Information Sciences 189 (2012) 255–265

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

Multi-image encryption by circular random grids

Tzung-Her Chen *, Kuang-Che Li

Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan

ARTICLE INFO

Article history:
Received 22 May 2009
Received in revised form 9 February 2011
Accepted 12 November 2011
Available online 22 November 2011

Keywords:
Visual secret sharing
Visual cryptography
Random grids
Multi-secret

ABSTRACT

Visual secret sharing (VSS) can encode a secret image into several share images where the original secret can be reconstructed and recognized by sight by stacking all share images. There are two categories of VSS schemes: visual cryptography (VC) and random grids (RG). VC has three main drawbacks: the large size, the need for the codebook to be redesigned for specific applications, and the ability to encode only one secret image at a time. RG removes the first two drawbacks. This paper proposes a novel RG-based VSS scheme that encodes multiple secret images at a time. The scheme encrypts multiple secret images into two circular cipher-grids and decrypts the images by stacking two circular cipher-grids to obtain the first secret and gradually rotating one circular cipher-grid at a fixed degree (based on the quantity of the secret images encrypted) to disclose other secrets. Compared with conventional VC-based VSS, the proposed scheme has no pixel expansion, a higher capacity for secret sharing, and no need for a complex VC codebook to be redesigned. Theoretical analysis of visual quality and security is demonstrated.

1. Introduction

Naor and Shamir [11] proposed a now well-known VSS scheme, visual cryptography (VC), in which a binary secret image is encrypted into two share images composed of disordered transparent and opaque pixels printed onto transparencies. The secret message is decrypted by directly stacking the two transparencies, so this decryption method required only the human visual system to distinguish the recovered secret. Naor and Shamir used encryption-matrices (codebook) composed of 0/1 (“0” for transparent, “1” opaque) to generate two meaningless and noise-like share images, with every original pixel expanded to become $n \times n$ sub-pixels (with the codebook to decide n) so that the size of each share image is expanded to $n \times n$. A 2×2 block produces two black and two white sub-pixels randomly (Table 1: white for “transparent,” black for “opaque”). We generate share image A, composed of equal numbers of black and white sub-pixels.

We transform the secret message into a one-dimension array of 0 and 1. Then, using the 2×2 block of the first share image A and the corresponding secret pixel of the array, we obtain the second share image B. If the value of a secret pixel is 0, we have a block with 2 black and 2 white sub-pixels after stacking two identical corresponding 2×2 blocks in share images A and B. Otherwise, we have the block with 4 black sub-pixels. Fig. 1 provides an example.

When share images A and B are collected, the secret image is recovered by stacking them correctly, as in Fig. 2.

Although the VC-based VSS scheme suffers from image expansion and the need for codebook redesign, and increasing number of researchers have applied VC to VC-related work, such as image encryption [8], image hiding [1,6], and visual identification [10], so VC-based VSS has played an important role in multimedia security.

Conventional VC encrypts only one secret image at a time [16,17], but many researchers [2,7,14,15] have worked on methods to encrypt more than one secret image at a time. Wu and Chang [15] proposed a novel multiple-secret-sharing

[*] Corresponding author. Fax: +886 5 2717741.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.11.026

Table 1
The codebook with 2 × 2 blocks based on visual cryptography.

The pixels of the	white □						black ■					
share *A*	▀	▄	▌	▐	▚	▞	▀	▄	▌	▐	▚	▞
share *B*	▀	▄	▌	▐	▚	▞	▄	▀	▐	▌	▞	▚
Stacking	▀	▄	▌	▐	▚	▞	█	█	█	█	█	█

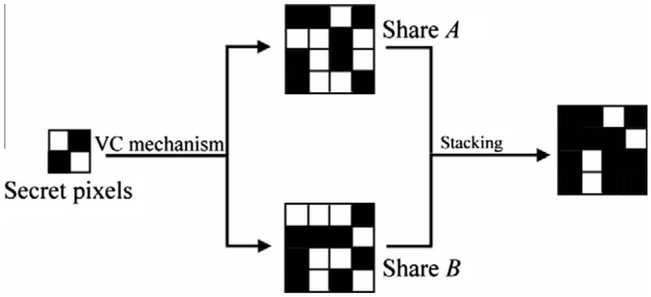

Fig. 1. Mechanism of VC and stacking.

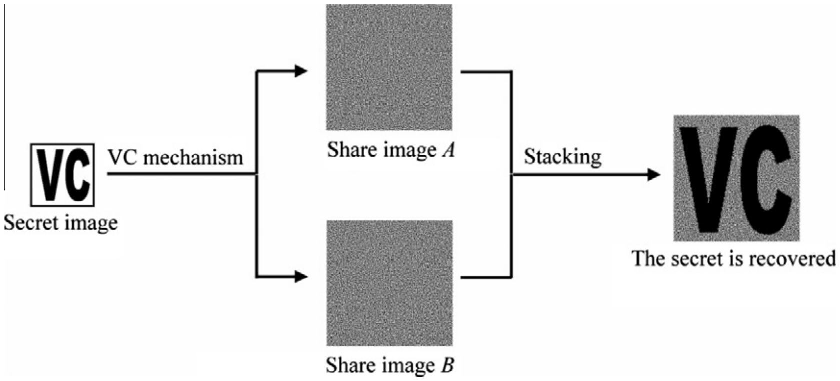

Fig. 2. A simple flowchart of visual cryptography.

scheme by creating two circular share images with two secret images encrypted. Shyu et al. [14] proposed a new VC scheme to encrypt a set of $m \geq 2$ secrets into two circle shares so that m secrets can be disclosed one by one by stacking one share and another rotated share with m different rotation angles while introducing the pixel expansion ratio $2 \times m$. Chen et al. [2] proposed the technique of using a circular share image in which 360 stacking types are designed to stack the multiple share images hidden in outer and inner rings. Hsu et al. [7] proposed a new circular VC scheme in which a flipping operation is added to the rotation operation in order to hide more secrets. Unfortunately, the aforementioned multi-secret VC schemes have many of the same problems as conventional VC.

To solve the problems of image expansion and sophisticated codebook generation inherent in VC, Kafri and Keren [9] proposed the VSS method known as random grids (RG) [4,12,13]. With this method, the binary secret image is turned into two meaningless cipher-grids that are the same as the original secret image, and the decryption operation is similar to that of VC. Shyu [12] extended the capability of encoding binary images to gray-level or color secret images. Kafri and Keren's and

Shyu's schemes are 2-out-of-2 VSS. In 2008, Chen and Tsao [4] and Shyu [13] proposed their own enhanced RG-based VSS to encrypt the secret into n ($n \geqslant 2$) cipher-grids without pixel expansion or the need for an additional codebook, called (n,n) RG-based VSS. Later, Chen and Tsao [5] presented their $(2,n)$ RG-based VSS.

To boost the capability of multiple secret sharing, Chen et al. [3] proposed the multi-secret VSS technique by rotating random grids to encrypt two secret images. These rectangular cipher-grids allow up to four angle rotating types to superimpose the grids.

This paper presents a new scheme that combines the techniques of circular VC [2,7] and random grids to generate circular cipher-grids, thereby attaining the goal of sharing multiple secret images without pixel expansion or the need for codebook generation. This is the first attempt to benefit from combining circular VC-based and conventional RG-based VSS to form a new one capable of encrypting more than two secret images without producing pixel expansion.

This paper is organized as follows. Section 2 briefly reviews the main technique of conventional VSS by random grids. Section 3 introduces the proposed scheme. Further discussions and theoretical analysis are given in Section 4. Section 5 shows the experimental results. Section 6 concludes the article.

2. Conventional random grid based VSS

Kafri and Keren [9] introduced the concept of *random grids* into visual binary image secret sharing, in which a random grid is regarded as a transparency with a two-dimensional array of pixels. Each pixel is either transparent or opaque. Each pixel is chosen by a random procedure in which there is no relationship among the pixels. According to random probability, the number of transparent pixels is probabilistically equal to that of the opaque pixels in the random grid, also called the cipher-grid.

Definition 1 (*Average light transmission*). For a certain pixel b in a binary image B, the *light transmission* of a white (black) pixel is defined as $t(b) = 1$ ($t(b) = 0$). For B with size $h \times w$, the average light transmission of B is defined as $T(B) = \frac{1}{h \times w}\sum_{i=1}^{h}\sum_{j=1}^{w} t(b[i,j])$.

Therefore, in Definition 1, the *average light transmission* of a cipher-grid is 1/2. We assume that G is a cipher-grid and that the average light transmission of G is defined as $T(G) = 1/2$. Considering pixel g in G, the probability that g is transparent or opaque is $Prob(g = 0) = Prob(g = 1) = ½$ ("0" for transparent; "1" for opaque), and we call g a *random pixel* in G.

Let G_1 and G_2 be two independent cipher-grids of the same size. When G_1 and G_2 are superimposed pixel by pixel, each pixel g_1 (transparent or opaque) in G_1 is stacked by a transparent or opaque pixel g_2 in G_2 if g_1 and g_2 are in the counter-position of G_1 and G_2. Let "$\oplus$" denote the generalized "bit-wise OR" operation, which describes the relationship of the superimposition of g_1 and g_2 (Table 2).

When both pixels are transparent (Table 2), the stacked result is transparent, but all other combinations are opaque. Thus, the light transmission of the superimposition of g_1 and g_2 is 1/4.

Kafri and Keren [9] proposed three different algorithms for encrypting binary images by random grids: the first algorithm (RGVSS) is cited without losing generality.

```
Algorithm RGVSS
Input: A binary secret image $S = \{S(i,j) | S(i,j) = 0 \text{ or } 1, 0 \leqslant i < w, 0 \leqslant j < h\}$
Output: Two cipher-grids $G_k = \{G_k(i,j) | G_k(i,j) = 0 \text{ or } 1, 0 \leqslant i < w, 0 \leqslant j < h\}$, where $k$ = "1" or "2"
1. For ($i$ and $j$, $0 \leqslant i < w$ and $0 \leqslant j < h$)//, generate a random grid $G_1$ and $T(G_1) = 1/2$
   $G_1(i,j)$ = random_pixel(0,1)//, and random_pixel(0,1) represents "randomly generating '0' or '1'"
2. For ($i$ and $j$, $0 \leqslant i < w$ and $0 \leqslant j < h$),
2.1     if($S(i,j)$ == 0)
2.2     $G_2(i,j) = G_1(i,j)$;
2.3     else
2.4     $G_2(i,j) = \overline{G_1(i,j)}$; // $\overline{G_1(i,j)}$ represents "the bit-inverse of $G_1(i,j)$"
3. Output $(G_1, G_2)$
```

When cipher-grids G_1 and G_2 are collected, secret S will be disclosed by stacking G_1 and G_2. Table 3 shows the probability for $g_1 \oplus g_2$ to be transparent (s is a pixel in S encrypted into g_1 and g_2 by Algorithm RGVSS). Fig. 3 shows the process and results of RGVSS, which do not result in pixel expansion.

Table 2
Results of the superimposition of two random grid pixels.

G_1	g_2	$g_1 \oplus g_2$
0	0	0
0	1	1
1	0	1
1	1	1

Table 3
Encoding s into g_1 and g_2 and the results of $g_1 \oplus g_2$ by Algorithm RGVSS.

s	g_1	g_2	$g_1 \oplus g_2$	$Prob(g_1 \oplus g_2)$
□	□ ■	□ ■	□ ■	1/2
■	□ ■	■ □	■ ■	0

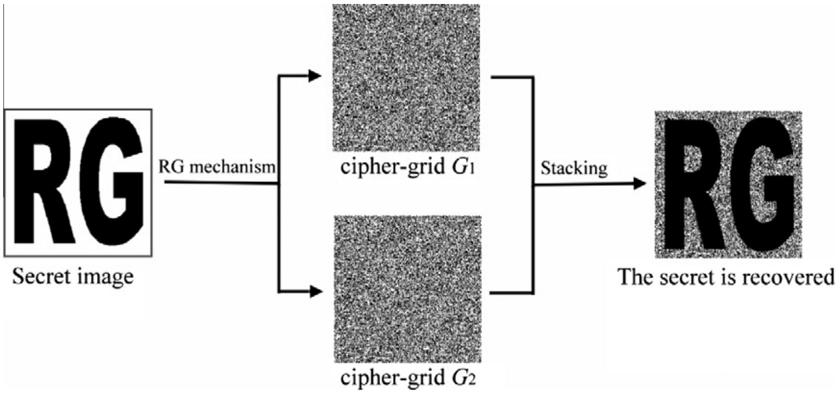

Fig. 3. The flowchart of RGVSS and the stacked result.

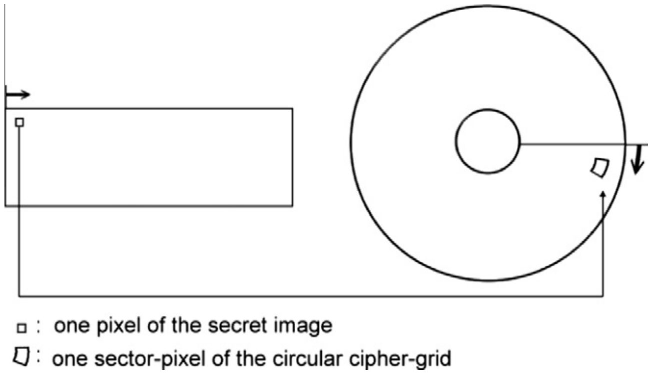
□ : one pixel of the secret image
: one sector-pixel of the circular cipher-grid

Fig. 4. The relationship of the position of one secret pixel to a random sector-pixel. Arrows represent the beginning position and direction.

3. Proposed scheme

3.1. Design of circular random grids

This section introduces an approach to combine circular random girds and fixed angle segmentation. Following are the processes to generate two circular cipher-grids to encrypt *one* secret image. Prior to describing the design, we depict the relationship of the position of one pixel of a secret image (left) with a small sector-pixel of a circular cipher-grid (right) in Fig. 4.

Assume a binary secret image with the size of $w \times h$ is to be encoded into two circular cipher-grids G^A and G^B. Without loss of generality, parameter w is the factor of 360. R is the radius of circular cipher-grids and $h < R$.

3.1.1. Generating the first circular cipher-grid A

Inspired by Chen et al.'s scheme [2], the procedure for generating circular cipher-grid A is shown below and in Fig. 5:

Step 1: Generate a black circle whose radius is $R - q$ pixels, and generate a white circle with radius of $r - q$ pixels. Let the radius $R - q > r - q$ and the initial value of $q = 0$, where $r < R$. Next, stack and center the white circle onto the black circle so a black ring C is generated.

Step 2: C is segmented and has the fixed unit "one degree of a segment." Hence, C has 360 sector-blocks, and every sector-block represents one sector-pixel, which in turn represents an expanded pixel of a sector-block in a circular cipher-grid. Next, by **Algorithm RGVSS,** assign pixels of the 360 sector-blocks as transparent or opaque to generate C'.

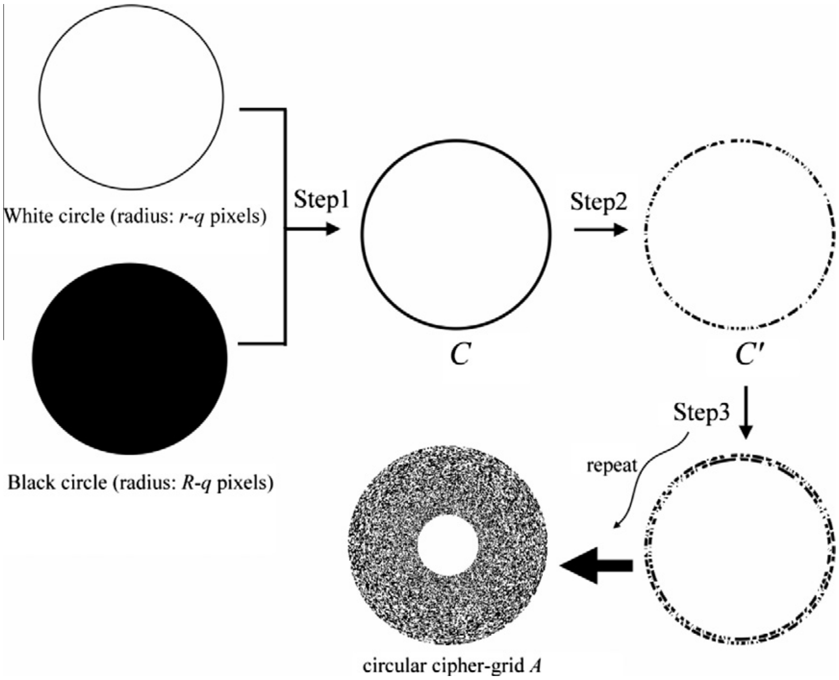
White circle (radius: *r-q* pixels)
Black circle (radius: *R-q* pixels)
Step1
C
Step2
C′
Step3
repeat
circular cipher-grid *A*

Fig. 5. Procedure for generating circular cipher-grid *A*.

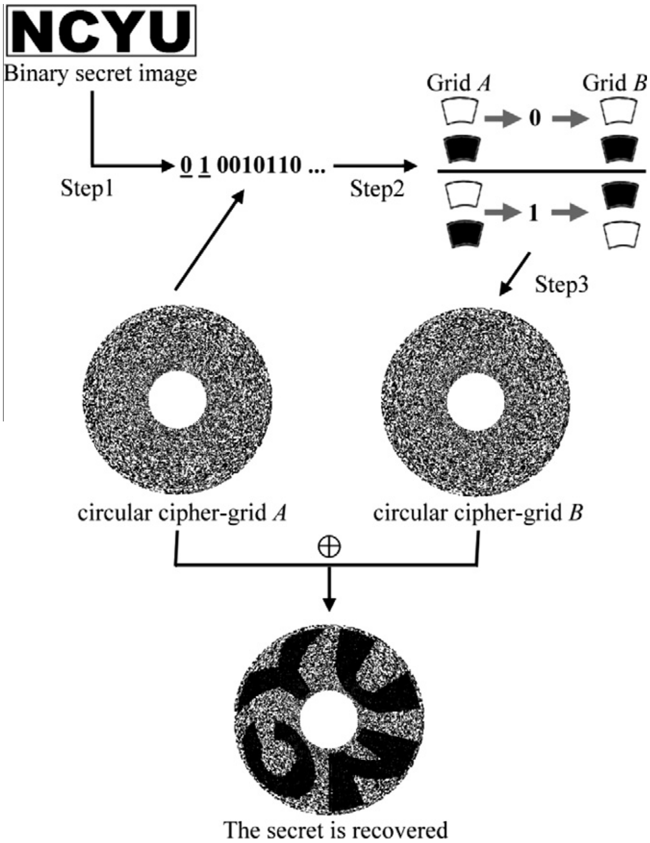

Fig. 6. Procedure for generating circular cipher-grid *B* and the stacked result.

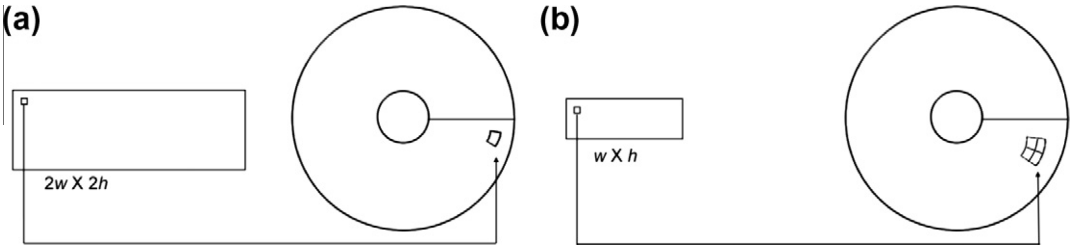

Fig. 7. Comparison of share generation between the proposed scheme and Chen et al.'s scheme [2].

Step 3: Repeat the process of Steps 1 and 2; q increases in an equal ratio after executing Step 1, and the black and white circle become smaller. Many rings composed of 360 sector-blocks are produced inside C' until the appropriate cipher-grid A is formed.

3.1.2. Generating the second circular cipher-grid B

The procedure for generating circular cipher-grid B appears below and in Fig. 6.

Step 1: Treat the binary secret image as a one-dimensional array of messages 0 and 1.
Step 2: Compare a binary secret message 0 or 1 with the corresponding sector-pixel of cipher-grid A individually to generate a sector-pixel of cipher-grid B by **Algorithm RGVSS**.
Step 3: In the same way as circular cipher-grid A was generated, repeat Step 2 to form all sector-pixels of cipher-grid B.

3.1.3. Recovering the secret

Decryption undertakes the same process as conventional visual secret sharing by VC and RG. Secret messages are revealed after stacking two cipher-grids together if the angles of A and B are matched, as in Fig. 6.

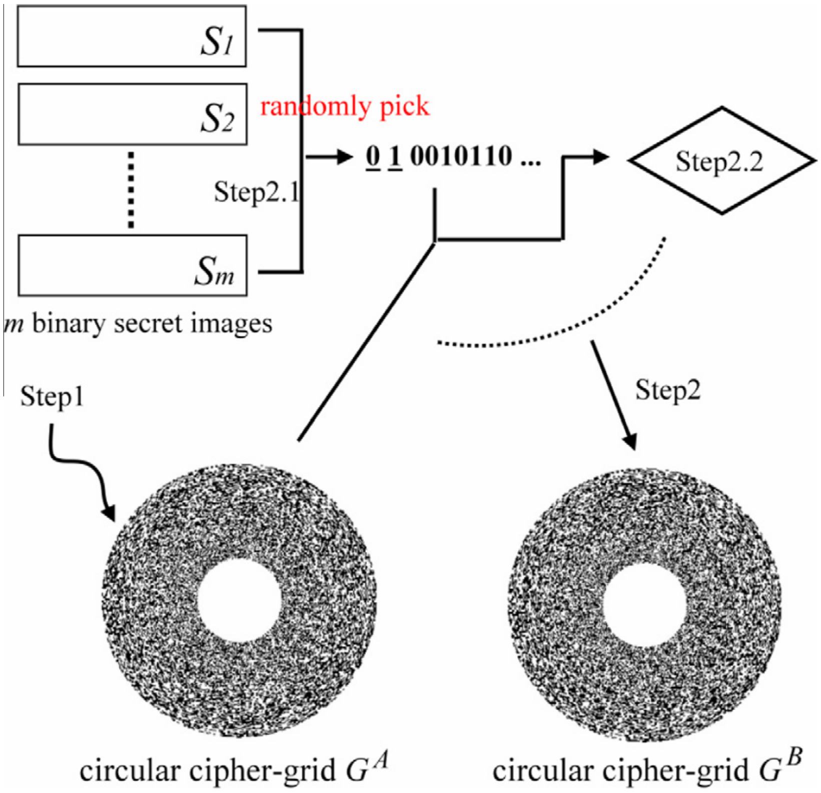

Fig. 8. Procedures for generating the circular cipher-grid G^A or G^B.

3.1.4. Advantage of adopting circular random grids

The purpose of the above design is to generate two corresponding sector-blocks in two cipher-grids to carry the message of a secret pixel of an image, as in Fig. 7(a). Chen et al.'s scheme (2005) used the concept of conventional VC to expand every original pixel of a secret image to become 2 × 2 sector-blocks, as in Fig. 7(b). Our scheme benefits from encrypting a fourfold size of secret images in the same size of circular share images.

This subsection has depicted an approach to encrypting a secret image that uses two circular random grids. The next subsection demonstrates the enhanced approach to encode more secrets at once.

3.2. Proposed RG-based multi-image encryption scheme

Suppose multiple binary secret images S_1, $S_2,\ldots,S_{m,}$, with the same size of $w \times h$, are encoded into two circular cipher-grids G^A and G^B. Without loss of generality, parameter w is the factor of 360. When we stack two circular cipher-grids, we disclose the secret image S_1. By gradually rotating one of the two cipher-grids at fixed $360/m$ degrees, we reconstruct secret images $S_2,S_3,\ldots,S_m$. The degree of rotation is based on the parameter m, that is, the number of secret images to encrypt. To begin with, we define related functions as follows:

Definition 2. $f_{GCG}()$: $f_{GCG}() \rightarrow G^A$, with the input of parameters R, and r, the function $f_{GCG}()$ represents the algorithm of "generating the first circular cipher-grid" in Section 3.1 and outputs a circular random grid.

Definition 3. *random_value*(.): function *random_value*(a) returns a random integer in the range 0 and $a - 1$.

Definition 4. $f_{RG}(,)$: $f_{RG}(a,s) \rightarrow b$, function $f_{RG}(,)$ represents the algorithm of "inputting sector-pixel a of circular cipher-grid G^A and a pixel s of secret image S will yield sector-pixel b of the other circular cipher-grid G^B" by extending Algorithm RGVSS via Algorithm 1.

Algorithm 1

```
Input: Binary sector-pixel $a$ and secret pixel $s$, where $a$ and $s$ are 0 or 1
Output: A sector-pixel $b = 0$ or 1
If $s == 0$, $b = a$,
else $b = \bar{a}$
```

3.2.1. Encryption process

The operations of the encryption process are shown in Fig. 8.

Step 1: Generate the first circular cipher-grid G^A and the corresponding matrix G_s^A.

(1.1) Create the first circular cipher-grid G^A by $f_{GCG}()$.

(1.2) Rearrange all sector-pixels in G^A to the 2-D matrix G_S^A, ordering from outer to inner rings.

Step 2: Use *Algorithm* 2 to generate G_S^B and form the second cipher-grid G^B. For each coordinate (i,j), perform the following operations.

(2.1) Randomly select secret image S_k where $k = random\_value(m)$.

(2.2) Generate $G_S^B(i,j)$ with $S_k(i,j)$ of secret image S_k and $G_S^A(i,(j+\frac{(k-1)}{m}w)/w)$, that is, $f_{RG}G_S^A(i,(j+\frac{(k-1)}{m}w)/w),S_k(i,j)) \rightarrow G_S^B(i,j)$. Rotate sector-pixel $G_S^B(i,j)$ clockwise at $k \times \frac{360}{m}$ degrees and stack with sector-pixel $G_S^A(i,(j+\frac{k}{m}w)/w)$ to visually disclose pixel $S_k(i,j)$ of image S_k.

After performing Steps 1 and 2 $w \times h$ times, G_S^B will emerge so a second circular cipher-grid G^B can be obtained subsequently by rearranging all values in the 2-D matrix G_S^B row by row into G^B from outer to inner rings.

Algorithm 2

```
Input: $m$ binary secret images $S_k = \{S_k(i,j)|S_k(i,j) = 0$ or $1, 0 \leqslant i < w, 0 \leqslant j < h\}$, where $k = 1, 2,\ldots,m$ and one matrix of
  sector-pixels $\mathbf{G}_S^A = \{\mathbf{G}_S^A(i,j)|\mathbf{G}_S^A(i,j) = 0$ or $1, 0 \leqslant i < w, 0 \leqslant j < h\}$
Output: one matrix of sector-pixels $G_S^B = \{G_S^B(i,j)|G_S^B(i,j) = 0$ or $1, 0 \leqslant i < w, 0 \leqslant j < h\}$
    for($i$ and $j$, $0 \leqslant i < w$ and $0 \leqslant j < h$)
    $k = random\_value(m)$
    $f_{RG}(G_S^A(i,(j+\frac{(k-1)}{m}w)/w),S_k(i,j)) \rightarrow G_S^B(i,j)$
```

3.2.2. Decryption process

By collecting the two circular cipher-grids G^A and G^B, we can reconstruct the secret information. First, directly stack the two circular cipher-grids G^A and G^B to recover the first secret image. Then stack G^B with G^A gradually rotated clockwise at $\frac{360}{m}$ degrees to recover other secret images.

4. Further discussion and analysis

4.1. Discussion

The purpose of the proposed method is to use the innate advantages of Kafri and Keren's method while increasing flexibility. The following discussion highlights the advantages of the proposed scheme compared with conventional VC.

(1) *No extra codebook needs to be redesigned:* The scheme does not require redesigning a sophisticated codebook to meet the new demand prior to encryption.
(2) *No extra pixel expansion is produced:* No extra pixel expansion occurs, so the scheme does not have the drawback of conventional VC-based VSS.
(3) *Multiple secrets can be encoded:* The scheme can encrypt more secrets than conventional VC- and RG-based VSS can.
(4) *Bandwidth and storage are saved:* The bandwidth and storage complexity depends on the size of the share images (pixel expansion). It also benefits from encrypting more secrets. Performance on properties 1, 2 and 3 in terms of bandwidth and storage is efficient.

Table 4 compares the functionality between related methods and the proposed method. The proposed RG-based VSS scheme works well in terms of pixel expansion and ability to encode multiple secrets.

4.2. Analysis

Two properties of visual secret sharing techniques must be highlighted and satisfied before a proposed scheme can be considered useful: visual quality and security.

(1) *Visual quality*: The stacked result of two cipher-grids must disclose the secret image to the naked human eye.
(2) *Security*: The information in a secret image must not be disclosed by the cipher-grid alone.

For limitations of space, some definitions and lemmas used to analyze properties are given without proofs. Readers may refer to Refs. [5,13] for details.

Assume that $S_k(0)$ ($S_k(1)$) is the corresponding area of all the white (black) pixels in the kth secret image S_k, where $S_k = S_k(0) \cup S_k(1)$ and $S_k(0) \cap S_k(1) = \varphi$. Hence, $B[S_k(0)]$ ($B[S_k(1)]$) is the area of the stacked image B that corresponds to all white (black) pixels in the secret image S_k.

Definition 5 (*Contrast*). The contrast of the stacked binary image B with respect to the original secret image S is

$$\alpha = \frac{T(B[S(0)]) - T(B[S(1)])}{1 + T(B[S(1)])}.$$

α should be as large as possible since the larger its value, the more recognizable the superimposed secret will be:

Table 4
Comparisons between related methods and the proposed method.

Comparisons	Encryption method	Codebook needed	Pixel expansion ratio	Multiple secrets
Naor and Shamir [11]	VC	Yes	2 or More	No
Wu and Chang [15]	VC	Yes	4	Yes
Shyu et al. [14]	VC	Yes	$2m^*$	Yes
Chen et al. [2]	VC	Yes	4	Yes
Hsu et al. [7]	VC	Yes	9	Yes
Kafri and Keren [9]	RG	No	1	No
Shyu [12]	RG	No	1	No
Chen and Tsao [4]	RG	No	1	No
Shyu [13]	RG	No	1	No
Chen and Tsao [5]	RG	No	1	No
Chen et al. [3]	RG	No	1	Yes (only 2)
The proposed scheme	RG	No	1	Yes (2 or more)

[*] m is the number of secret images.

Lemma 1. *The expected value of the average light transmission of random grid G is* 1/2, that is, $T(G) = 1/2$.

Lemma 2. *The bit-wise OR operation over random grids has the following properties*:

(1) *When two "identical" random grids – that is, $G \oplus G$, where operation $\oplus$ is denoted as bit-wise OR operation – are superimposed, the result is the same as G.*
(2) *When two "inversing" random grids – that is, $\overline{G} \oplus G$, where $\overline{G}$ is the bit-wise complement of G – are superimposed the result of $\overline{G} \oplus G$ is a fully black image.*

Lemma 3. *When two independent random grids, G^A and G^B, are superimposed as a binary image, the expected value of the average light transmission is* 1/4, that is, $T(G^A \oplus G^B) = 1/4$.

Lemma 4. *When two cipher-grids, G^A and G^B, generated by Algorithm RGVSS, are superimposed as a binary image B, the expected values of the average light transmission of $B[S(0)]$ and $B[S(1)]$ are 1/2 and 0, respectively. That is:*

(1). $T(B[S(0)]) = 1/2$ *and*
(2). $T(B[S(1)]) = 0$.

Hereafter, we analyze performance in terms of visual quality (contrast > 0) and security.

Theorem 1 (*Contrast*). *When cipher-grids G^A and G^B are superimposed, the contrast of the superimposed result B_k is high enough, precisely, $\frac{2}{5m-1}$, to reveal the secret images $S_k (k = 1, 2, \ldots, m)$, that is, $B_k = G^A \oplus G^B$ is visually recognizable in order to disclose the secrets in the proposed scheme.*

Proof. Assume that m ($m > 1$) secret images are turned into two circular cipher-grids. If the contrast with the parameter m is proved greater than zero, the stacked result of the two circular cipher-grids will reveal the secret by Definition 5.

By step 2 in the encryption process, every sector-pixel $G^B_S(i,j)$ created by function $f_{RG}(.)$ has the probability $\frac{1}{m}$, corresponding to the relative pixel $S_k(i,j)$. When cipher-grids G^A and G^B are superimposed for the average light transmissions of the corresponding areas in B_k with respect to the white areas in S_k, we have the $\frac{1}{m}$ area obtained by Algorithm RGVSS and the remainder: that is, $\frac{m-1}{m}$ area is randomly created in a random way. We have $T(B_k[S_k(0)]) = \frac{1}{m} \times \frac{1}{2} + \frac{m-1}{m} \times \frac{1}{4} = \frac{m+1}{4m}$ by Lemma 4(1) and Lemma 3 and, likewise, the black area $T(B_k[S_k(1)]) = \frac{1}{m} \times 0 + \frac{m-1}{m} \times \frac{1}{4} = \frac{m-1}{4m}$ by Lemma 4(2) and Lemma 3. The contrast of the superimposed result is:

$$\alpha = \frac{T(B_k[S_k(0)]) - T(B_k[S_k(1)])}{1 + T(B_k[S_k(1)])} = \frac{\frac{m+1}{4m} - \frac{m-1}{4m}}{1 + \frac{m-1}{4m}} = \frac{2}{5m-1}.$$

Consequently, the contrast of the superimposed results in the proposed scheme is $\frac{2}{5m-1} > 0$. By Definition 5, proof is obtained.

Theorem 2 (*Security*). *Each cipher-grid, G^A or G^B, alone reveals no information of secrets S_k, that is, G^A and G^B, each seen alone, are visually meaningless in the proposed scheme.*

Proof. The proof demonstrates how the contrast of each cipher-gird is equal to zero such that each cipher-grid is meaningless.

In step 1 in the encryption process, a sector-pixel $G^A_S(i,j) \in G^A$ is created by function $f_{GCG}(.)$, so $Prob(G^A_S\ G^A_S\ (i,j) = 0) = Prob(G^A_S\ (i,j) = 1) = 1/2$. The expected value of the average light transmission of the corresponding area in G^A with respect to the white (black) area in secret image S_k is $T(G^A[S_k(0)]) = 1/2$ ($T(G^A[S_k(1)]) = 1/2$). With cipher-grid G^A alone, the contrast of G^A is:

$$\alpha = \frac{T\Big(G^A[S_k(0)]\Big) - T\Big(G^A[S_k(1)]\Big)}{1 + T\Big(G^A[S_k(1)]\Big)} = \frac{\frac{1}{2} - \frac{1}{2}}{1 + \frac{1}{2}} = 0$$

By Definition 5, G^A is meaningless; that is, we cannot visually recognize the information using G^A alone. From step 2 in the encryption process, we know that every sector-pixel $G^B_S(i,j)$ is created by function $f_{RG}(.)$ and has probability $\frac{1}{m}$ corresponding to the relative pixel $S_k(i,j)$ from the kth secret image S_k. Thus, the expected value of the average light transmission of the corresponding area in G^B with respect to the white area in S_k is $T(G^B[S_k(0)]) = \underbrace{\frac{1}{m} \times \frac{1}{2} + \frac{1}{m} \times \frac{1}{2} + \cdots + \frac{1}{m} \times \frac{1}{2}} = \frac{1}{2}$.

Likewise, $T(G^B[S_k(1)]) = 1/2$. With cipher-grid G^B alone, the contrast of G^B is:

$$\alpha = \frac{T(G^B[S_k(0)]) - T(G^B[S_k(1)])}{1 + T(G^B[S_k(1)])} = \frac{\frac{1}{2} - \frac{1}{2}}{1 + \frac{1}{2}} = 0.$$

Hence, we cannot recognize the information visually using G^B alone.

5. Experimental results

To demonstrate the feasibility of the proposal, this section conducts experiments by hiding two, three, and four secrets.

5.1. Simulation 1

Simulation 1 inputs two secret images with 180 × 360 pixels, as in Fig. 9(a and b). Experimental results are shown as follows. Encrypted cipher-grids G^A and G^B are in Fig. 9(c and d). The secret cannot be revealed by a random grid alone. Fig. 9(e and f) show the results by superimposing two cipher-grids. After directly stacking the two circular cipher-grids, G^A and G^B, the first secret message is presented visually in Fig. 9(e). Then, if stacking G^B and clockwise rotated G^A at 180 degree, the second secret is reconstructed as in Fig. 9(f).

5.2. Simulation 2

Three secret images with the size of 270 × 360 pixels, as in Fig. 10(a–c), are input and the encrypted circular cipher-grids G^A and G^B are generated, as in Fig. 10(d and e). Once we directly stack cipher-grids G^A and G^B, the first secret message is presented visually, as in Fig. 10(f). Then, if we stack G^B and the clockwise rotated G^A at 120 degrees a, the second secret message is reconstructed in Fig. 10(g). Finally, if we stack G^B and the clockwise rotated G^A at 240 degree, the third secret message is reconstructed in Fig. 10(h).

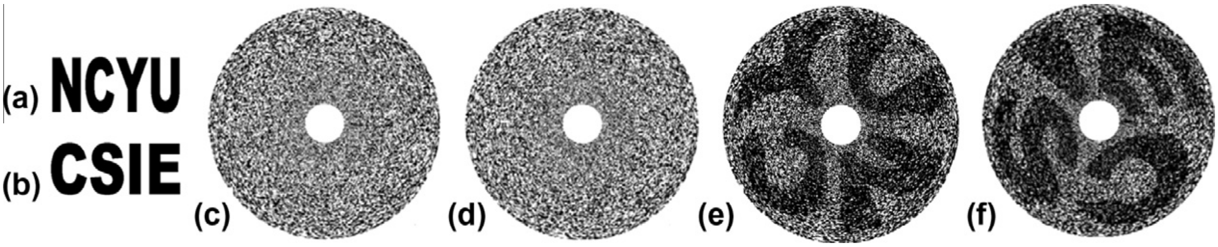

Fig. 9. (a) and (b) Original secret images for the test; (c) and (d) generated circular cipher-grids; (e) and (f) recovered secrets.

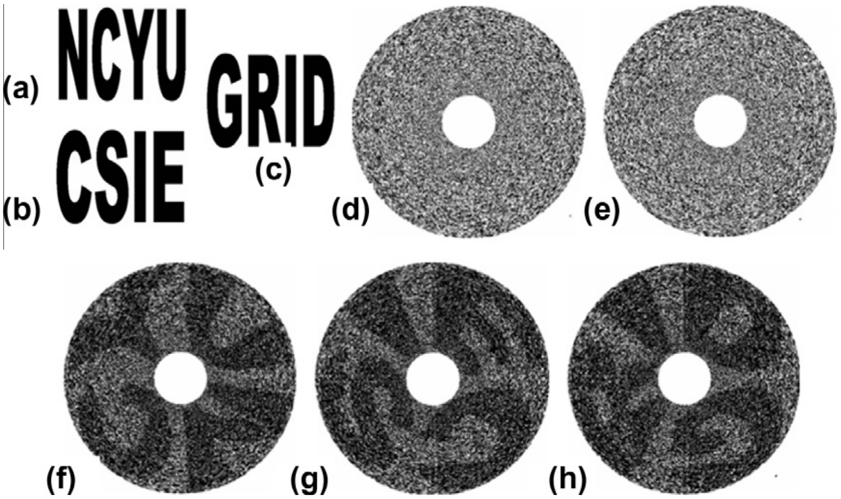

Fig. 10. (a)–(c) Three original images for testing; (d) and (e) two generated circular cipher-grids; and (f)–(h) recovered secrets.

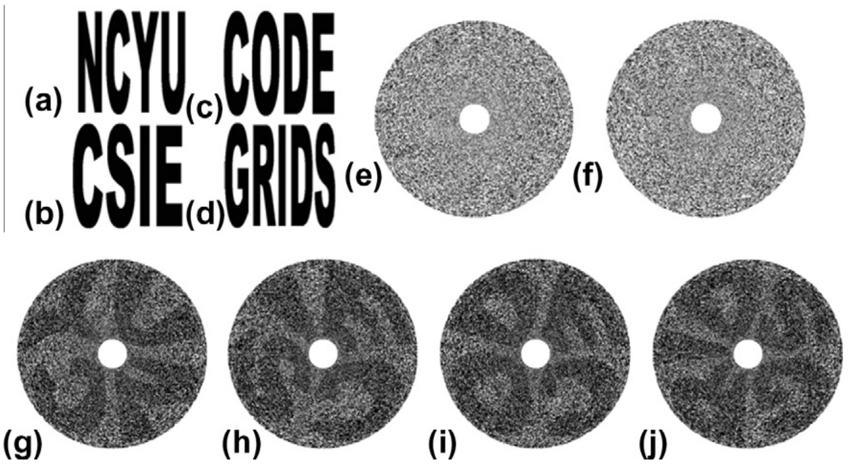

Fig. 11. (a)–(d) Four images to test; (e) and (f) two generated circular cipher-grids; and (g)–(j) recovered secrets.

5.3. Simulation 3

We input four secret images with the size of 360 × 360 pixels, as in Fig. 11(a)–(d), with encrypted circular cipher-grids G^A and G^B in Figs. 11(e) and (f). After we stack G^A and G^B, the first secret message is visible, as in Fig. 11(g). If we stack G^B and clockwise rotated G^A at 90 degrees, the second secret is reconstructed in Fig. 11(h); Fig. 11(i) demonstrates secret message of stacking G^B and clockwise rotated G^A at 180 degrees, while Fig. 11(j) demonstrates that of G^B and clockwise rotated G^A at 270 degrees.

6. Conclusion

This paper proposes a novel RG-based VSS scheme with the capability of encrypting multiple secret images at once into only two circular cipher-grids. To decrypt all secrets, decoders stack the two circular cipher-grids to disclose the first secret and then gradually rotate one circular cipher-grid at a fixed degree to reveal the second. Theoretical analysis demonstrates the accuracy and security of the proposed method.

Acknowledgements

This research was partly supported by National Science Council Contract NSC 95-2221-E-415-009-MY3. The authors thank the Graduate School of Computer Science and Information Technology, National Taichung Institute of Technology, for providing source code for circular visual cryptography.

References

[1] 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, 2005, pp. 300–304.
[2] J. Chen, T.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.
[3] T.H. Chen, K.H. Tsao, K.C. Wei, Multiple-image encryption by rotating random grids, in: Proceedings of the 8th International Conference on Intelligent System Design and Applications (ISDA'2008), Kaohsiung, Taiwan, 2008.
[4] T. H. Chen, K.H. Tsao, Image encryption by (n,n) random grids, in: Proceedings of the 18th Information Security Conference, Hualien, Taiwan, 2008.
[5] T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, Pattern Recognition 42 (2009) 2203–2217.
[6] W.P. Fang, J.C. Lin, Visual cryptography with extra ability of hiding confidential data, Journal of Electronic Imaging 15 (2) (2006).
[7] H.C. Hsu, J. Chen, T.S. Chen, Y.H. Lin, Special type of circular visual cryptography for multiple secret hiding, The Imaging Science Journal 55 (3) (2007) 175–179.
[8] R. Lukac, K.N. Plataniotis, Bit-level based secret sharing for image encryption, Pattern Recognition 38 (5) (2005) 767–772.
[9] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Optics Letters 12 (6) (1987) 377–379.
[10] M. Naor, B. Pinkas, Visual authentication and identification, in: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes in Computer Science, vol. 1294, Santa Barbara, California, USA, 1997, pp. 322–336.
[11] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.
[12] S.J. Shyu, Image encryption by random grids, Pattern Recognition 40 (3) (2007) 1014–1031.
[13] S.J. Shyu, Image encryption by multiple random grids, Pattern Recognition 42 (7) (2009) 1582–1596.
[14] S.J. Shyu, S.Y. Huang, Y.K. Lee, R.Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognition 40 (12) (2007) 3633–3651.
[15] H.C. Wu, C.C. Chang, Sharing visual multi-secrets using circle shares, Computer Standards & Interfaces 28 (1) (2005) 123–135.
[16] D.S. Tsai, G. Horng, T.H. Chen, Y.T. Huang, A novel secret image sharing scheme for true-color images with size constraint, Information Sciences 179 (19) (2009) 3247–3254.
[17] C.C. Chang, C.C. Lin, C.H. Lin, Y.H. Chen, A novel secret image sharing scheme in color images using small shadow images, Information Sciences 178 (11) (2008) 2433–2447.