

The Comparative Study on Visual Cryptography and Random Grid Cryptography

G.Deepa¹

¹(Master of computer Applications, Bharathiar university, India)

Abstract: Visual cryptography scheme is a cryptographic technique which allows visual information to be encrypted into several shares in such a way that the decryption can be performed by the human visual system, without the aid of computers. Random grid is a methodology to construct visual secret sharing (vss) scheme without pixel expansion in which an RG scheme takes an input image and transforms it into multiple cipher-grids that provide no information on the original image and the resulting decrypted image retains the size of the original image. Intent of this paper is on comparative study of visual cryptography and Random grid cryptography on the basis of analysis and correctness of simple VC schemes and RG schemes, improving contrast of the reconstructed image using various algorithms and multiple-image encryption using rotating angles.

Keywords - ideal contrast, random grid scheme, ring shadow technology, rotating random grids, visual cryptography scheme.

I. Introduction

In recent years the people from all over the world rely on internet in order to transmit and share their information where they concern mostly on information security to protect the data from unauthorized hacking processes. For security purpose people go for secret data with symmetric or asymmetric cryptography where these cryptographic methods need high computation cost in encryption and decryption processes. Therefore, many visual secret sharing schemes and random grids schemes were proposed where visual secret sharing (VSS) scheme is an efficient secure method for hiding a secret image by dividing it into meaningless share images so that it cannot leak any information of the shared secret and any one can decode it easily by the human visual system without using complex cryptographic algorithms. The other is the random grid (RG) scheme takes an input image and transforms it into multiple cipher-grids that provide no information on the original image and it have the additional benefit that they require no pixel expansion.

This paper provides an comparative study of visual cryptography (VC) schemes and random grid (RG) cryptography schemes where the contrast of the reconstructed image, Pixel expansion factor and support of multiple secret images is of significance. A recovered image with lower contrast will result in the hidden content being faded and unclear. The hidden content becomes less discernable to the human eye. As such, the pixel expansion factor and the contrast ratio are the two most important metrics in the evaluation of VSS and RG schemes efficiency.

II. Analysis and Correctness of Naor and Shamir's 2 out of 2 Algorithm

2.1 Introduction

The simplest VC algorithm was given by Naor and Shamir on visual cryptography. They presented a 2 out of 2 scheme, in which 2 shares would be generated ($n = 2$) for each image encrypted, while decryption would require these 2 shares ($k = 2$) to be super-imposed. At its most basic level, the 2 out of 2 algorithm works by representing each pixel in the original image by 2 pixels in each share. Each pixel in the original image is read and, if a white pixel is encountered, one of the first two rows in Fig. 1 is selected with equal probability, and each share is assigned a 2 pixel block as shown in the third and fourth columns. Similarly, if a black pixel is encountered, one of the last two rows is selected with equal probability, from which a subpixel is assigned to each share.

If two white pixels overlap when two shares are superimposed, the resulting pixel will be white. By contrast, if a black pixel in one share overlaps with either a white or black pixel in the other share, the resulting pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure 1 shows the resulting subpixel when the subpixels of both shares in the third and fourth columns are superimposed.

As demonstrated in Fig. 1, if a pixel in the original image was black, the subpixel in the superimposition of the two shares will be fully black. Similarly, if a pixel in the original image was white, the subpixel in the superimposition of the two shares will be black and white. However, because the pixels are small and situated

very close together, the human eye averages the relative contributions of the black and white pixels, resulting in a grey pixel.

The following Fig. 1 shows the pixel table of Naor and Shamir's 2 out of 2 A lgorithm:

















OriginalPixel	Probability	Share1 sub-pixel	Share2 sub-pixel	Share1 Share2
	0.5			
	0.5			
	0.5			
	0.5			

Fig.1: 2 out of 2 using 2 subpixels per original pixel

2.2 Analysis of Naor and Shamir's 2 out of 2 Algorithm:

Let w be the width of the original image, and h be its height. Then, $n = w \times h$ is the number of pixels in the original image. To encrypt an image using the 2 out of 2 algorithm, each pixel in the original image must be read, and a block of m subpixels must then be written to each share. Thus, for each pixel in the original image, $2m$ subpixels are written, and each share contains $n \times m$ pixels. As such, a total of $2(n \times m)$ pixels are written in the encryption process. As long as $m < n$, we thus have a linear time complexity of $O(n)$ for the encryption algorithm.

When superimposition is done by a computer, each subpixel in each share must be read sequentially, computing the Boolean OR of the subpixels from each share as they are read. This computation requires $O(m)$ time, and there are n such computations. Once again, as long as $m < n$, decryption takes place in linear time.

2.3 Correctness of Naor and Shamir's 2 out of 2 Algorithm

The correctness of the decryption routine relies on the correctness of the Boolean OR function and the ability of the human eye to average relative contributions made by neighbouring colours. For each white pixel in the original image, a BWWB or WBBW is written to each share with equal probability. When two identical pixels from each share are superimposed, the resulting subpixel will not change, and will be 50% black. The human eye therefore averages this as a grey pixel. Similarly, for each black pixel in the original image, complementary pixels are written to each share. When these complementary subpixels are superimposed, the resulting pixel will be 100% black, resulting in a black pixel in the decrypted image.

In order to repair the contrast of a decrypted image the author used a very simple contrast repair algorithm which works by scanning each subpixel in the decrypted image. If a subpixel is found to be 100% black, then it should remain a black pixel. However, if it is found to be 50% white, then it should be written as a white pixel.

III. Analysis and Correctness of Kafri and Keren's First Random Grid Algorithm

3.1 Introduction:

While the approach by Naor and Shamir offers perfect security when one possesses only a single share, it suffers from the need to represent each pixel in the original image by multiple pixels in each share, resulting in a decrypted image that is 2 - 4 times larger than the original image. Here additional time is required to encrypt and decrypt images - as well as to transfer encrypted images across a network - than would be required in a scheme that did not require the use of pixel expansion.

Such a scheme was proposed by Kafri and Keren which uses the random grids (RG) without pixel expansion. An RG scheme takes an input image and transforms it into multiple cipher-grids that provide no information on the original image. However, RG schemes have the additional benefit that they require no pixel

expansion, and thus each share - along with the resulting decrypted image - retains the size of the original image. The following section details an algorithm employing random grids.

3.2 2 out of 2 using Random Grids:

Kafri and Keren proposed 2 out of 2 algorithm which takes an input image of size height x width. It then initializes two cipher-grid images R_1 and R_2 with the same dimensions as the input image. In lines 6 - 8, the algorithm randomizes the contents of R_1 , producing an image of random black and white pixels. R_2 is next generated based on the input image and R_1 in lines 11 - 15. This process occurs by scanning each pixel of the input image. If a pixel at location $[x, y]$ in the input image is found to be white, then the pixel $R_2[x, y]$ is set to be the same as $R_1[x, y]$. If, instead, the pixel at $[x, y]$ in the input image is black, then the pixel $R_2[x, y]$ is set to be the complement of $R_1[x, y]$.

A pseudo-code listing of Kafri-Keren-Algorithm is presented in Fig.2

```

Input : Input image I of size height x width
Output : Two cipher-grids  $R_1, R_2$  both of size height x width
1 Setup constants
2 WHITE 0
3 BLACK 1
4 Randomize the first cipher-grid  $R_1$ 
5 for row  $\leftarrow$  1 to height
6 do for col  $\leftarrow$  1 to width
7 do  $R_1[\text{row}, \text{col}] = \text{RANDOM}(\text{WHITE}, \text{BLACK})$ 
8 Create the second cipher-grid  $R_2$  based on I and  $R_1$ 
9 for row  $\leftarrow$  1 to height
10 do for col  $\leftarrow$  1 to width
11 do if  $I[\text{row}, \text{col}] = \text{WHITE}$ 
12 then  $R_2[\text{row}, \text{col}] = R_1[\text{row}, \text{col}]$ 
13 else  $R_2[\text{row}, \text{col}] = 1 - R_1[\text{row}, \text{col}]$ 
14 return  $R_1, R_2$ 
    
```

Fig.2 Random Grid algorithm proposed by Kafri and Keren

The following Fig.3 shows the Pixel table for Kafri and Keren's first random grid algorithm:

















$I[x, y]$	$R_1[x, y]$	$P(R_1[x, y])$	$R_2[x, y]$	$R_1[x, y] \parallel R_2[x, y]$
		0.5		
		0.5		
		0.5		
		0.5		

Fig.3 Pixel table for Kafri and Keren's first random grid algorithm

Fig.3 shows the possibilities for the pixels written to each share based on a given pixel in the input image. As the table shows, if a white pixel is encountered in the input image and a white pixel is randomly selected for R_1 (with probability 0.5), a white pixel will also be written to R_2 . If, instead, a black pixel is selected for R_1 , then a black pixel will be written to R_2 . Thus, when the shares are overlaid, the share pixels generated from a white input image pixel will be correct only 50% of the time. This also implies that, on average, 50% of the white pixels in the input image will appear unaltered in each share.

For black pixels in the input image, one can see that, regardless of the pixel selected for R_1 - white or black, with equal probability - the resulting pixel when both shares are superimposed will be black. This is

because, if a black pixel is selected for R_1 , the resulting superimposed pixel will be black regardless of the pixel selected for R_2 due to the properties of the Boolean OR operation. By contrast, if a white pixel is selected for R_1 , then the resulting superimposed pixel will also be black, since R_2 is always chosen as the complement of R_1 and will thus be assigned a black pixel. Thus, all black pixels in the input image will be black in the decrypted image.

3.3 Analysis of Kafri and Keren's First Random Grid Algorithm:

To encrypt an image using this random grid method, the cipher-grid R_1 of size n ($n = \text{width} \times \text{height}$ be the number of pixels in the original image) must first be created by randomly assigning an integer value in the range $[0, 1]$ to each of its pixels. Since 0 and 1 can be represented in 1 bit, generating a random value requires constant time. Thus, R_1 is generated in $O(n)$ time.

To generate R_2 , each pixel of the original image must be read, and a constant time comparison decides the next pixel value to be written to R_2 . As such, the creation of R_2 also takes place in linear time. Thus, the encryption algorithm runs in time linear in the number of pixels in the input image.

3.4 Correctness of Kafri and Keren's First Random Grid Algorithm:

Let W represent a white pixel and B represent a black pixel. If share1 is decrypted by an intruder means it provides no information about the original image, since share1 is generated randomly. Then he tried to decrypt the share2 and examines the first pixel as B (black pixel) i.e., $R_2[x, y] = B$. Looking at Fig.3, we see that given a black pixel in the second share, the original pixel could be black or white with equal probability. That is, $P(I[x, y] = B | R_2[x, y] = B) = P(I[x, y] = W | R_2[x, y] = B) = 0.5$. Thus, the intruder can obtain no information about the original image from this pixel.

IV. Ideal Contrast using vcs by linear error correcting code without pixel expansion

As we know the linear code is very easy to realize by a computer. This scheme uses linear error-correcting code, so its computation is very easy. This (k, n) -VCS is based on linear error-correcting code in $GF(2)$. Our system must be involved in one dealer and n participants.

The scheme is as following. And all the following computation is on the finite field $GF(2)$, just mean their addition is XOR operation and the multiplication is on $GF(2)$ too. Our scheme is motivated by Linear Secret Sharing Scheme (LSSS).

Firstly, the dealer D choose an $[n+1, m]$ linear error correcting code C in $GF(2)$. Let G be generator matrix of C and $g_0 = [g_{00}, g_{01}, \dots, g_{0, m-1}, 0]^T$ be the first column of the generator matrix G . Let $s \in GF(2)$ denote the secret pixel. If $s = 0$ secret pixel s is white and if $s = 1$ secret pixel s is black. Then the information vector $s = (s_0, s_1, \dots, s_{m-1})$ is chosen to be any vector of $GF(2)^m$ such that $s \cdot g_0 = \sum_{i=0}^{m-1} s_i g_{i0} = 1$

The codeword corresponding to this information vector s is $t = (t_0, t_1, \dots, t_n) = sG$. We can give t_i to the participant P_i as their share pixel, where $t_i \in GF(2)$. So $t_i = 0$ or 1, if $t_i = 0$ then the share pixel of P_i is white and $t_i = 1$ then the share pixel of P_i is black. The first component $t_0 = s$ of the codeword t is the secret pixel.

It is not hard to prove that in the secret sharing scheme based on a generator matrix $G = [g_0, g_1, \dots, g_n]$ of an $[n+1, m]$ linear code such that g_0 is a linear combination of the other n columns g_1, g_2, \dots, g_n , the secret t_0 is determined by the set of shares $\{t_{i_1}, t_{i_2}, \dots, t_{i_k}\}$ if and only if g_0 is a linear combination of the vector $g_{i_1}, g_{i_2}, \dots, g_{i_k}$ where $1 \leq i_1, \dots, i_k \leq n$ and $k \leq n$.

Reconstructing the secret pixel is straight forward :

Solve the linear equation:

$$s \cdot g_0 = \sum_{j=1}^k x_j g_{ij} \quad 2$$

to find x_j , and the secret is then given by

$$t_0 = s \cdot g_0 = \sum_{j=1}^k x_j s \cdot g_{ij} = \sum_{j=1}^k x_j t_{ij} \quad 3$$

The best advantage of this scheme is without pixel expansion, every participant just shares one pixel for any one secret pixel. At the same time, the (k, n) -VCS is ideal scheme because it can fully reconstruct the original secret pixel by solving linear equation, so there is no contrast problem.

V. The lossless secret reconstruction and improvement in the contrast using Kafri and Keren's VSS Scheme under the Proposed Decryption Operation XOR for the Random grids:

In Kafri and Keren's $(2, 2)$ VSS scheme, a binary image is encrypted in two cipher grids and recovered by superimposing both cipher grids. Kafri and Keren proposed the three different algorithms to encrypt a binary image into two cipher grids, which are regarded as Algorithms 1-3.

Input: Binary secret image A of size $h \times w$ such that $A[i, j] \in \{0, 1\}$, where $1 \leq i \leq h$ and $1 \leq j \leq w$.

Output: Two random cipher grids R_1 and R_2 of size $h \times w$ such that $R_1[i, j] \in \{0, 1\}$ and $R_2[i, j] \in \{0, 1\}$, where $1 \leq i \leq h$ and $1 \leq j \leq w$.

Algorithm 1.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = \text{randomValue}(0, 1)$ for $1 \leq i \leq h$ and $1 \leq j \leq w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
if (A[i, j] = 0) R2[i, j] = R1[i, j]
else R2[i, j] =  $\overline{R_1[i, j]}$ 
}
```

Algorithm 2.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = \text{randomValue}(0, 1)$ for $1 \leq i \leq h$ and $1 \leq j \leq w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
if (A[i, j] = 0) R2[i, j] = R1[i, j]
else R2[i, j] = randomValue(0, 1)
}
```

Algorithm 3.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = \text{randomValue}(0, 1)$ for $1 \leq i \leq h$ and $1 \leq j \leq w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
if (A[i, j] = 0) R2[i, j] = randomValue(0, 1)
else R2[i, j] =  $\overline{R_1[i, j]}$ 
}
```

$\text{randomValue}(0, 1)$ is a function that returns a random value either 0 or 1 by using a coin flip procedure. \overline{R} is defined as an inverse grid of a binary grid R of size $h \times w$, which is obtained by bitwise complementing of R, i.e., $\overline{R[i, j]} = 1 - R[i, j]$ for $1 \leq i \leq h$ and $1 \leq j \leq w$.

The effectiveness of VSS schemes based on random grids is measured by the contrast of the reconstructed image, which is defined in terms of the average light transmission.

Table 1. Contrast of the Reconstructed Image Obtained under OR and XOR Operation

Algorithm	α_{OR}	α_{XOR}	Remarks
1	$1/2$	1	$\alpha_{XOR} > \alpha_{OR}$
2	$1/5$	$1/3$	$\alpha_{XOR} > \alpha_{OR}$
3	$1/4$	$1/2$	$\alpha_{XOR} > \alpha_{OR}$

The proposed operation improves the contrast of the reconstructed image for all three Algorithms. In case of Algorithm 1, the contrast value of the reconstructed image under the proposed operation is 1, i.e., the reconstructed image is exactly same as the original secret image and recognizable perfectly. While for Algorithm 2 and 3, the reconstructed image will be more visually recognizable under the proposed XOR operation compared to the OR operation.

VI. A novel visual secret sharing scheme for multiple secret images using Ring Shadow technology

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. 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.

6.1 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, \dots, S_m are all sized $X \times Y$, where X is a multiple of m . 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.4.

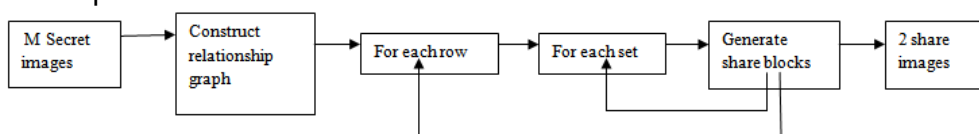


Fig.4 The flowchart of the proposed share image generation process

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 $0, 360^\circ/m, 360^\circ/m \times 2, \dots, 360^\circ/m \times (m - 1)$ 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. An example of a $(2, 2)$ -3-VSSM scheme is illustrated in Fig.5, 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.

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

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_{ij}^p denote the j -th pattern of the share block a_i^p and b_{ij}^p denote the j -th pattern of b_i^p . In the p -th sub-process, the proposed scheme first fills $a_{i,i}^p$ with effective visual pattern P_e for all i and fills a_{ij}^p with ineffective visual patterns P_i for all $i \neq j$. Then b_{ij}^p is filled with the white pattern P_w if

$S_{1+((i-j) \bmod m)}^{(r, p+(j-1)X/m)} = 0$; otherwise, b_{ij}^p 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.

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.

$$\begin{aligned}
 &P_e \text{ if } i = j \\
 a_{ij}^p = & \hspace{15em} 4 \\
 &P_i \text{ if } i \neq j
 \end{aligned}$$

$$\begin{aligned}
 &P_w \text{ if } S_{1+((i-j) \bmod m)}^{(r, p+(j-1)X/m)} = 0 \\
 b_{ij}^p = & \hspace{15em} 5 \\
 &P_B \text{ else.}
 \end{aligned}$$

Thus for each row, it needs to repeat the sub-processes X/m times for $p=1, 2, \dots, X/m$. 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.

6.2 The decryption process of the proposed scheme:

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 $360/m^\circ$. The third secret is revealed by rotating the inner share image anticlockwise $2 \times 360/m^\circ$ 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. 6.

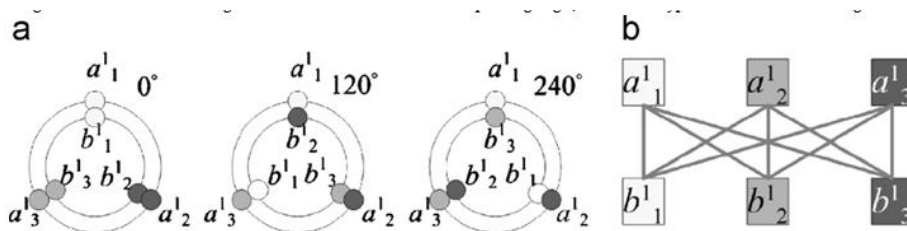


Fig.5. An example of the proposed (2, 2)-3-VSSM model: (a) Decryption of a (2, 2)-3-VSSM model. (b) Relationship graph of a set of blocks.

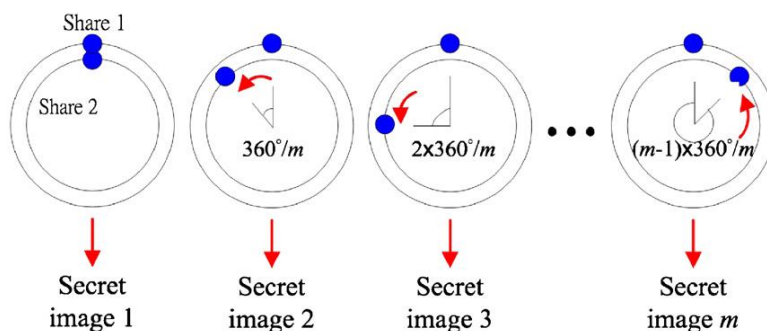


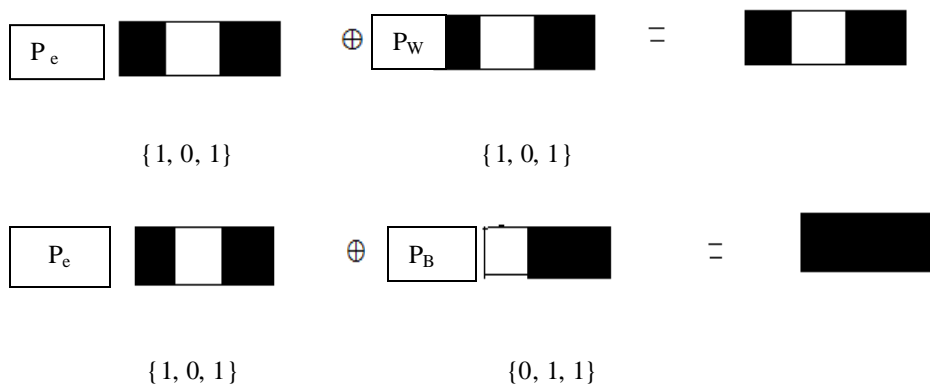
Fig.6. The decryption model of the proposed scheme.

The visual patterns P_e , P_i , P_w , and P_B are used to produce some special features. As shown in Table 2, 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.

Table 2. 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

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. 7.



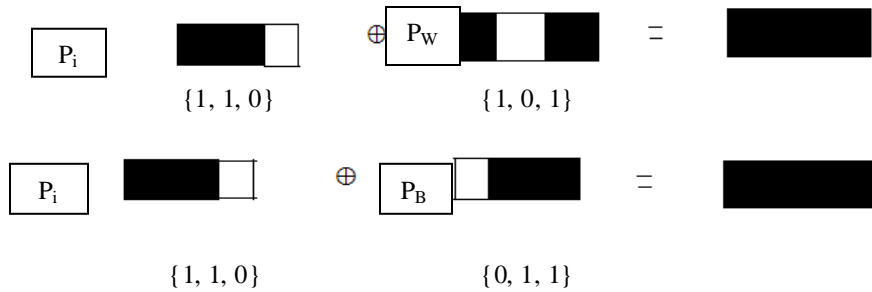


Fig 7. Stacking results of the chosen visual patterns.

The following Fig. 8 shows an example of the (2, 2)-3-VSSM scheme:

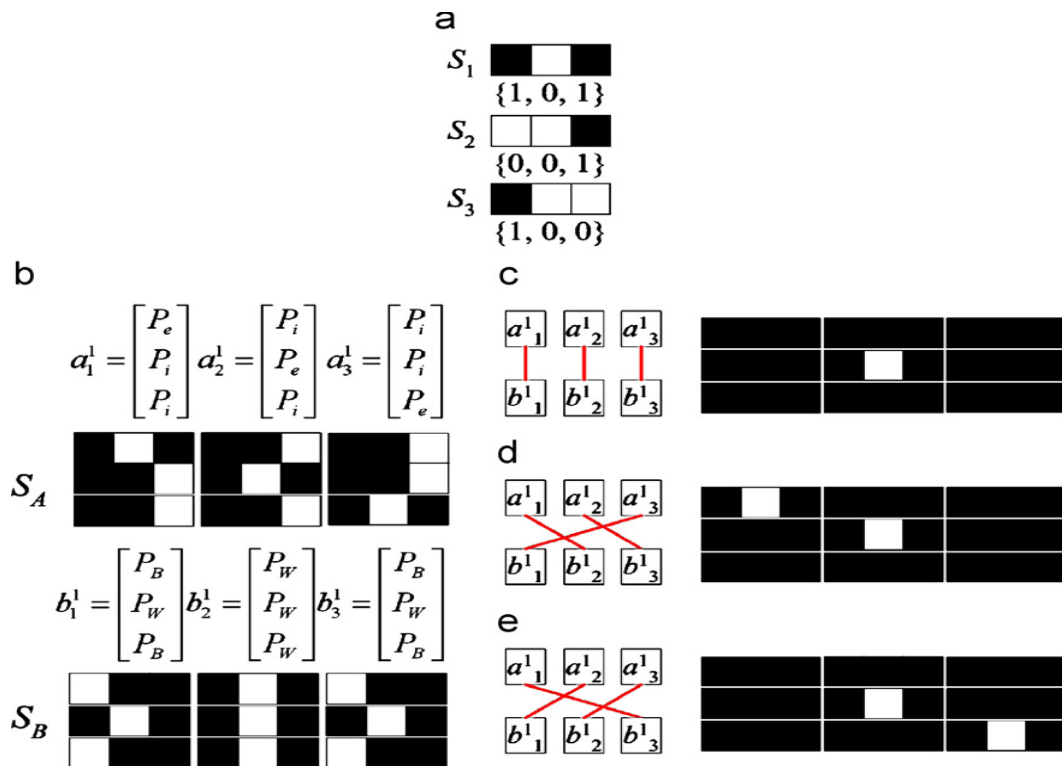


Fig.8: An example of the (2, 2)-3-VSSM scheme: (a) The target secret images. (b) The generated share images. (c) The stacking secret image at normal degree. (d) The stacking secret image at 120°. (e) The stacking secret image at 240°.

VII. Multiple-image encryption by rotating random grids

The features of the Tzung-Her Chen’s multiple-image encryption using random grids scheme are:

- Share many secret images at the same time (up to four secret images)
- No pixel expansion
- Simple but efficient
- Formally proof correctness

7.1 The Proposed Method:

There are two secret images S_A and S_B with the size of $m \times m$ will be encrypted into two cipher-grids G^1 and G^2 with the size of $m \times m$ without any pixel expansion and, later, the secrets can be recovered by directly stacking and rotating one of two cipher-grids at either 90, 180 or 270 degree in the decryption process.

Before describing the details of the encoding process, the related functions are defined as follows:

Definition 1: $f_{RSP}(\cdot): Y \leftarrow f_{RSP}(X)$, Y is the output of the function $f_{RSP}(\cdot)$ with the inputs X , where $f_{RSP}(\cdot)$ is that randomly select a pixel of X .

Definition 2: $f_{RG}(\cdot): Y||Z \leftarrow f_{RG}(X)$, Y and Z are the outputs of the function $f_{RG}(\cdot)$ with the input X, where $f_{RG}(\cdot)$ is the function by the random-grids algorithm which inputs a pixel of the secret image, then outputs two cipher-pixels.

Definition 3: $\bar{f}_{RG}(\cdot): X \leftarrow \bar{f}_{RG}(Y, Z)$, X is the output of the function $\bar{f}_{RG}(\cdot)$ with the inputs Y and Z, where $\bar{f}_{RG}(\cdot)$ is the function based on the random-grids algorithm which inputs a cipher-pixel of cipher-grids and a pixel of the secret image, then outputs the other cipher-pixel.

The diagram of the proposed scheme by rotating random grids is shown in Fig. 9 and the algorithm is described as Algorithm 4 in the encryption phase.

7.2 Encryption phase:

Algorithm 4:

Input: Four binary secret images $S^k = \{S^k(i, j) | S^k(i, j) = 0 \text{ or } 1, 0 \leq i \leq (m-1), 0 \leq j \leq (m-1)\}$ where $k = A, B, C$, and D .
Output: Two cipher-grids $G^p = \{G^p(i, j) | G^p(i, j) = 0 \text{ or } 1, 0 \leq i \leq (m-1), 0 \leq j \leq (m-1)\}$ where $p = 1$ and 2 .

Repeat

//Randomly select a pixel $S^A(i, j)$ to encrypt
 $S^A(i, j) \leftarrow f_{RSP}(S^A)$ //Step 1
 //Encode four secret pixels from S^A, S^B, S^C , and S^D into two cipher-pixels of cipher-grids
 $G^1(i, j) || G^2(i, j) \leftarrow f_{RG}(S^A(i, j))$ //Step 2
 $G^2(j, (m-1)-i) \leftarrow \bar{f}_{RG}(S^B(j, (m-1)-i), G^1(i, j))$ //Step 3
 $G^1(j, (m-1)-i) \leftarrow \text{Random}(\cdot)$ //Step 4
 $G^2((m-1)-j, i) \leftarrow \bar{f}_{RG}(S^C((m-1)-j, i), G^1(j, (m-1)-i))$ //Step 5
 $G^1((m-1)-j, i) \leftarrow \text{Random}(\cdot)$ //Step 6
 $G^2((m-1)-i, (m-1)-j) \leftarrow \bar{f}_{RG}(S^D((m-1)-i, (m-1)-j), G^1((m-1)-j, i))$ //Step 7
 $G^1((m-1)-i, (m-1)-j) \leftarrow \text{Random}(\cdot)$ //Step 8
 Until both cipher-grids are generated completely //Step 9



Fig.9: The diagram of the processes in the encryption phase

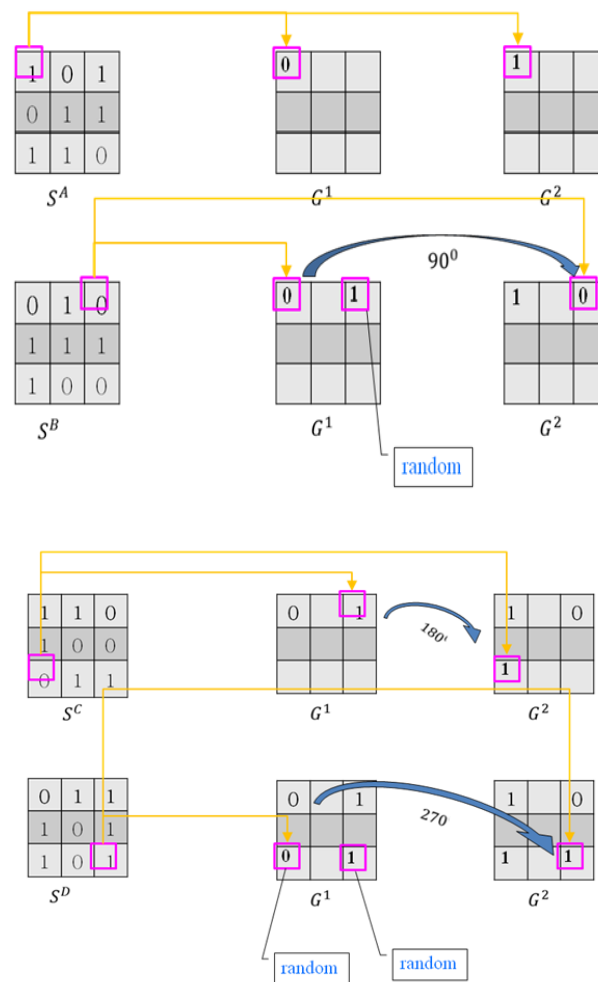


Fig.10: The diagrams of the proposed scheme

After the encryption process, the cipher-grids G^1 and G^2 are generated. The users, receiving one of the two cipher-grids, cannot recognize any secret information from the cipher-grid.

7.3 Decryption phase:

Upon collecting the two cipher-grids, the users can easily recover the first secret image S^A by directly stacking two cipher-grids, the second secret image S^B can be recovered by stacking G^2 and the rotated G^1 right at 90 degrees, the third secret image S^C can be recovered by stacking G^2 and the rotated G^1 right at 180 degrees and the fourth secret image S^D can be recovered by stacking G^2 and the rotated G^1 right at 270 degrees.

VIII. Conclusion

In this paper the comparative study of VC and RG schemes on the basis of various criteria leads to the selection of any one scheme which depends on the pixel expansion factor or improving contrast or number of secret images used where the quality of the reconstructed image is of significance. New VSS and RG techniques are evolving day by day but the selection of these techniques completely relies on the size and the quality of the recovered image. The techniques discussed in this paper mainly promote the contrast and the number of secret images used. The extension of this paper can be on comparing various upcoming VC and RG techniques focusing on the above criteria.

References

- [1]. Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology–Eurocrypt, pp 1-12,1995.
- [2]. C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
- [3]. 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, pp. 996–1001, March 2004.

- [4]. O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. *Optics Letters*, 12:377-379, 1987.
- [5]. Tzung-Her Chen and Kai-Hsiang Tsao, "Visual secret sharing by random grids revisited". *Pattern Recognition*, 42(9):2203 - 2217, 2009. ISSN 0031-3203.
- [6]. C.Blundo, A.De Santis and D. R. Stinson, "On the contrast in visual cryptography schemes", *Journal Cryptology*, vol.12, 1999, pp. 261- 289.
- [7]. J.L.Massey, "Some applications of coding theory in cryptography", in *Cryptography and Coding IV*, Oxford University Press, 1995, pp.33-47.
- [8]. T. H. Chen, and C. S. Wu, "Efficient Multi-secret Image Sharing based on Boolean Operations", *Signal Processing*, Vol. 91, No. 1, (2011), pp. 90-97.
- [9]. Tzung-Her Chen, Kai-Hsiang Tsao, Kuo-Chen 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, Nov. 26-28, 2008.
- [10]. R.Z. Wang, Y.K. Lee, S.Y. Huang, T.L. Chia, "Multilevel visual secret sharing," in: Proceedings of the Second International Conference on Innovative Computing, Information and Control, Kumamoto, Japan, 2007.