Pattern Recognition 41 (2008) 3572 – 3581

Contents lists available at ScienceDirect

Pattern Recognition

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

Visual secret sharing for multiple secrets

Jen-Bang Feng[a], Hsien-Chu Wu[b,*], Chwei-Shyong Tsai[c], Ya-Fen Chang[b], Yen-Ping Chu[d]

[a]*Department of Computer Science and Engineering, National Chung Hsing University, 250, Kuo Kuang Road, Taichung City, Taiwan, ROC*
[b]*Department of Computer Science and Information Engineering, National Taichung Institute of Technology, 129, Section 3, San Min Road, Taichung City, Taiwan, ROC*
[c]*Department of Management Information Systems, National Chung Hsing University, Taiwan, ROC*
[d]*Department of Computer Science and Information Engineering, Tunghai University, 181, Section 3, Taichung Port Road, Situn District, Taichung City, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 4 November 2006
Received in revised form 28 February 2008
Accepted 29 May 2008

Keywords:
Visual cryptography
Visual secret sharing
Multiple secret sharing
Visual pattern

ABSTRACT

Conventional visual secret sharing schemes are designed for a single secret image so it is inefficient to generate numerous share images for multiple secret images simultaneously. Therefore, a novel visual secret sharing scheme for multiple secret images is proposed in this paper. In the proposed encryption process, a stacking relationship graph of secret pixels and share blocks is generated to indicate the encryption functions, and a set of visual patterns is defined to produce two share images according to this graph. Based on the stacking properties of these patterns, the secret images can be obtained from the two share images at aliquot stacking angles. The proposed scheme makes the number of secret images not restricted and further extends it to be general. As a result, the proposed scheme enhances visual secret sharing schemes' ability for multiple secrets.

1. Introduction

With the rapid growth of computer technologies, plenty of applications have been proposed to make human life more and more convenient. On the contrary, the security of secret data is threatened because anyone may tend to intrude the system or eavesdrop via the communication channel. One approach to have the essential information secure not retrieved by malicious users easily is making the essential information shared among several participants. Secret sharing schemes proposed by Blakley [1] and Shamir [2], respectively, are to distribute secret information to participants. The secret can only be obtained by the cooperation of these participants. The ordinary concept of secret sharing is sharing the secret key, and secret sharing schemes are also wildly used for secret transmission nowadays. But most secret sharing schemes are based on cryptography [3–11] such that the encryption and decryption processes need high computation costs. Visual cryptography, a kind of secret sharing schemes, differs from traditional secret sharing in terms of the efficient decryption process. Visual secret sharing schemes hide the secret image into several share images and distribute these share images to participants. With no computation, human beings are able to obtain the secret image by stacking share images. This property makes visual cryptography especially suited to the low computation load requirement.

In 1994, Naor and Shamir first proposed a (k, k)-threshold visual secret sharing scheme, namely the (k, k)–VSS scheme, to achieve secret sharing [12]. In the (k, k)–VSS scheme, the latter number "k" means that the secret image is hidden into k share images, and the former "k" means that it needs all the k share images to retrieve the secret image. In visual secret sharing schemes, every secret pixel is hidden into a block of sub-pixels. By the property that black pixels absorb the light but transparent (white) pixels do not, two blocks with the same numbers of black and white sub-pixels can get different stacked results according to the different pixel distribution. Therefore, visual colors of the stacked blocks are distinguished from the relative difference.

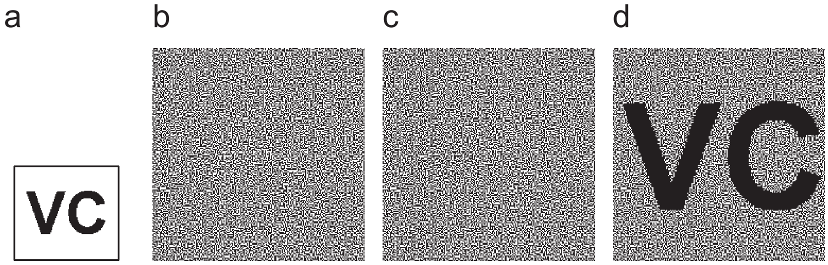
Many visual cryptography schemes have been proposed to support different requirements. From the (k, k)–VSS scheme, (k, n)–VSS schemes were also proposed to support variable threshold numbers [12–16], in which the secret image is hidden into n share images and the secret can be retrieved by the cooperation of at least k of them. Then, Ateniese et al. [17] proposed a visual secret sharing scheme that the decryption rule is more general than the threshold ones. Researchers also extended visual secret sharing schemes to support grayscale images [3,18] and color images [19–26], and the contrast is also taken into consideration [18–20,27]. Iwamoto and Yamamoto [28] proposed another scheme to support color secret images with general decryption rules, and Nakajima and Yamaguchi [29] indicated how to enhance the share images to be meaningful.

[*] Corresponding author. Fax: +886 4 22196311.
E-mail addresses: jbonf@cs.nchu.edu.tw (J.-B. Feng), wuhc@ntit.edu.tw (H.-C. Wu), tsaics@nchu.edu.tw (C.-S. Tsai), cyf@cs.ccu.edu.tw (Y.-F. Chang), ypchu@thu.edu.tw (Y.-P. Chu).

0031-3203/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2008.05.031

Table 1
Share blocks of the (2, 2)–VSS scheme

Secret pixel color	White						Black					
Share blocks												
2 × 2 block of the first share	▚	▞	▐	▌	▀	▄	▚	▞	▐	▌	▀	▄
2 × 2 block of the second share	▚	▞	▐	▌	▀	▄	▞	▚	▌	▐	▄	▀
Stacked 2 × 2 block	▚	▞	▐	▌	▀	▄	█	█	█	█	█	█



Original secret image

First share image

Second share image

Stacked result of (a) and (b)

Fig. 1. An example of the (2, 2)–VSS scheme: (a) Original secret image. (b) First share image. (c) Second share image. (d) Stacked result of (a) and (b).

In addition, Chen et al. proposed a scheme to make the decryption result significant only at a desired stacking angle [30]. But all of the above schemes aim to deal with only one secret image. Participants have to possess lots of share images for different secret images during transmissions. This property results in inefficiency, so some researchers made effort to hide more secret images into two share images [31,32]. Unfortunately, the existing visual secret sharing schemes restrict the number of secret images.

To extend the number of secret images, this paper proposes a novel visual secret sharing scheme for hiding multiple secret images into two share images. The proposed scheme analyzes the secret pixels and the corresponding share blocks to construct a stacking relationship graph, in which the vertices denote the share blocks and the edges denote two blocks stacked together at the desired decryption angle. According to this graph and the pre-defined visual pattern set, two share images are generated. Unlimited secret images can be hidden (encrypted) such that each secret image can be obtained (decrypted) by stacking these two share images at the corresponding angle. The security of secret images can be also guaranteed since no secret information will leak out in any share image.

The remainder of this paper is organized as follows. In Section 2, the related works of visual cryptography are briefly reviewed. The proposed scheme is introduced in Section 3. Thereafter, the experimental results and comparisons are shown in Section 4. Finally, the Conclusions and future works are provided in the last section.

2. Visual cryptography for multiple secret images

The basic concept of visual cryptography is introduced in Section 2.1. Then the existing visual secret sharing schemes for multiple secret images are introduced in Sections 2.2 and 2.3.

2.1. Threshold visual secret sharing

Naor and Shamir first proposed a (k, k)-threshold visual secret sharing scheme to share a secret image [12]. In this scheme, a secret image is hidden into k share images for participants and can be decrypted only by all the share images. This scheme not only provides the frontiers of visual cryptography but also inspires researchers to develop various visual secret sharing schemes for more flexible applications, various kinds of secret images, meaningful share images, and so on.

Table 2
Constructing rules of Chen and Wu's scheme

The two secret pixels before–after rotation	White–White	White–Black	Black–White	Black–Black
Blocks				
Share block 1	▛	▛	▛	▛
Share block 2	▀	▌	▐	▄
Stacked block	▛	▛	█	█
Stacked block for 90° rotated share block 1	▜	█	▜	█

The (2, 2)–VSS scheme is illustrated to introduce the basic concepts of threshold visual secret sharing schemes. In the encryption process, every secret pixel is turned into two blocks, and each block belongs to the corresponding share image. At last, two share images are obtained. In the decryption process, two corresponding blocks are stacked together to retrieve the secret pixel. Two share blocks of a white secret pixel are the same while those of a black secret pixel are complementary as listed in Table 1. Consequently, a white secret pixel is represented by a block with the stacked result of half white sub-pixels, and a black secret pixel is all black. An example of the (2, 2)–VSS scheme is shown in Fig. 1, where the share images are 2 × 2 times larger than the original secret image.

The disadvantage of conventional visual secret sharing schemes is that only one secret image is hidden at a time, and numerous share images have to be generated and maintained for multiple secret images.

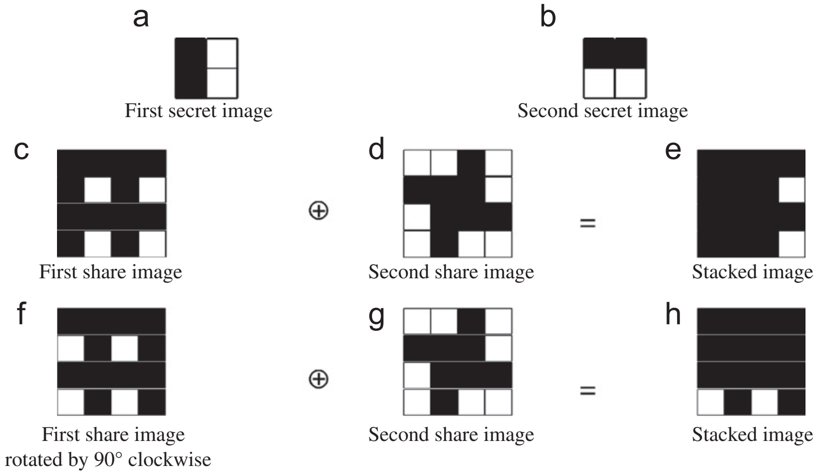


Fig. 2. An example of Chen and Wu's scheme: (a) First secret image. (b) Second secret image. (c) First share image. (d) Second share image. (e) Stacked image. (f) First share image rotated by 90° clockwise. (g) Second share image. (h) Stacked image.

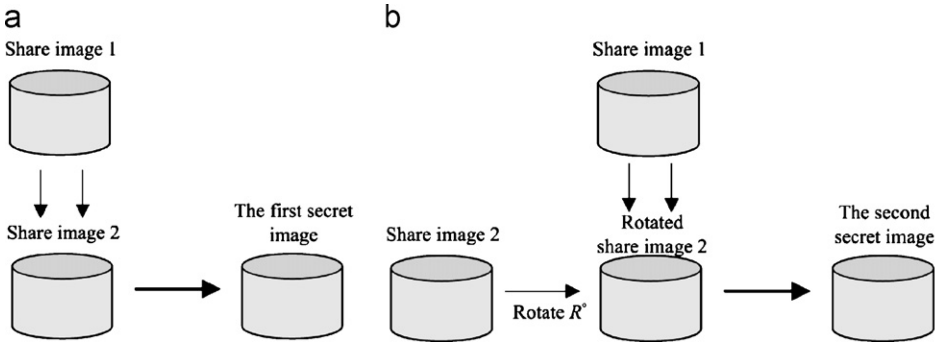


Fig. 3. The decryption method of rings: (a) Stacking for the first secret image. (b) Stacking for the second secret image.

2.2. Chen and Wu's visual secret sharing scheme for two secret images

Chen and Wu proposed a (2, 2)-threshold visual secret sharing scheme for two secret images [31]. The first secret image is decrypted by only stacking two share images. The second secret image is decrypted also by stacking two share images while one share image is rotated. The rotating angle can only be 90°, 180°, or 270° such that the images are in rectangular form.

Each secret pixel P_i is turned into two share blocks b_1^i and b_2^i sized 2×2 for the two share images S_1 and S_2, respectively. There is only one white sub-pixel in all b_1^i's. Let p_i denote the corresponding position of the white sub-pixel in b_1^i and p_i' denote the corresponding position of the white sub-pixel in b_1^i after rotation. For example, if the second secret image is decrypted by rotating the first share image 90° clockwise and p_i is bottom right as shown on the first row of Table 2, p_i' is bottom left. The encryption process first sets the two sub-pixels of b_2^i in positions p_i and p_i' according to the corresponding secret pixels' colors, and it then sets the other sub-pixels' colors arbitrarily to make the block b_2^i half black and white. In the example, if the secret pixels are both white before and after rotation, sub-pixels of b_2^i in positions p_i and p_i' (the bottom sub-pixels) are white and the others (the upper sub-pixels) are black in b_2^i. Therefore, a white sub-pixel appears in the stacking results both before and after rotation. In the decryption process, the stacked result of b_1^i and b_2^i are decided according to the colors of the sub-pixels colors in positions p_i and p_i'. An example of Chen and Wu's scheme is illustrated in Fig. 2. Chen and Wu's scheme successfully hides two secret images into two share images. However, the rotating angle is fixed to be 90°, 180°, or 270°. Moreover, this scheme is unable to share more than two secret images into two share images.

2.3. The ring shadow image technology

To overcome the angle restriction of Chen and Wu's scheme, Hsu et al. proposed another scheme to hide two secret images in two share images with arbitrary rotating angles [32]. Their scheme rolls up the share images to become rings so that it is easy to rotate the share image at any desired angle as shown in Fig. 3.

Since each row of the share images is independent of other rows, Hsu et al.'s scheme encrypts one row at a time. Every secret pixel is turned into share blocks sized 2×2. Assume that the second secret image is decrypted with an $R°$ rotated share image, where R is a factor of 360. In the following, the decryption process is shown. Stacking the block at angle $(i \times R)°$ of the first share image and the block at angle $(i \times R)°$ of the second share image can obtain the information of the first secret image at angle $(i \times R)°$. Stacking the block at angle $((i+1) \times R)°$ of the first share image and the block at angle $(i \times R)°$ of the second share image can produce the information of the second secret image at angle $(i \times R)°$.

Therefore, each row can be separated into several sets according to the stacking relations. For the first set, there are positions at angles of $0°, R°, 2R°, \ldots, (360-R)°$. The positions of the second set are the positions right next to those of the first set, and vice versa for other sets. The pixel processing order of a set is interactive in the two secret images and from the starting angle to the end angle, as shown

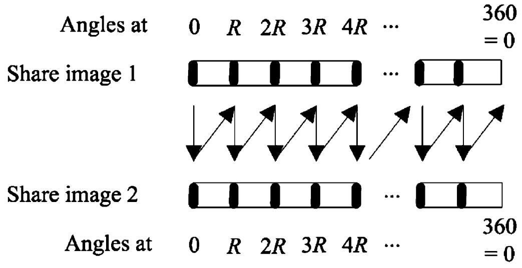


Fig. 4. Processing order of secret pixels.

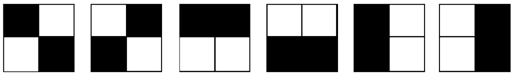


Fig. 5. Six possible initial share blocks.

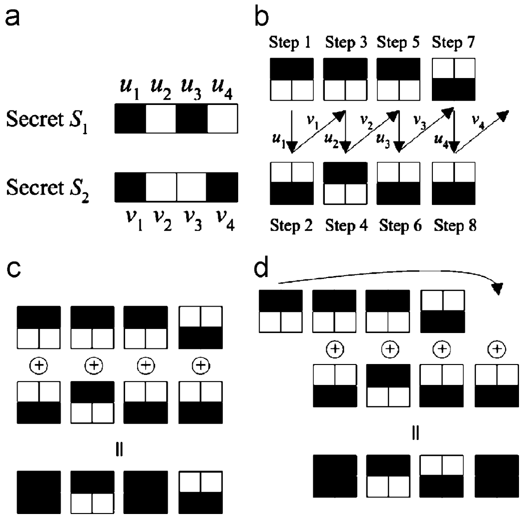


Fig. 6. An example of the ring shadow image technology: (a) The two secret images. (b) The encryption process with $R=90$. (c) Decryption for the first secret image. (d) Decryption for the second secret image.

in Fig. 4. And the whole processes can be separated into three major parts.

Step 1: An arbitrary block is initially selected from the six possible blocks in Fig. 5 to fill the share block at 0° in the first share image.

Step 2: The current processing share block is constructed according to the previous block and the decision rule that two share blocks are identical if the corresponding secret pixel is white, or the two share blocks are complementary if the pixel is black.

Step 3: Repeating the above Step 2 for all sets and all rows to get the share images.

An example of two secret images sized 1×4 and R equal to 90 is shown in Fig. 6. The first share block, in which the two upper subpixels are black and the bottoms are white, is randomly selected. Followed by the first block, there are total eight steps to decide all the blocks listed in Fig. 6(b). The two stacking results are listed in Figs. 6(c) and (d).

This ring scheme overcomes the angle restriction, and the decrypted secret images of this scheme is better than Chen and Wu's scheme since the difference between black and white stacked blocks are larger. However, the number of secret images remains limited. Therefore, a novel visual secret sharing scheme is proposed in this paper for arbitrary number of secret images to further explore this research area.

3. The proposed scheme

In order to share multiple secret images in two share images, a novel scheme is proposed to hide m secrets and to reveal the secrets by stacking the share images at m aliquot angles, respectively. The proposed scheme is a 2-out-of-2 m-way extended visual secret sharing scheme for m secret images, denoted as a (2, 2)-m-VSSM scheme. Before constructing the two share images, the stacking rules and the relationship between these two share images must be indicated. Then the proposed scheme can be developed according to the relation of share images afterwards.

3.1. *The decryption model of the proposed scheme*

The most important feature of visual cryptography is the computation-free decryption process. The proposed scheme employs the image stacking method of the ring shadow image technology, mentioned in Section 2.3, and extends it to support the decryption for the m secret images. In the encryption process, a relationship graph for the share images is first constructed. Then the share images are generated according to this graph. The share image generation process can be divided into sub-processes for each set of every row, and the flowchart of it is shown in Fig. 7. For clarity, the details are introduced in the following section.

In the decryption process, the share images are rolled into rings and the first secret image is revealed by stacking the share images. The second secret image is revealed by rotating the inner share image anticlockwise $360/m°$. The third secret is revealed by rotating the inner share image anticlockwise $2\times 360/m°$ and so on. That is, each secret image can be obtained by stacking two share images with the inner share image rotated anticlockwise at the corresponding angle, and this decryption model is shown in Fig. 8.

3.2. *The encryption process of the proposed scheme*

In a (2, 2)-m-VSSM scheme, secret images are revealed at m aliquot angles. Assume that the secret images $S_1, S_2, \ldots, S_m$ are all sized $X\times Y$, where X is a multiple of m.

3.3. *Construction of the relationship graph*

From the properties of the decryption model, each row of the images is independent of other rows. Thus the proposed scheme encrypts one row at a time. For the first row, collect blocks in the positions of two share images at angles

$$0, \frac{360^\circ}{m}, \frac{360^\circ}{m}\times 2, \ldots, \frac{360^\circ}{m}\times(m-1)$$

to form a graph. Note that the share blocks have not been generated at present. In this graph, vertexes denote the share blocks in the positions, and the edges denote the relation between the two blocks when they meet (or are stacked) at some angle. Since secrets can be decrypted at all the aliquot angles, every share block is related to all the share blocks in the other share image. Therefore, this graph is a complete bipartite graph $K_{m,m}$. An example of a (2, 2)-3-VSSM scheme is illustrated in Fig. 9, where the corresponding share blocks form a graph $K_{3,3}$. The share blocks belonging to $K_{3,3}$ form a set. Therefore, all the share blocks on a row can be separated to X/m sets. For example, if the two secret images are sized 300×300, then there are 100 sets for each row, and are total 30,000 sets.

Without loss of generality, $a_1^p, a_2^p, \ldots, a_m^p$ denote the m blocks of the p-th set in the first share image S_A, and $b_1^p, b_2^p, \ldots, b_m^p$ denote the m blocks of the p-th set in the other share image S_B.

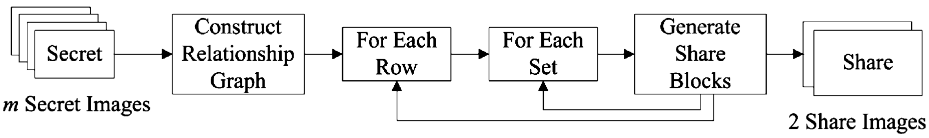


Fig. 7. The flowchart of the proposed share image generation process.

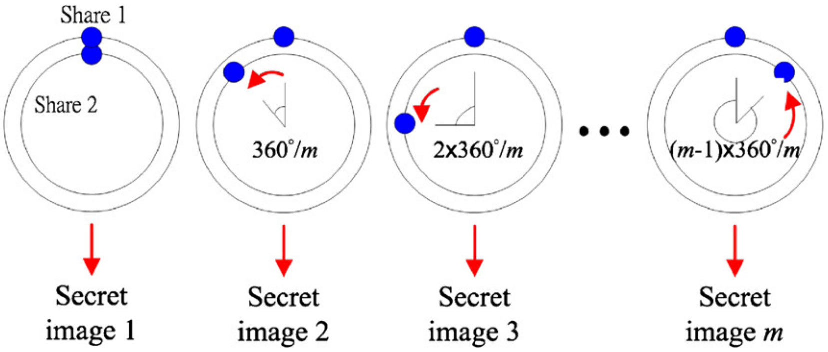


Fig. 8. The decryption model of the proposed scheme.

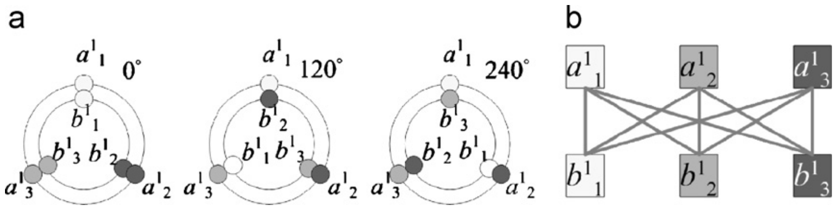


Fig. 9. An example of the proposed (2, 2)-3-VSSM model: (a) Decryption of a (2, 2)-3-VSSM model. (b) Relationship graph of a set of blocks.

Table 3
Necessary relations between visual patterns

Stacking operations	Block of results
$P_e \oplus P_W$	White
$P_e \oplus P_B$	Black
$P_i \oplus P_W$	Black
$P_i \oplus P_B$	Black

3.4. Generation of a set of share blocks

In the (2, 2)-m-VSSM scheme, each share block is filled by using m visual patterns. Let $a^p_{i,j}$ denote the j-th pattern of the share block a^p_i and $b^p_{i,j}$ denote the j-th pattern of b^p_i. In the p-th sub-process, the proposed scheme first fills $a^p_{i,i}$ with effective visual pattern P_e for all i and fills $a^p_{i,j}$ with ineffective visual patterns P_i for all $i \neq j$. Then $b^p_{i,j}$ is filled with the white pattern P_W if $S_{1+((i-j)\bmod m)}(r,p+(j-1)X/m)=0$; otherwise, $b^p_{i,j}$ is filled with the black pattern P_B, where $S_i(x,y)$ is the secret pixel of the i-th secret S_i on row x and column y, and r is the index of the current row.

3.5. Properties of the visual patterns

The visual patterns P_e, P_i, P_W, and P_B are used to produce some special features. As shown in Table 3, the effective visual pattern P_e will reveal meaningful stacking results visual patterns P_W and P_B while the ineffective visual pattern P_i will always cause black blocks. Any set of visual patterns satisfying these properties can be selected in the proposed scheme.

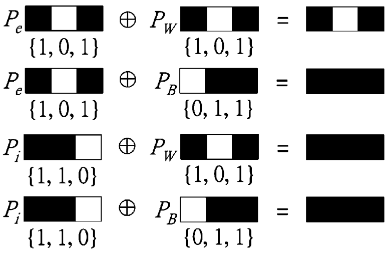


Fig. 10. Stacking results of the chosen visual patterns.

After testing various visual patterns, $P_e=\{1,0,1\}$, $P_i=\{1,1,0\}$, $P_W=\{1,0,1\}$, and $P_B=\{0,1,1\}$ are chosen in the proposed scheme, where "1" denotes a black pixel and "0" denotes a transparent (white) pixel. It is simple to verify that the selected visual patterns satisfy the requirements of the proposed scheme in Fig. 10.

3.6. Pixel-wise sub-process of the proposed scheme

For every fixed i, the stacking result of a^p_i and b^p_j reveals the color of $b^p_{j,i}$, because only $a^p_{i,i}$ is effective. Therefore, when two share images are stacked at $r \times 360/m^\circ$ for $0 \leqslant r < m$, a^p_i reveals the i-th pattern's color in the corresponding share block, which is decided by the corresponding secret pixel of the r-th secret image. Consequently, every secret image is decrypted at its own stacking angle.

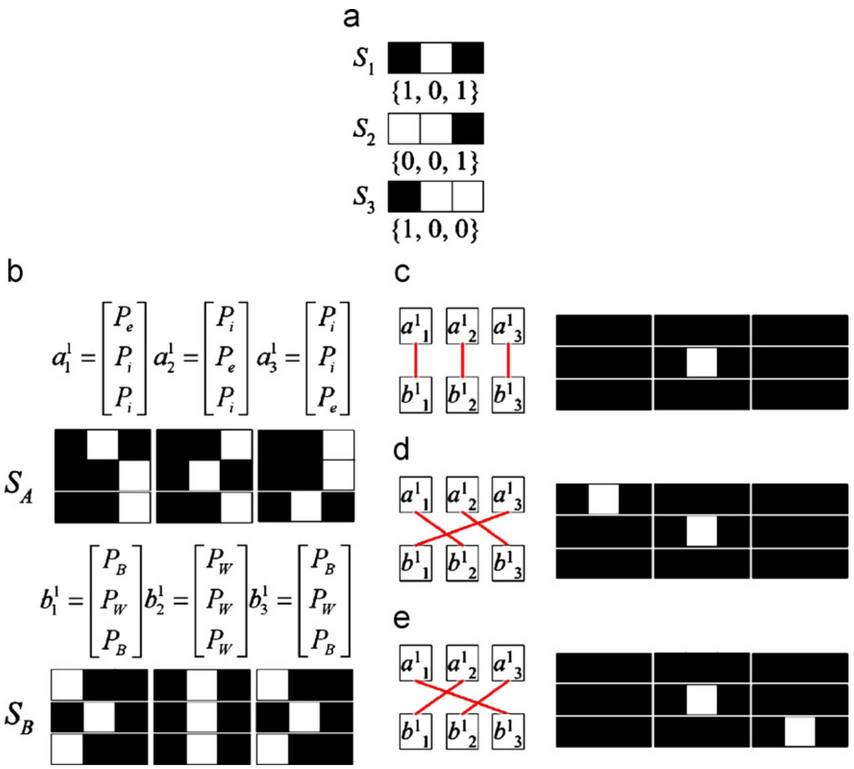

a
S_1
{1, 0, 1}
S_2
{0, 0, 1}
S_3
{1, 0, 0}
b
$a_1^1 = [P_e, P_i, P_i]$ $a_2^1 = [P_i, P_e, P_i]$ $a_3^1 = [P_i, P_i, P_e]$
S_A
$b_1^1 = [P_B, P_W, P_B]$ $b_2^1 = [P_W, P_W, P_W]$ $b_3^1 = [P_B, P_W, P_B]$
S_B
c
a^1_1 a^1_2 a^1_3
b^1_1 b^1_2 b^1_3
d
e

Fig. 11. An example of the (2, 2)-3-VSSM scheme: (a) The target secret images. (b) The generated share images. (c) The stacking secret image at normal degree. (d) The stacking secret image at 120°. (e) The stacking secret image at 240°.

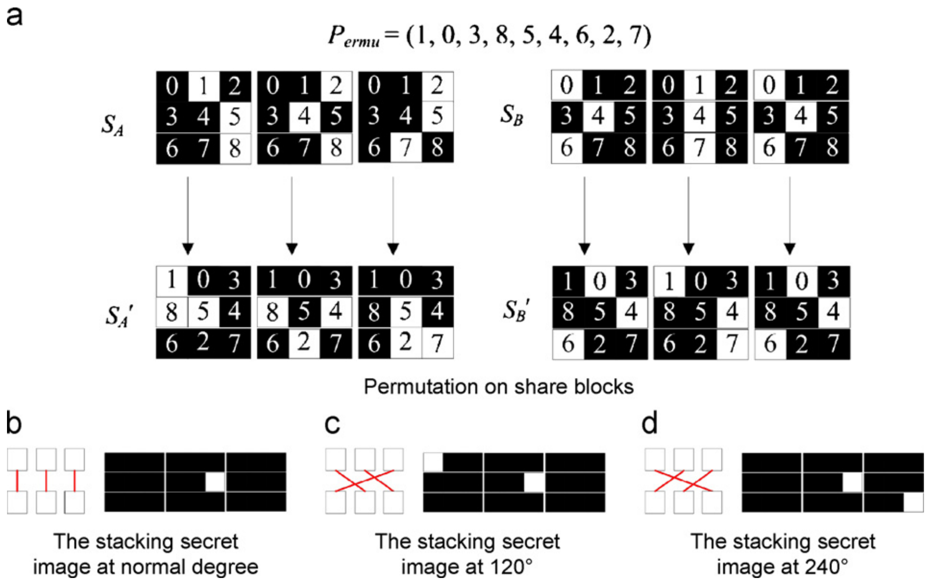

a
$P_{ermu} = (1, 0, 3, 8, 5, 4, 6, 2, 7)$
S_A
0 1 2
3 4 5
6 7 8
S_B
S_A'
1 0 3
8 5 4
6 2 7
S_B'
Permutation on share blocks
b
c
d
The stacking secret image at normal degree
The stacking secret image at 120°
The stacking secret image at 240°

Fig. 12. The example of the (2, 2)-3-VSSM scheme with permutation: (a) Permutation on share blocks. (b) The stacking secret image at normal degree. (c) The stacking secret image at 120°. (d) The stacking secret image at 240°.

Although the encryption is according to the above relationship graph, we can further formalize this relationship to speed up the shares construction process. For the p-th process on the r-th row, a_i^p and b_i^p are generated for all i according to the following equations. Therefore, when these two equations are used, the sub-routine of constructing relationship graph in Fig. 7 is replaced in each calculating sub-processes.

$$a_{i,j}^p = \begin{cases} P_e & \text{if } i = j, \\ P_i & \text{if } i \neq j. \end{cases} \tag{1}$$

$$b_{i,j}^p = \begin{cases} P_W & \text{if } S_{1+((i-j) \bmod m)}\left(r, p + \dfrac{(j-1)X}{m}\right) = 0, \\ P_B & \text{else.} \end{cases} \tag{2}$$

Thus for each row, it needs to repeat the sub-processes X/m times for $p = 1, 2, \ldots, X/m$. Note that in a single sub-process, a_i^p is the block on the $(p + (i-1)X/m)$-th column of the share image S_A and b_i^p is the block on the $(p + (i-1)X/m)$-th column of the share image S_B. After repeating the sub-processes for all rows, the share images are obtained.

Table 4
Comparisons of visual secret sharing schemes for multiple secrets

Schemes	Chen and Wu's scheme [31]		Hsu et al.'s scheme [32]		The proposed scheme	
No. of secrets	Contrast	Expanding size	Contrast	Expanding size	Contrast	Expanding size
2	1/4	4	1/2	4	1/6	6
3	N/A	N/A	N/A	N/A	1/9	9
4	N/A	N/A	N/A	N/A	1/12	12
m	N/A	N/A	N/A	N/A	$1/3m$	$3m$

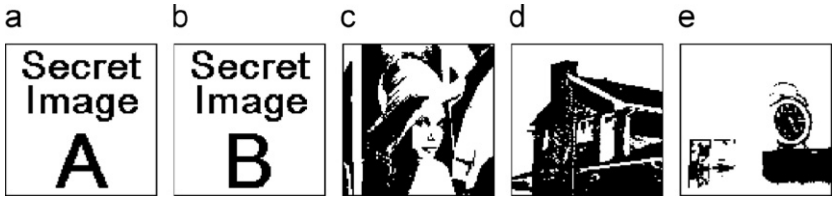


Fig. 13. Secret images: (a) Secret image 1. (b) Secret image 2. (c) Secret image 3. (d) Secret image 4. (e) Secret image 5.

3.7. Example

A simple example of the (2, 2)-3-VSSM scheme is illustrated in Fig. 11, where 0°, 120°, and 240° can reveal secret images $S_1 = [1\ 0\ 1]$, $S_2 = [0\ \ 0\ \ 1]$, and $S_3 = [1\ \ 0\ \ 0]$, respectively. There is only one sub-process needed with $r=1$ and $p=1$. According to Eq. (1), $a_1^1 = [P_e P_i P_i]$, $a_2^1 = [P_i P_e P_i]$, and $a_3^1 = [P_i P_i P_e]$.

From Eq. (2), $b_{1,1}^1$ is P_B since $S_1(1,1)$ is black, $b_{1,2}^1$ is P_W since $S_3(1,2)$ is white, and $b_{1,3}^1$ is P_B since $S_2(1,3)$ is black. As a result, $b_1^1 = [P_B P_W P_B]$. After performing the same process for b_2 and b_3, $b_2^1 = [P_W P_W P_W]$ and $b_3^1 = [P_B P_W P_B]$ are gotten.

After using the selected visual patterns to substitute for share images, $a_1^1 = [101110110]$, $a_2^1 = [110101110]$, $a_3^1 = [110110101]$, $b_1^1 = [011101011]$, $b_2^1 = [101101101]$, and $b_3^1 = [011101011]$ can be obtained. The results using a_i^1 and b_i^1 for $i = 1, 2, 3$ to generate the share images are shown in Fig. 11.

3.8. Breaking the fixed patterns

The last part of the sub-process is using random permutation for every block to break up the regular pixel distribution. For the above example, let a random permutation be applied to the blocks. Then the pixel positions in a single share image are no longer related to the secrets. In other words, the share images do not suffer from the false contour problem. Meanwhile, the secrets can still be decrypted by stacking the share images as shown in Fig. 12.

Algorithm (*Encryption Process of (2, 2)-m-VSSM*).

Input: Secret images $S_1, S_2, \ldots, S_m$

Output: Two share images S_A, S_B

Step 1: Adjust the size of all secret images to $X \times Y$ that the X must be a multiple of m.

Step 2: Initialize the processing row $r = 1$ of the images.

Step 3: Start the p-th process of the proposed scheme with $p = 1$.

Step 4: Select the $1, m+1, 2m+1, \ldots, X-m+1$ secret pixels to generate the blocks $a_1^p, a_2^p, \ldots, a_m^p$ and $b_1^p, b_2^p, \ldots, b_m^p$ according to Eqs. (1) and (2). Note that Eqs. (1) and (2) are inducted from the relationship graph and substitute the graph.

Step 5: Perform permutation on generated blocks $a_1^p, a_2^p, \ldots, a_m^p$ and $b_1^p, b_2^p, \ldots, b_m^p$.

Step 6: Fill the blocks in the shareimages such that a_i^p is the block on the r-th row and $(p + X(i-1)/m)$-th column of share image S_A and b_i^p is the block on the r-th row and $(p + X(i-1)/m)$-th column of share image S_B.

Step 7: If $p < X/m$, return to Step 4 for the next process $p := p + 1$.

Step 8: If $r < Y$, return to Step 3 for the next row $r := r + 1$.

Step 9: Out put the two share images S_A and S_B.

4. Comparisons and experimental results

For visual secret sharing schemes, there are two evaluation terms: expanding size and contrast. Expanding size is the ratio of the share image size over the original secret image size, and the smaller number means a better performance. In Naor and Shamir's (2, 2)–VSS scheme, the expanding size is 4 since each secret pixel becomes a share block with 4 sub-pixels. Contrast is the difference between the revealed black and white secret pixels. The larger contrast indicates that it is easier to distinguish the decrypted secret pixels. The contrast of Naor and Shamir's (2, 2)–VSS scheme is 1/2 since there is half white sub-pixels in a white stacked block and all black sub-pixels in a black stacked block.

In the encryption process, every share block is filled with m visual patterns and the two share images are $3m$ (that is, $m \times$(pattern size)) times larger than the original secret image. The contrast of the proposed scheme is $1/3m$ because there is one transparent sub-pixel in a white stacked block and fully opaque in a black stacked block. Compared with the other schemes, Chen and Wu's scheme [31] and Hsu et al.'s scheme [32] both expand a secret pixel to four sub-pixels. There is only one white sub-pixel in a stacked white block in Chen and Wu's scheme, and there are two white sub-pixels in Hsu et al.'s scheme. Although the proposed scheme does not perform as well as the previous ones for two secret images, it can deal with more than two secrets while the existing schemes cannot. Table 4 lists the comparisons of the schemes, where both Chen and Wu's scheme [31] and Hsu et al.'s scheme [32] cannot handle more than two secrets.

A (2, 2)-5-VSSM scheme experiment is provided to demonstrate the results of the proposed scheme. In Fig. 13, the first two secret images are text images and the other three images are binary images, where all the secrets are sized 100 × 100. Though the expanding size is 15 (that is, 3 × 5) in the proposed scheme, one sub-pixel was wasted to make the block become square. As a result, the size of share blocks was increased to 4×4, and the additional sub-pixel was left black in this experiments. The share images are shown in Figs. 14(a) and (b), and the stacked results of the proposed scheme are shown in Figs. 14(c)–(g).

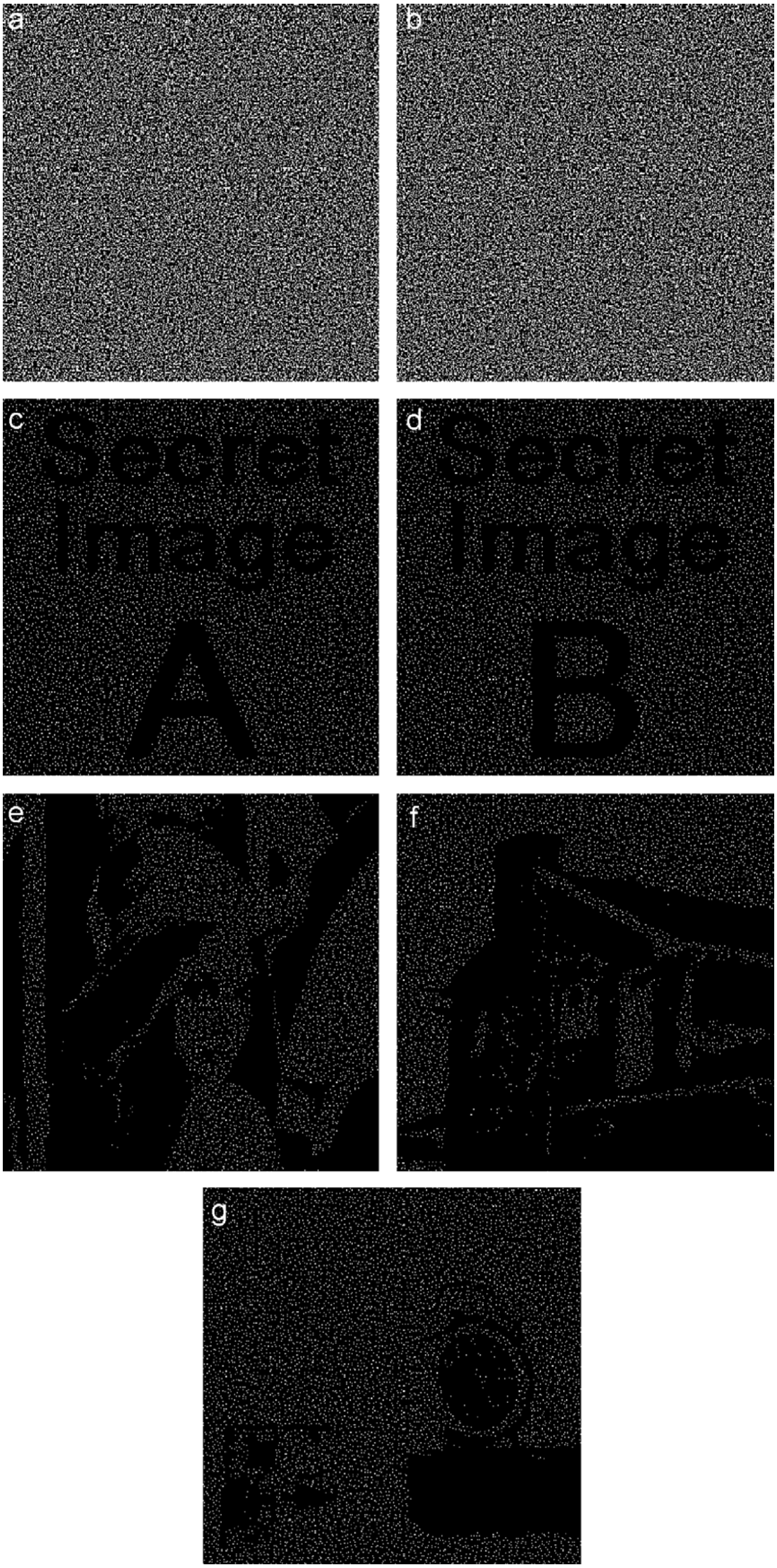


Fig. 14. A (2, 2)-5-VSSM scheme experiment: (a) Share image 1. (b) Share image 2. (c) Revealed secret image with 0° rotated. (d) Revealed secret image with 72° rotated. (e) Revealed secret image with 144° rotated. (f) Revealed secret image with 216° rotated. (g) Revealed secret image with 288° rotated.

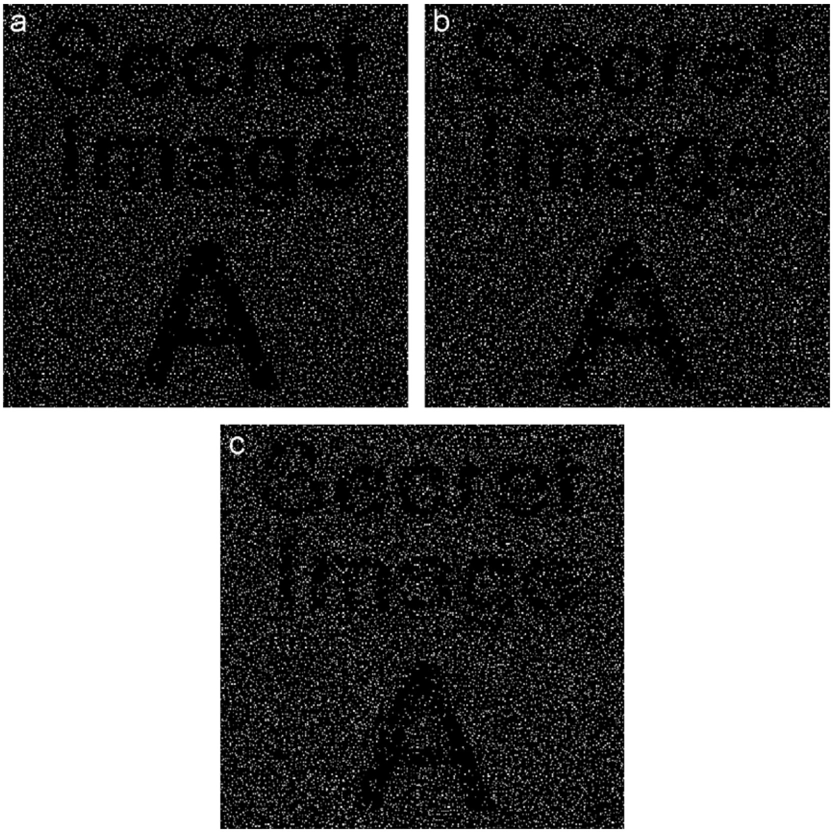


Fig. 15. Stacked results of destroyed shares: (a) The stacked result of the first stacked secret for 5% distortions of Share 2. (b) The stacked result of the first stacked secret for 10% distortions of Share 2. (c) The stacked result of 5% distortions of both shares.

From this experiment, it is obvious that the proposed share images do not leak any secret information from the share images, and all the secret images are decrypted successfully by stacking the share images at the corresponding angles. The proposed scheme not only achieves the desired goals but also improves the efficiency of visual cryptography for numerous secret images.

If the share images are damaged during transmission or reproduction, the results of the stacked secret are also affected. According to the block relationship mentioned in Section 3.2, if a block is distorted, the related secret blocks are all affected. Therefore, the secret distortion ratio is directly related to the share destruct ratio. To show this result, we add 5% and 10% random distortions on the second share image in our experiment, respectively. In addition, 5% random distortions are added to both share images. The stacked results of the first secret images are shown as follows. From these revealed results, it is obvious that the distortions are related to the share noise, and the secret information is still clear enough to be recognized by human vision (Fig. 15).

5. Conclusions and future works

This paper proposes an extended visual secret sharing scheme to share multiple secret images into two share images. The relationship between blocks of share images is modeled first. Then the share images are constructed by using the pre-defined visual patterns. An arbitrary number of different secret images can be hidden in two share images, and they can be decrypted at aliquot stacking angles. From the properties described in Section 4, the visual patterns are directly related to the quality of the decryption results and should be selected carefully.

The decryption angles in the proposed scheme are designed to be aliquot angles so that the relationship graph is able to be constructed, and a designated set of stacking angles is a unique way for the next step. Moreover, extending visual secret sharing schemes of multiple secrets to a general k-out-of-k model is one of the goals.

References

[1] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, vol. 48, NJ, USA, 1979, pp. 313–317.

[2] A. Shamir, How to share a secret, Commun. ACM 22 (1) (1979) 612–613.

[3] C. Blundo, A. De Santis, M. Naor, Visual cryptography for gray-level image, Info. Process. Lett. 75 (2001) 255–259.

[4] C.-C. Chang, H.-C. Wu, A copyright protection scheme of images based on visual cryptography, Imaging Sci. J. 49 (2001) 141–150.

[5] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-P. Chu, A new multi-secret images sharing scheme using largrange's interpolation, J. Syst. Software 76 (2005) 327–339.

[6] C.-S. Tsai, C.-C. Chang, A generalized secret image sharing and recovery scheme, in: Advanced in Multimedia Information Processing-PCM2001, Lecture Notes in Computer Science, Springer, Germany, vol. 2195, 2001, pp. 963–968.

[7] C.-S. Tsai, C.-C. Chang, A new repeating color watermarking scheme based on human visual model, Eurasip J. Appl. Signal Process. 13 (2004) 1965–1972.

[8] C.-S. Tsai, C.-C. Chang, T.-S. Chen, Sharing multiple secrets in digital images, J. Syst. Software 64 (2) (2002) 163–170.

[9] C.-S. Tsai, S.-F. Tzeng, M.-S. Hwang, Improved non-repudiable threshold proxy signature scheme with known signers, Informatica 14 (3) (2003) 393–402.

[10] H.-C. Wu, C.-C. Chang, Hiding digital watermarks using fractal compression technique, Fundam. Inf. 58 (2003) 189–202.

[11] H.-C. Wu, C.-C. Chang, Detection and restoration of tampered JPEG compressed images, J. Syst. Software 64 (2002) 151–161.

[12] M. Naor, A. Shamir, Visual cryptography in: Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Springer, Germany, vol. 950, 1995, pp. 1–12.

[13] W. Koga, On the practical secret sharing scheme, IEICE Trans. Fundam. E84-A (1) (2001) 256–261.

[14] M. Naor, A. Shamir, Visual cryptography II: improving the contrast via the cover base, in: Security Protocols, Lecture Notes in Computer Science, Springer, Germany, vol. 1189, April 1996, pp. 197–202.

[15] D. Stinson, Visual cryptography and threshold schemes, Potentials of IEEE 18 (1) (1999) 13–16.
[16] E.R. Verheul, H.C.A. van Tilborg, Constructions and properties of *k*-out-of-*n* visual secret sharing scheme, Des. Codes Cryptography 1 (2) (1997) 179–196.
[17] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Info. Comput. 129 (2) (1996) 86–106.
[18] M. Iwamoto, H. Yamamoto, The optimal n-out-of-n visual secret sharing scheme for gray-scale images, IEICE Trans. Fundam. E86-A (10) (2003) 2238–2247.
[19] S. Cimato, R. De Prisco, A. De Santis, Optimal colored threshold visual cryptography schemes, Des. Codes Cryptogr. 35 (2005) 311–335.
[20] S. Cimato, R. De Prisco, A. De Santis, Contrast optimal colored visual cryptography schemes, in: Proceedings of 2003 IEEE Information Theory Workshop, Paris, France, March–April 2003, pp. 139–142.
[21] Y.-C. Hou, Visual cryptography for color images, Pattern Recognition 36 (7) (2003) 1619–1629.
[22] T. Ishihara, H. Koga, New constructions of the lattice-based visual secret sharing scheme using mixture of colors, IEICE Trans. Fundam. E85-A (1) (2002) 158–166.
[23] T. Ishihara, H. Koga, A visual secret sharing scheme for color images based on meanvalue-color mixing, IEICE Trans. Fundam. E86-A (1) (2003) 194–197.
[24] H. Koga, An analytic construction for the visual secret sharing scheme for color images, IEICE Trans. Fundam. E84-A (1) (2001) 262–272.
[25] V. Rijmen, B. Preneel, Efficient color visual encryption or shared colors of Benetton, in: EUROCRYPTO'96, Rump Session, Berlin, Germany, 1996.
[26] C.-H. Tang, C.-S. Laih, New colored visual secret sharing schemes, Des. Code Cryptogr. 20 (2000) 325–335.
[27] S. Cimato, A. De Santis, A.L. Ferrara, B. Masucci, Ideal contrast visual cryptography schemes with reversing, Info. Process. Lett. 93 (2005) 199–206.
[28] M. Iwamoto, H. Yamamoto, A construction method of visual secret sharing schemes for plural secret images, IEICE Trans. Fundam. E86-A (10) (2003) 2577–2588.
[29] M. Nakajima, Y. Yamaguchi, Extended visual cryptography for natural images, J. WSCG 10 (2) (2002) 303–310.
[30] T.-S. Chen, J.-H. Shiesh, H.-W. Chen, Using circular shadow image and fixed angle segmentation for visual cryptography system, in: Pan-Yellow-Sea International Workshop on Information Technologies for the Network Era, Saga, Japan, March 2002, pp. 214–220.
[31] L.-H. Chen, C.-C. Wu, A Study on Visual Cryptography, Master Thesis, National Chiao Tung University, Taiwan, ROC, 1998.
[32] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing, in: Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 2004, pp. 996–1001.

About the Author—JEN-BANG FENG was born in Taichung, Taiwan, on January 10, 1978. He received his B.S. and M.S. degrees in the Department of Applied Mathematics in 2001 and 2003, and his Ph.D. degree in Department of Computer Science and Engineering in 2008 from the Chung Hsing University. He is an Assistant Professor of Department of Information Engineering and Informatics of Tzu Chi College of Technique. His current research interests include visual cryptography, secret sharing, data hiding, image processing, and multimedia system.

About the Author—HSIEN-CHU WU was born in Tainan, Taiwan, Republic of China, on October 26, 1962. She received the B.S. and M.S. degrees in Applied Mathematics in 1985 and 1987, respectively, from the National Chung Hsing University, Taichung, Taiwan. She received her Ph.D. in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From 1987 to 2002, she was a lecturer of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. From August 2002 to July 2005, she was an associate professor of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Since August 2005, she has worked as an professor of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Her research interests include image authentication, digital watermarking, data hiding, image processing and information security.

About the Author—CHWEI-SHYONG TSAI was born in Changhua, Taiwan, Republic of China, on September 3, 1962. He received his B.S. degree in Applied Mathematics in 1984 from the National Chung Hsing University, Taichung, Taiwan. He received his M.S. degree in Computer Science and Electronic Engineering in 1986 from the National Central University, Chungli, Taiwan. He received his Ph.D. degree in Computer Science and Information Engineering in 2002 from the National Chung Cheng University, Chiayi, Taiwan. In August 2002, he received his tenure as associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Since August 2004, he is an associate professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. His research interests include image watermarking, image authentication, information hiding, bio-information and E-learning.

About the Author—YA-FEN CHANG received her B.S. degree in Computer Science and Information Engineering from National Chiao Tung University, Hsinchu, Taiwan in 2000. She received her Ph.D. degree in Computer Science and Information Engineering in 2005 from National Chung Cheng University, Chiayi, Taiwan. Since 2006, she has been an Assistant Professor of National Taichung Institute of Technology. Her current research interests include electronic commerce, information security, cryptography, and mobile communications.

About the Author—YEN-PING CHU is a Professor of the Computer Science and Information Engineering and Head of the Library of Tung Hai University, Taichung, Taiwan. His research interests include high-speed networks, operating system, neural network, and computer assistant learning.