visual system. Naor and Shamir [4] presented a (n,n) VSS scheme which encodes/encrypts a secret binary image into n meaningless share images such that the information of the secret image can be decoded/decrypted by superimposing all n share images later. Generally speaking, (2,2) VSS is regarded as an image encryption approach in which two basic matrices S^0 and S^1 are used to encode a secret binary image. The basic matrices are shown as follows for example:

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Each pixel of the secret image is encoded into 2 subpixels, namely the factor of pixel expansion is 2. If the pixel of S is white, the subpixels of two shares are assigned as $[0 \quad 1]$ and $[0 \quad 1]$ from matrix S^0; otherwise, the subpixels of two shares are assigned as $[0 \quad 1]$ and $[1 \quad 0]$ from matrix S^1.

Unfortunately, traditional VSS suffers pixel expansion and low image quality. A rapid progress of visual secret sharing in the recent researches [5–12] aiming to improve the problems of either reducing pixel expansion or increasing contrast (quality) in reconstructed images has

* Corresponding author. Tel.: +886 5 2717723; fax: +886 5 271 7741.
E-mail addresses: thchen@mail.ncyu.edu.tw (T.-H. Chen), cswu94@mail.csie.ncyu.edu.tw (C.-S. Wu).

0165-1684/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2010.06.012

been continually made so far while Yang et al.'s scheme [22] tried to remove the alignment problem in the secret decoding phase.

On the other hand, more and more multiple-secret sharing schemes [13–16] have been proposed based on traditional VSS. To this end, the goal of designing a new multi-secret VSS aims at using the same or even less number of share images but sharing multiple secrets. Wu and Chen [13] firstly presented a visual secret sharing scheme in which two secret images are encoded into two meaningless share images, say A and B. The first secret image can be directly revealed by superimposing A and B, and the second secret image can be obtained by superimposing A′ and B, where A′ is the result from rotating A at 90° counter-clockwise. Wu and Chang [14] further extended Wu and Chen's idea to design another secret sharing scheme in which two secret images are encoded into two circular share images. Although theoretically speaking, the share images can be rotated by some default angles to reveal more secrets, their scheme did suffer pixel expansion. The scheme in Ref. [15] is similar to that in Ref. [14] and thus the same shortcoming, i.e., pixel expansion, still exists. In Ref. [16], Shyu et al. proposed multiple-secret sharing algorithm using circular share images without maintaining the codebook. But the problem of pixel expansion still depends on the number of secrets.

The abovementioned schemes for encoding multiple secrets have the following common drawbacks.

(1) The reconstructed secret images in traditional VSS are inherently not easy to visually recognize because the contrast is low. The more secrets are shared, the contrast become worse dramatically.
(2) The schemes suffer the problem of pixel expansion. It causes more cost to transmit or store the share images. The more secret images are encoded; the size of share images and the complexity of designing the codebook both become cost-expensive dramatically.
(3) The schemes are only suitable for dealing with binary secret images rather than gray-level or color images directly.
(4) During decoding process, the alignment of stacking share images is not easy to do in practical even for experienced participants. Even though the deviation of superimposing two share images is from only few pixels or angles, the information appeared on the stacked image is hard to recognize.

On the other hand, more and more VSS-based image hiding researches [17–19] have been proposed to combine data hiding and VSS. In Ref. [17], the secret image is firstly turned into two share images which are subsequently embedded into the least significant bits (LSBs) of two cover images, respectively. The drawback in this hiding method is that the quality of extracted image is not well-recognized compared to general hiding approaches. Chang and Yu [18] presented a new secret sharing and hiding scheme based on VSS. A gray image is hidden in two different shares by a Boolean matrix designed in accordance with the secret image and a random number generator. However, their scheme needs to additionally maintain a Color Index Table (CIT) in order to recover the higher quality of the secret image. In Ref. [19], Chang and Yu's scheme [18] has been improved to recover a lossless secret image.

Unfortunately, the abovementioned VSS-based hiding schemes suffer either hard-to-easy-recognize or pixel expansion. Wang et al. [12] proposed a Boolean-based VSS with no pixel expansion and perfect contrast of the reconstructed image by means of introducing a little computation cost to reconstruct the secret image in the decoding phase.

Inspired from Boolean-based VSS, a new (n+1,n+1) multi-secret sharing scheme based on Boolean-based VSS is proposed to enhance the sharing capacity of VSS. To begin with, the Boolean-based VSS technology, used to encode the secret images, generates n random matrices; then the n secret images are subsequently encoded into the n+1 meaningless share images. In the decoding phase, the participants collect all n+1 share images to reconstruct all n secret images.

Compared with traditional VSS-based image sharing schemes [13–16], the proposed scheme benefits certain valuable merits worthwhile to highlight as follows:

(1) *Lossless secret reconstruction*: The reconstructed images are identical to the original secret images.
(2) *No pixel expansion*: Since no pixel expansion occurs, it saves bandwidth to transmit and storage to store.
(3) *Generalization of image format*: The secrets can be in the form of binary, gray-level, or color images.
(4) *Not-easy-to-align*: Thanks to light computation involved, the difficulty of aligning all the share images precisely in the decoding phase is removed.
(5) *No codebook required*: There is no codebook required to pre-define and share among participants such that the burden of maintaining codebook is removed.

Compared with the schemes in Refs. [12,17–19] combining VSS and image hiding technique, the proposed scheme has the following advantages:

(1) *Multi-secret sharing*: Compared with existing VSS-based sharing schemes, the sharing ability of the proposed scheme is extended to encode n images rather than one image only. n secret images can be shared at once by means of sharing $n+1$ share images instead of $2n$ share images in Wang et al.'s Boolean-based VSS. The more the secret images; the more efficient is the proposed scheme.
(2) *Computational efficiency*: Thanks to the age of ubiquitous computing, people possess or utilize computational devices as essential items in daily life. Since the encoding and decoding processes without involving complex operations, it is easy and simple to implement with low computational cost on lightweight devices.

The rest of the paper is organized as follows. In Section 2, the present image hiding method based on

Boolean-based VSS is proposed. The experimental results and further discussions are shown in Section 3. Finally, the conclusions are given in Section 4.

2. Proposed scheme

In this section, a multi-secret sharing (n+1,n+1) algorithm based on Boolean-based VSS is proposed. Prior to demonstrating the proposed scheme, the schemes proposed by Wang et al. [12] are briefly introduced.

2.1. Review of (n,n) Boolean-based VSS

Wang et al. brought up two different algorithms, called deterministic (n,n) and probabilistic (2,n), with Boolean-based VSS to encode binary image, gray-level and color images. The (n,n) Boolean-based VSS for binary, gray-level, and color images is adopted in this paper. Suppose that a gray-level image G of size $h \times w$ pixels is encoded to n share images S_i, i=1,2,…,n.

First, the image matrix exclusive-OR operation and the image matrix chain exclusive-OR operation, which are the main operations in this paper, are defined.

Definition 1. Image matrix exclusive-OR operation.

Assume A and B are two image matrices with the same dimension $p \times p$ while C and D are two random matrices with the same dimension as A, where the elements of matrices A, B, C, and D are binary.

Case 1: Binary image matrix $A \oplus B=[a_{i,j} \oplus b_{i,j}]$, where i,j=0,1,…,p−1 and $\oplus$ is bit-wise exclusive-OR operation.

Case 2: For 256-gray-level image, each pixel is represented with eight bits. 256-gray-level image matrix $A \oplus B=[a_{i,j,k} \oplus b_{i,j,k}]$, where i,j=0,1…,p−1, k=0,1,…,7.

Case 3: For 24-bit color image, assume the additive model (so-called RGB system) [24] is adopted for example. Each color pixel is represented with three primary colors, red (R), green (G), and blue (B), in which each is represented with eight bits. 24-bit color image matrix $A \oplus B=[a_{i,j,kr,kg,kb} \oplus b_{i,j,kr,kg,kb}]$, where i,j=0,1,…,p−1, k_r=0,1,…,7, k_g=0,1,…,7, k_b=0,1…,7. Thus, it satisfies

(1) $A \oplus B=B \oplus A$;
(2) $A \oplus A=0$;
(3) $A \oplus C$ is random; and
(4) $A \oplus C=D$ implies $C \oplus D=A$.

Definition 2. Image matrix chain exclusive-OR operation.

A_i, i=1,…,k, are image matrices with the same dimension $p \times p$. The exclusive-OR operation to all A_i is defined as $\Psi_{i=1}^{k} A_i = A_1 \oplus A_2 \oplus \cdots \oplus A_k$.

The encoding process involves two steps:

Step 1: Generate n−1 random matrices B_1, B_2, …, and B_{n-1}. Note that if a well-defined random number generator, such as a "linear feedback shift register", is adopted, the generated random matrices B_1, B_2, …, and B_{n-1} will be distinct.

Step 2: Compute the share images S_i (i=1,…,n) by the following operations:

$$S_k = \begin{cases} B_k & \text{if } k=1 \\ B_k \oplus B_{k-1} & \text{if } k=2,\ldots,n-1 \\ G \oplus B_{k-1} & \text{if } k=n \end{cases} \quad (1)$$

where G is the secret image

Theorem 1. The generated share images S_i (i=1,2,…,n) are n distinct random matrices. Each S_i does not contain any information of the original secret image.

Proof. Since all random matrices B_i are distinct, the obtained share images S_i are also random and distinct. Thus, S_i does not reveal any information of the secret image.

The details are described in Algorithm 1 for gray-level images, for example. □

Algorithm 1a. Encoding.

Input: A gray-level secret image $G=\{G[i,j] | G[i,j] \in [0,255], 1 \leqq i \leqq h, 1 \leqq j \leqq w\}$
Output: n share images $S_m=\{S_m[i,j] | S_m[i,j] \in [0,255], 1 \leqq i \leqq h, 1 \leqq j \leqq w\}$, m=1,2,…,n

```
//Generate n−1 random matrices B1, B2,…, Bn−1
For k=1 to n−1
  For i=1 to h
      For j=1 to w
          Bk[i, j]=Random(0, 255)
//Random(0, 255) generates a value in the range [0, 255]
randomly
//Compute the share images
For i=1 to h
  For j=1 to w
    S1[i, j]=B1[i, j];
For k=2 to n−1
  For i=1 to h
    For j=1 to w
      Sk[i, j]=Bk[i, j]⊕Bk−1[i, j];
For i=1 to h  For j=1 to w     Sn[i, j]=Bn−1[i, j]⊕G[i, j]
```

Algorithm 1b. Decoding.

Input: n share images S_m, m=1,2,…,n
Output: A reconstructed gray-level secret image G′

```
//Reconstruct the secret image
For i=1 to h
  For j=1 to w
    G′[i, j]=S1[i, j]⊕S2[i, j]⊕⋯⊕Sn[i, j];
```

In the decoding phase, n share images are used to reveal the secret image by exclusive-OR operation as follows:

$$G = \Psi_{i=1}^{n} S_i \quad (2)$$

Although the decoding process needs a little computation cost for exclusive-OR operations, the time is negligible and the reconstructed image is lossless.

Theorem 2. *The original secret G can be reconstructed by means of exclusive-ORing all n share images* $G = \Psi_{i=1}^{n} S_i = S_1 \oplus S_2 \oplus \cdots \oplus S_n$.

Proof. Based on Definition 1, exclusive-OR operation is associative and $B_i \oplus B_i$ is a zero matrix. Thus, $S_1 \oplus S_2 \oplus S_3 \oplus \cdots \oplus S_{n-1} \oplus S_n = B_1 \oplus (B_2 \oplus B_1) \oplus (B_3 \oplus B_2) \oplus \cdots \oplus (B_{n-1} \oplus B_{n-2}) \oplus (G \oplus B_{n-1}) = G$. □

2.2. The proposed secret sharing scheme for multiple secret images

Without losing the generality, the secret gray-level images are taken for example although the proposed scheme is also suitable for encoding binary or color images. In the proposed scheme, n secret images G_i, i=0, 1, …, n−1, are encoded into n+1 share images S_m, m=0, 1, 2, …, n. Furthermore, we assume that all images G_i are with high entropy, such as natural images photographed by digital camera, and distinct one another. If not the case, the slight modification is given later.

The encoding phase consists of three steps:

Step 1: Generate a random integer matrix as the first share image S_0 with the same size of secret images. The random values in S_0 are in the range between 0 and 255.

Step 2: Generate n−1 random matrices B_i by the following operations:

$$B_k = G_k \oplus S_0$$

where

$$k = 1,2,\ldots,n-1$$

Step 3: Compute the other share images S_i by the following operations:

$$S_k = \begin{cases} B_k & \text{if } k = 1 \\ B_k \oplus B_{k-1} & \text{if } k = 2,\ldots,n-1 \\ G_0 \oplus B_{k-1} & \text{if } k = n \end{cases} \quad (4)$$

The proposed encoding scheme is sketched in Fig. 1 and described in detail by Algorithm 2 for gray-level images for example.

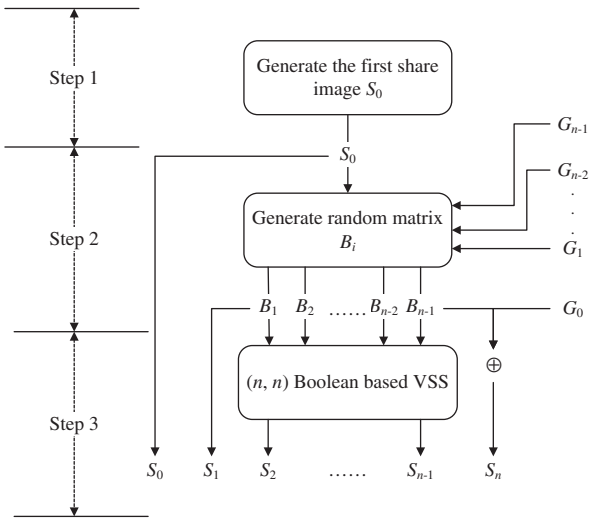

Fig. 1. Multi-secret sharing by Boolean-based VSS.

Algorithm 2. Image encoding

Input: n gray-level secret images $G_k=\{G_k[i, j] | G_k[i, j] \in [0, 255], 1 \leqq i \leqq h, 1 \leqq j \leqq w\}$, k=0, 1, …, n−1.
Output: n+1 share images $S_m=\{S_m[i, j] | S_m[i, j] \in [0, 255], 1 \leqq i \leqq h, 1 \leqq j \leqq w\}$, m=0, 1, 2, …, n.

```
Step 1: //Generate a random matrix as the first share image S0
        For i=1 to h
          For j=1 to w
            S0[i, j]=Random(0, 255)
        //Random(0, 255) generates a value in the range [0, 255] randomly
Step 2: //Generate n−1 random matrices B1, B2, …, Bn−1
        For k=1 to n−1
          For i=1 to h
            For j=1 to w
              Bk[i, j]=Gk[i, j]⊕S0[i, j]
Step 3: //Compute the other share images
        For i=1 to h
          For j=1 to w
            S1[i, j]=B1[i, j]
        For k=2 to n−1
          For i=1 to h
            For j=1 to w
              Sk[i, j]=Bk[i, j]⊕Bk−1[i, j]
        For i=1 to h
          For j=1 to w
            Sn[i, j]=G0[i, j]⊕Bn−1[i, j]
```

Theorem 3. *Assume that n $(n > 1)$ distinct secret images G_k with high entropy, k=0, 1, …, n−1, are encoded into n+1 share images S_m, m=0, 1, 2,…, n. Any share image alone, say S_m, will not reveal the information of any secret image.*

Proof. Since S_0 is a random matrix and $B_k=G_k \oplus S_0$ if $k=1,2,\ldots,n-1$, B_k is still a random matrix according to Definition 1.

Furthermore,

$$S_k = \begin{cases} B_k & \text{if } k = 1 \\ B_k \oplus B_{k-1} & \text{if } k = 2,\ldots,n-1 \\ G_0 \oplus B_{k-1} & \text{if } k = n \end{cases}$$

thus, all S_k are still random matrices. Hence, any share image alone will not reveal the information of any secret image. □

2.3. The proposed decoding scheme for multiple secret images

The decoding phase consists of three steps:

Step 1: All n+1 share images collected together are used to reconstruct the first secret image as follows:

$$G'_0 = \Psi_{i=1}^{n} S_i \quad (5)$$

Step 2: Generate n−1 random matrices B_i, which are obtained as follows:

$$B_k = \begin{cases} S_k & \text{if } k = 1 \\ S_k \oplus B_{k-1} & \text{if } k = 2,\ldots,n-1 \end{cases} \quad (6)$$

Step 3: Reconstruct the other $(n-1)$ secret images G'_m by the following operations:

$$G'_k = B_k \oplus S_0 \text{ if } k = 1,\ldots,n-1 \quad (7)$$

The proposed decoding scheme is shown in Fig. 2 and described in detail by Algorithm 3.

Algorithm 3. Image decoding

Input: n+1 share images $S_m=\{S_m[i,j] \mid S_m[i,j]\in[0,255], 1\leqq i\leqq h, 1\leqq j\leqq w\}$, m=0, 1,2,…,n.
Output: n gray-level images $G'_k=\{G'_k[i,j] \mid G'_k[i,j]\in[0,255], 1\leqq i\leqq h, 1\leqq j\leqq w\}$, k=0, 1, …, n−1.

Step 1: //Reconstruct the first secret image
For i=1 to h
  For j=1 to w
    $G'_0[i,j]=S_1[i,j]\oplus S_2[i,j]\oplus\cdots\oplus S_n[i,j]$
Step 2: //Compute n−1 random matrices $B_1, B_2,\ldots, B_{n-1}$
For i=1 to h
  For j=1 to w
    $B_1[i,j]=S_1[i,j]$
For k=2 to n−1
  For i=1 to h
    For j=1 to w
      $B_k[i,j]=S_k[i,j]\oplus B_{k-1}[i,j]$
Step 3: //Reconstruct the other secret images $G'_1, G'_2,\ldots, G'_{n-1}$.
For k=1 to n−1
  For i=1 to h
    For j=1 to w
      $G'_k[i,j]=B_k[i,j]\oplus S_0[i,j]$

Theorem 4. *Assume that n $(n>1)$ distinct secret images G_k with high entropy, k=0, 1,…, $n-1$, are encoded into n+1 share images S_m, m=0, 1, 2,…, n. The secret images can be reconstructed correctly by the following formula*:

$$G_k = \begin{cases} \overset{n}{\underset{i=1}{\Psi}} S_i & \text{if } k=0 \\ \overset{k}{\underset{i=0}{\Psi}} S_i & \text{otherwise} \end{cases}$$

Proof. The proof is shown by demonstrating two cases:
Case 1: k=0

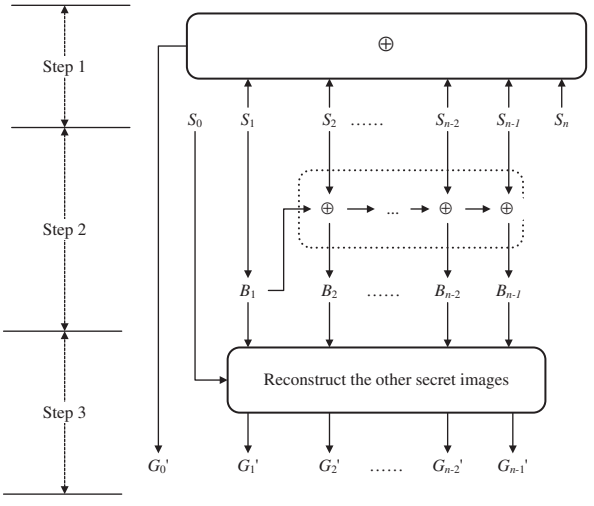

Fig. 2. Multi-secret reconstruction by Boolean-based VSS.

We have $\Psi_{i=1}^{n} S_i = S_1 \oplus S_2 \oplus \cdots \oplus S_n = G_0$ as the proof in Theorem 2.

Case 2: k > 1

We have $\Psi_{i=0}^{k} S_i = S_0 \oplus S_1 \oplus S_2 \oplus \cdots \oplus S_k = S_0 \oplus B_1 \oplus (B_2 \oplus B_1) \oplus \cdots \oplus (B_k \oplus B_{k-1}) = S_0 \oplus B_k = G_k$. □

2.4. The slight modified version of the proposed scheme for low entropy secret images

Taking secret images with low entropy into account, it is technically not correct to say that $S_k=B_k\oplus B_{k-1}=G_k\oplus G_{k-1}$, where k=2,…, n−1, is random if G_k and G_{k-1} are two low-entropy images.

In order to remove this potential security problem, the slight modification is given below. Firstly, the encoding operation Eq. (4) is modified as

$$S_k = \begin{cases} G_k \oplus S_0 & \text{if } k=1 \\ G_k \oplus G_{k-1} \oplus S_0 & \text{if } k=2,\ldots,n \end{cases} \quad (8)$$

Secondly, the decoding operations Eqs. (5)–(7) should be modified as

$$G'_k = \overset{k}{\underset{i=(k+1) \bmod 2}{\Psi}} S_i \quad (9)$$

That is, $G_1 = S_0 \oplus S_1$, $G_2 = S_1 \oplus S_2$, $G_3 = S_0 \oplus S_1 \oplus S_2 \oplus S_3$, $G_4 = S_1 \oplus S_2 \oplus S_3 \oplus S_4$, and so on.

3. Experimental results and discussions

3.1. Experimental results

To demonstrate the feasibility of the present multi-secret sharing scheme, the encoding/decoding experiments are conducted by adopting (3,3) Boolean-based VSS for example. Three gray-level secret images G_0, G_1, and G_2 of size 512×512 pixels, as shown in Fig. 3(a)–(c), will be encoded into four share images S_0, S_1, S_2, and S_3 as shown in Fig. 4(a)–(d). In the decoding phase, the reconstructed image G'_0, G'_1, and G'_2, as shown in Fig. 5(a)–(c), are computed from S_0, S_1, S_2, and S_3.

3.2. Performance of functionality

For the original Boolean-based sharing scheme, it costs n share images to encode one secret image. Upon encoding n secret images, 2n share images are generated in Wang et al.'s scheme. With n+1 share images, the proposed scheme can encode n secret images. Compared with the other schemes in Refs. [12–16], the proposed scheme has much higher capacity of sharing. Since the pixel expansion raises the performance of reducing the burden of storage and transmission bandwidth, it should be taken into account while comparing image sharing capacity. The sharing capacity is defined as

$$\frac{\text{the number of secret images}}{\text{the number of the share images} \times \text{pixel expansion}} \quad (10)$$

Obviously, the proposed scheme has the following features: (1) lossless secret reconstruction, (2) no pixel expansion, (3) use of different image formats, (4) easy to

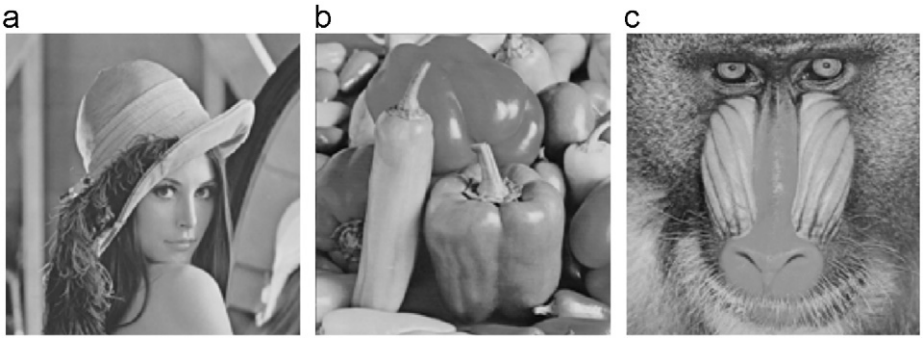

Fig. 3. (a) Secret image G_0, (b) secret image G_1, and (c) secret image G_2.

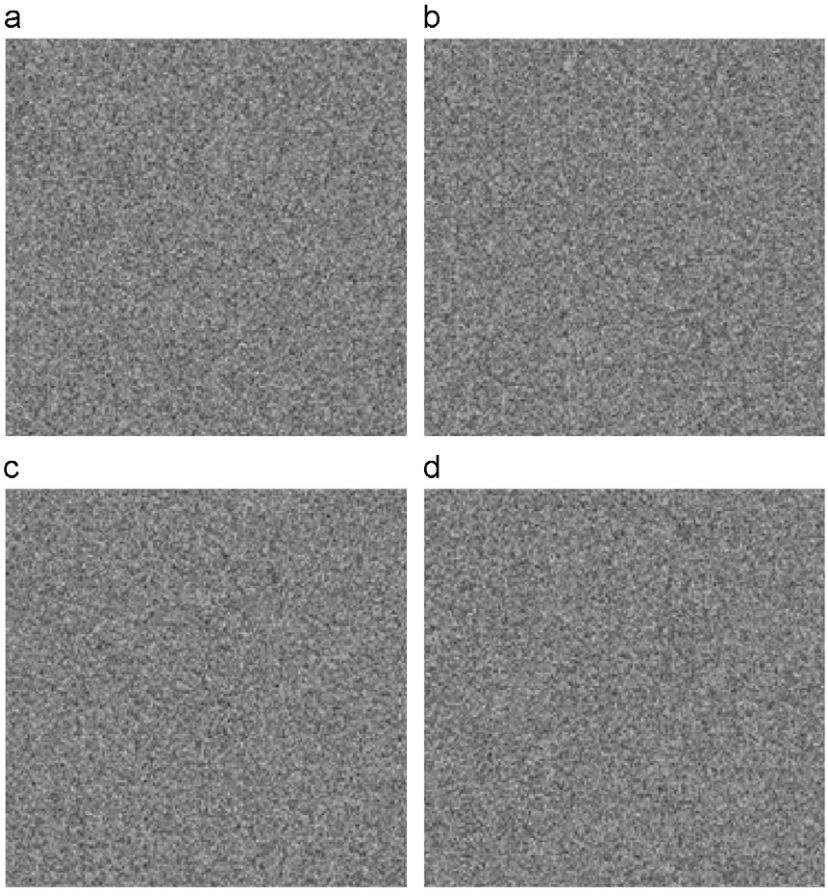

Fig. 4. (a) Share image S_0, (b) share image S_1, (c) share image S_2, and (d) share image S_3.

align, and (5) no codebook required. The comparison between the related image sharing methods and the proposed scheme is shown in Table 1.

As mentioned above, the proposed scheme can be regarded as an image hiding scheme. That is, n secret images are turned into (n+1) shares. Every share is hidden into a cover image. From this point of view, the proposed scheme can embed one secret image and extra $n-1$ hiding images, into n+1 cover images. If the hiding capacity is defined as

$$\frac{\text{the size of secret images}}{\text{the size of cover images}} \tag{11}$$

Hence, the hiding capacity is $1+(n-1)/n+1=n/n+1$. Compared with the related schemes, the capacity of the proposed scheme is much larger than that of the others.

The related methods are compared with the proposed scheme in Table 2.

Fig. 5. (a) Reconstructed image G'_0, (b) reconstructed image G'_1, and (c) reconstructed image G'_2.

Table 1
Functionality comparison between the related image sharing and the proposed scheme.

	Wu and Chen[13]	Wu and Chang [14]	Chen et al. [15]	Shyu et al. [16]	Wang et al. [12]	The proposed
Lossless secret construction	Recognizable	Recognizable	Recognizable	Recognizable	Lossless	Lossless
Pixel expansion	Yes	Yes	Yes	Yes	No	No
Image format	Binary	Binary	Binary	Binary	Binary gray-level Color	Binary gray-level Color
Alignment	Hard	Hard	Hard	Hard	Easy	Easy
Need codebook	Yes	Yes	Yes	No	No	No
Share shapes	Rectangle	Circle	Circle	Circle	Rectangle	Rectangle
Sharing capacity	$\frac{2}{2\times 4}$	$\frac{2}{2\times 4}$	$\frac{n}{2\times 4}$	$\frac{n}{2\times(2\times n)}$	$\frac{1}{n\times 1}$	$\frac{n}{(n+1)\times 1}$

Table 2
Comparison between the related image hiding and the proposed scheme.

	Chang et al. [17]	Chang and Yu [18]	Youmaran et al. [19]	The proposed
Hiding method	VSS	VSS	VSS	Boolean VSS
Need codebook	Yes	No	No	No
Pixel expansion	Yes	Yes	Yes	No
Reconstructive image quality	Recognizable	Recognizable	Recognizable	Lossless
Embedding image format	Binary	Binary gray-level Color	Binary gray-level Color	Binary gray-level Color
Capacity	1/64	$1/n$	$1/n$	$\frac{n}{n+1}$

3.3. Performance of computational efficiency

In order to demonstrate the efficiency, we carry on the abovementioned experiments. The original Boolean-based sharing scheme [12] spends 0.046 s in encoding three secret images into six share images. The proposed scheme takes 0.015 s to encode three secret images into four share images. In the two schemes, the computation cost mainly depends on the cost of generating the random matrices in Step 1 of Algorithms 1 and 2 rather than the cost of exclusive-OR operations, the computation cost of exclusive-OR negligible. The more images to encode; the higher efficiency the proposed scheme has.

On the other hand, the computation cost in the decoding phase is analyzed below. The computation complexity of reconstructing the secret of the image sharing methods by adopting polynomial evaluation and interpolation such as Refs. [20,21] is $O(m \log^2 m)$, where m is the number of shares. For the Boolean operation based secret sharing schemes, Wang et al.'s (m,m) scheme reconstructs one secret image in Eq. (2). The computation cost is proportional to m, i.e., O(m). In the case of reconstructing n secret images, the cost will be $O(m \times n)$.

In the proposed scheme, the computation cost of decoding n secret images includes O(m) in Eq.(5), O(m) in Eq.(6), and O(m) in Eq.(7). Approximately, the decoding computation complexity for n secret images in the proposed scheme is O(m). Table 3 shows the comparison in term of computation complexity in the decoding phase between the related works and the proposed scheme.

4. Conclusions

A multi-secret sharing scheme based on Boolean-based VSS is presented to benefit from not only preserving the

Table 3
Computational complexity comparison between the related works and the proposed scheme in the decoding phase.

Schemes	Complexity for one secret	Complexity for n secret
Traditional secret sharing [20]	$O(m \log^2 m)$[a]	$O(n \times m \log^2 m)$
Traditional VSS [4]	$O(m)$	$O(m \times n)$
Wang et al. [12]	$O(m)$	$O(m \times n)$
Ours	$O(m)$	$O(m)$

[a] m is the number of shares.

valuable advantages of Boolean-based VSS but also increasing the capacities of secret image sharing and image hiding. Precisely, the proposed scheme can encode n secret images by sharing n+1 share images among the participants instead of 2n share images in the related schemes. Compared with tradition VSS-based image sharing schemes, the proposed scheme benefits valuable merits including lossless secret reconstruction, no pixel expansion, generalization of image format, no not-easy-to-align problem, and no codebook required. Compared with the schemes combining VSS and image hiding technique, the proposed scheme has the two main advantages: high sharing capacity and computational efficiency of multi-secret sharing. The experimental results demonstrate that the present (n+1,n+1) VSS scheme does work well.

References

[1] K. Li, Y.C. Soh, C. Zhang, A frequently aliasing approach to chaos-based cryptosystems, IEEE Transactions on Circuits and Systems—I: Regular Papers 51 (12) (2004) 2470–2475.
[2] R. Tenny, L.S. Tsimring, Additive mixing modulation for public key encryption based on distributed dynamics, IEEE Transactions on Circuits and Systems—I: Regular Papers 52 (3) (2005) 672–679.
[3] R. Bose, S. Pathak, A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system, IEEE Transactions on Circuits and Systems—I: Regular Papers 53 (4) (2006) 848–856.
[4] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology-Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.
[5] M. Nakajima, Y. Yamaguchi, Extended visual cryptography for natural images, in: Proceedings of the 10th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision, 2002, pp. 303–340.
[6] C.N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters 25 (4) (2004) 481–494.
[7] C.N. Yang, T.S. Chen, Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion, Pattern Recognition Letters 26 (2) (2005) 193–206.
[8] D. Jin, W.Q. Yan, M.S. Kankanhalli, Progressive color visual cryptography, Journal of Electronic imaging 14 (3) (2005) 033019-1–033019-13.
[9] S. Cimato, A.D. Santis, A.L. Ferrara, B. Masucci, Ideal contrast visual cryptography schemes with reversing, Information Processing Letters 93 (4) (2005) 199–206.
[10] C.N. Yang, T.S. Chen, Size-adjustable visual secret sharing schemes, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E88-A (9) (2005) 2471–2474.
[11] C.N. Yang, T.S. Chen, Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation, Pattern Recognition 39 (7) (2006) 1300–1314.
[12] D. Wang, L. Zhang, N. Ma, X. Li, Two secret sharing schemes based on Boolean operations, Pattern Recognition 40 (10) (2007) 2776–2785.
[13] C.C. Wu, L.H. Chen, A study on visual cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.
[14] H.C. Wu, C.C. Chang, Sharing visual multi-secrets using circle shares, Computer Standards & Interfaces 134 (28) (2005) 123–135.
[15] J. Chen, Y.S. Chen, H.C. Hsu, H.W. Chen, New visual cryptography system based on circular shadow image and fixed angle segmentation, Journal of Electronic Imaging 14 (3) (2005) 033018-1–033018-5.
[16] S.J. Shyu, S.Y. Huang, Y.K. Lee, R.Z. Wang, Sharing multiple secrets in visual cryptography, Pattern Recognition 40 (12) (2007) 3633–3651.
[17] C.C. Chang, J.C. Chuang, P.Y. Lin, Sharing a secret two-tone image in two gray-level images, in: Proceedings of the 11th International Conference on Parallel and Distributed Systems, vol. 2, pp. 300–304, 2005.
[18] C.C. Chang, T.X. Yu, Sharing a secret gray image in multiple images, in: Proceedings of the International Symposium on Cyber Worlds: Theories and Practice, 2002, pp. 230–237.
[19] R. Youmaran, A. Adler, A. Miri, An improved visual cryptography scheme for secret hiding, in: Proceedings of the 23rd Biennial Symposium on Communications, 2006, pp. 340–343.
[20] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–613.
[21] C.C. Chang, R.J. Hwang, Sharing secret images using shadow codebooks, Information Sciences 111 (1998) 335–345.
[22] C.N. Yang, A.G. Peng, T.S. Chen, MTVSS: (M)isalignment (T)olerant (V)isual (S)ecret (S)haring on resolving alignment difficulty, Signal Processing 89 (8) (2009) 1602–1624.
[23] X. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator, Signal Processing 89 (4) (2009) 480–491.
[24] Z.N. Li, M.S. Drew, Fundamentals of Multimedia, Pearson Prentice-Hall, 2004.