



# On the difficulty of aligning VSS random grids



Tzung-Her Chen<sup>a,\*</sup>, Yao-Sheng Lee<sup>a</sup>, Chih-Hung Lin<sup>b</sup>

<sup>a</sup> Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan, ROC

<sup>b</sup> Graduate Institute of Mathematics and Science Education, National Chiayi University, Chiayi 621, Taiwan, ROC

## ARTICLE INFO

### Article history:

Received 28 June 2015

Received in revised form

21 March 2016

Accepted 21 March 2016

Available online 25 March 2016

### Keywords:

Visual cryptography

Random grid

Visual secret sharing

Alignment problem

## ABSTRACT

Visual secret sharing (VSS) schemes are classified into two categories—visual cryptography-based (VC) and random grid-based (RG)—with the purpose of encoding a secret into several meaningless shared images that can be superimposed to reveal the secret again. VC-based VSS suffers from the problems of pixel expansion and difficulty in alignment. Although the first problem has been solved by RG-based VSS, the latter remains. This paper proposes a new deviation-tolerant RG-based VSS method without pixel expansion. To demonstrate its feasibility, experiments are conducted to show that the reconstructed secret image is still recognizable visually when one shared image shifts by one or more pixels. Compared with related works, the proposed scheme not only has higher misalignment tolerance but also avoids the significant drawbacks in the related work.

© 2016 Elsevier B.V. All rights reserved.

## 1. Introduction

In 1995, Naor and Shamir [10] proposed the  $(k,n)$  visual cryptography (VC) technique, in which a secret image is divided into  $n$  meaningless shares. In the decoding phase,  $k$  shares are collected and then superimposed directly. The secret over the superimposed result can be recognized by the human visual system.

Inspired by VC, an increasing number of applications have been proposed. For example, instead of binary images, many studies have proposed encoding gray-level images [6,18] and color images [1,2,7]. However, the size of the generated shared images is at least four times larger than the secret image. Thus, some studies [13,14,16] have tried to solve the pixel-expansion problem.

As claimed in [3,12], the traditional VC technique has two main drawbacks: (1) pixel expansion, and (2) the need for a tailor-made codebook. In its attempt to avoid the codebook-design and pixel-expansion problems, the VSS scheme of binary secret images by random grids (RG) presented by Kafri and Keren [8] in 1987 drew the attention of academia. In the encoding phase, all grid-pixels in the first random grid are generated by a coin-flip function, and every grid-pixel in the other random grid is generated according to a certain pixel of the secret image and the corresponding grid-pixel in the first random grid; the result is that the size of the generated random grid is the same as that of the secret image.

Inspired by Kafri and Keren's scheme, Shyu (2007) [11] proposed another RG-based VSS scheme to deal with gray-level and color images. To remove the limitations of the  $(2,2)$  RG-based VSS [8,11], Chen and Tsao [3,4] and Shyu [12] proposed their own  $(2,n)$ ,

$(k,n)$  and  $(n,n)$  schemes established with RG-based VSS. Furthermore, an easy-to-manage RG-based VSS scheme was presented by Chen and Tsao [5]. It is also a new trend to recover the secret in multiple ways [20].

No matter whether a scheme is VC-based or RG-based, VSS must align the shares precisely in the decoding phase. The traditional VC solves the alignment problem by adding a solid frame to help align the shares. In 2004, Yan et al. [15] proposed a novel method of embedding invisible alignment marks by Walsh transform to help align the shares precisely.

However, whether a solid frame or a mark is used, one still needs to align the shares precisely. In 2009, Liu et al. [9] presented the alignment-tolerant VC-based VSS scheme that does not require the shares to be precisely aligned when reconstructing the secret image. Their scheme assumes that the factor of pixel expansion is  $m$ , and the secret can be disclosed when one share shifts at most  $m-1$  pixels. Another scheme proposed by Yang et al. [17] in 2009 adopted two subpixels of different sizes (the “big” and “small” blocks) to generate the shares, and the secret can be disclosed even if some shares are misaligned, although the big block is more robust to the misalignment error than the small block. However, Yang et al.'s scheme [17] will lead to incorrect reconstruction of the secret image if there is a slight misalignment (see Section 4), and the visual quality of the reconstructed image will diminish as the misalignment deviation increases. Although Wang et al. [19] presented a quality-enhanced scheme compared with Liu et al.'s [9] and Yang et al.'s [17], their scheme still suffers from the potential disadvantages from VC.

This paper proposes a new RG-based VSS method to overcome the misalignment problem. The method has four primary advantages: (1) recovering the secret image without the need to

\* Corresponding author.

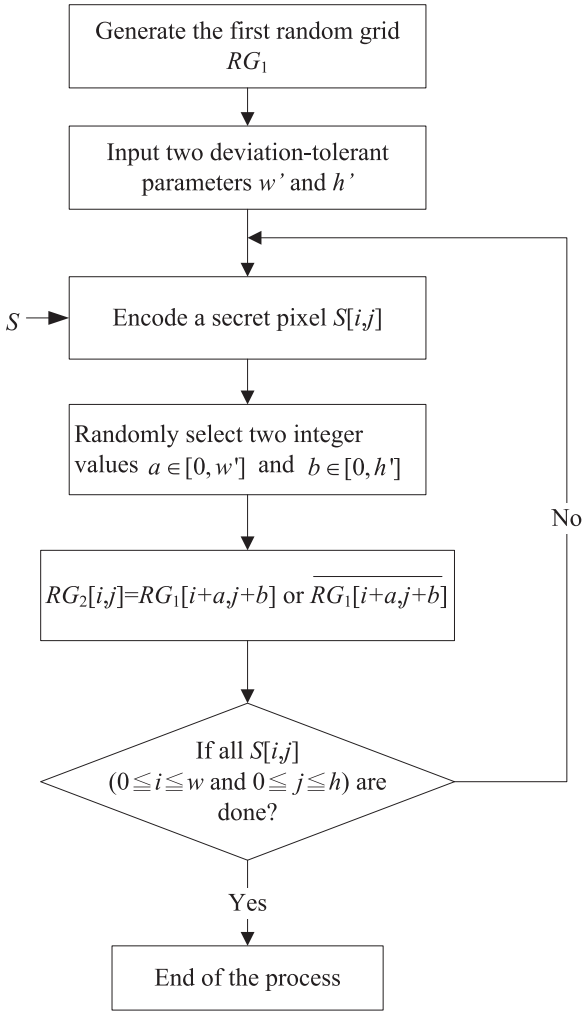


Fig. 1. the processes of encoding a secret image.



Fig. 2. Secret image with the size of 1024 × 1024.

The rest of this paper is organized as follows. The proposed method is described in the next section. The analysis of security and visual quality is given in Section 3. The experimental results and discussions are presented in Sections 4 and 5, and Section 6 concludes.

## 2. The proposed scheme

The proposed RG-based VSS scheme with high deviation tolerance is extended from Kafri and Keren's [8] method. A secret image  $S$  is encoded into two random-grids  $RG_1$  and  $RG_2$ .

A secret image  $S = \{S[i,j] | S[i,j] = 0 \text{ or } 1, 1 \leq i \leq w, 1 \leq j \leq h\}$  in which the value "0" or "1" is used to represent a transparent or opaque pixel, and two pre-defined parameters  $w'$  and  $h'$  are chosen as inputs, where  $w'$  and  $h'$  denote the amount of pixel-shift tolerance in width and height, respectively. The information of a secret image should appear with smooth areas (not texture) such as characters and logos of simple shape. The proposed scheme outputs two meaningless random-grids  $RG_k = \{RG_k[i,j] | RG_k[i,j] = 0 \text{ or } 1, 1 \leq i \leq w, 1 \leq j \leq h\}$  ( $k=1,2$ ) with the same size as  $S$ . In the decoding process, two random grids are superimposed and can be aligned and recognized by the human visual system without extra computational cost.

The process of encoding a secret image is illustrated in Fig. 1. First, the random grid  $RG_1$  is generated by a coin-flip function. Second, the secret image and two pre-defined parameters  $w'$  and  $h'$ , called the deviation-tolerance factors, are chosen as inputs to encode a secret pixel  $S[i,j]$ . The pixel value  $RG_2[i,j]$  of random grid  $RG_2$  is generated according to the two random values  $a$  and  $b$ , and the secret pixel.

The encoding process encompasses the following operations.

**Step 1:** All pixels  $RG_1[i,j] \in RG_1$  are assigned the values 0 or 1, which are randomly selected by a coin-flip function.

**Step 2:** Two deviation-tolerance factors  $w'$  and  $h'$  are determined.

**Step 3:** For each grid-pixel  $RG_2[i,j]$ , the following two steps are performed.

**Step 3.1** Randomly generate two integer values  $a$  and  $b$ , where  $a \in [0, w']$  and  $b \in [0, h']$ .

**Step 3.2** Generate  $RG_2$  by the following rules.

If  $S[i, j] = 0$ ,  $RG_2[i, j] = RG_1[i + a, j + b]$ ;  
otherwise,  $RG_2[i, j] = \overline{RG_1[i + a, j + b]}$ .

**Step 4:** Repeat Step 3 until all random-pixels  $RG_2[i, j]$  are obtained.

The algorithm of the proposed encoding process is illustrated below.

**Input:** a secret image  $S = \{S[i,j] | S[i,j] = 0 \text{ or } 1, 1 \leq i \leq w, 1 \leq j \leq h\}$  and two deviation-tolerant factors  $w'$  and  $h'$

**Output:** two meaningless random-grids  $RG_k = \{RG_k[i,j] | RG_k[i, j] = 0 \text{ or } 1, 1 \leq i \leq w, 1 \leq j \leq h\}$  ( $k=1,2$ )

$RG_1[i,j] \leftarrow 0 \text{ or } 1$  for all  $i$  and  $j$

For  $i = 1$  to  $w, j = 1$  to  $h$

Generate two random integers  $a$  and  $b$ , where

$a \in [0, w']$  and  $b \in [0, h']$ .

If  $S[i, j] = 0$

$RG_2[i,j] \leftarrow RG_1[i + a, j + b]$

else

$RG_2[i,j] \leftarrow \overline{RG_1[i + a, j + b]}$

//Step 1

//Step 3

//Step 3.1

//Step 3.2

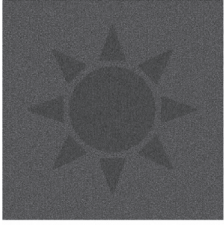

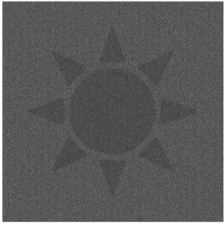

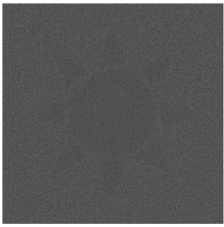

//Step

3.2.1

//Step

3.2.2

align the shares precisely, (2) removing the problem of pixel expansion, (3) removing the need for a redesigning codebook, and (4) removing the drawback of decreased visual quality. Compared with related work, the proposed scheme has higher tolerance for misalignment.

scheme $\langle x, y \rangle$	Yang et al.'s [17]	Proposed scheme with $\langle w', h' \rangle = \langle 1, 1 \rangle$
$\langle 0, 1 \rangle$	 (a)	 (d)
$\langle 1, 0 \rangle$	 (b)	 (e)
$\langle 1, 1 \rangle$	 (c)	 (f)

**Fig. 3.** Comparison of the visual quality between the proposed scheme and Yang et al.'s scheme: (a–c) the experimental results using Yang et al.'s scheme with the size of  $2048 \times 2048$ ; (d–f) the experimental results using the proposed scheme with the size of  $1024 \times 1024$  and  $\langle w', h' \rangle = \langle 1, 1 \rangle$ .

Thanks to the design of the high misalignment tolerance, the stacking process becomes easier.

### 3. Performance analysis

Before analyzing theoretically the performance of the method in terms of security and visual quality, some definitions are useful:

















**Definition 1.** (Light transmission)

For a certain pixel  $p$  in binary image  $R$ , the light transmission of a transparent (resp. opaque) pixel  $p \in R$  is defined as  $l[p]=1$  (resp.  $l[p]=0$ ). The average light transmission of  $R$  with the size of  $w \times h$  is defined as  $L[R] = \frac{1}{w \times h} \sum_{i=1}^w \sum_{j=1}^h l[p[i, j]]$ .

**Definition 2.** (Contrast)

The contrast  $\sigma = \frac{L[R[S_{(0)}]] - L[R[S_{(1)}]]}{1 + L[R[S_{(1)}]]}$  is defined to estimate the visual quality of the reconstructed image  $R$  for a secret image  $S$ , where  $L[R[S_{(0)}]]$  (resp.  $L[R[S_{(1)}]]$ ) denotes the average light transmission of the partial area in  $R$ , which corresponds to the transparent (resp. opaque) area in  $S$ .

The reconstructed binary image  $R$  is recognized as the secret image  $S$  when the contrast  $\sigma > 0$ . The case  $L[R[S_{(0)}]] > L[R[S_{(1)}]]$  means  $R$  can be recognized as  $S$  visually since it causes  $\sigma$  to be

scheme $\langle x, y \rangle$	Yang et al.'s [17]	Proposed scheme with $\langle w', h' \rangle = \langle 2, 2 \rangle$
$\langle 0, 1 \rangle$	 (a)	 (i)
$\langle 1, 0 \rangle$	 (b)	 (j)
$\langle 1, 1 \rangle$	 (c)	 (k)
$\langle 0, 2 \rangle$	 (d)	 (l)
$\langle 1, 2 \rangle$	 (e)	 (m)
$\langle 2, 0 \rangle$	 (f)	 (n)
$\langle 2, 1 \rangle$	 (g)	 (o)
$\langle 2, 2 \rangle$	 (h)	 (p)

**Fig. 4.** Comparison of the visual quality between the proposed and Yang et al.'s scheme: (a–h) the experimental results with the size of  $2048 \times 2048$  of Yang et al.'s scheme, (i–p) the experimental results with the size of  $1024 \times 1024$  of the proposed scheme with  $\langle w', h' \rangle = \langle 2, 2 \rangle$ .

positive. On the other hand, if  $L[R[S_{(0)}]] = L[R[S_{(1)}]]$ ,  $R$  is meaningless.

**Lemma 1.** The bit-wise OR operation over random-grids has the following properties:

- (1) When superimposing two identical random-grids  $RG$  as

Secret pixel	□						■					
Share 1												
Share 2												
Stacked results												

(a) A VC codebook

Secret pixel	□						■					
Share 1												
Share 2												
Stacked results												

(b) The VC codebook with a one-pixel horizontal deviation

**Fig. 5.** Comparison of the stacked results between the generic VC and Yang et al.'s VC [17], adopting small blocks with a one-pixel horizontal deviation. (a) A VC codebook. (b) The VC codebook with a one-pixel horizontal deviation.

**Table 1**

Numbers of white and black pixels in a specific area of a reconstructed image and the contrast with the first experiment

< x,y > Parameter	< 0,0 >	< 0,1 >	< 1,0 >	< 1,1 >
# of black pixels in $R[S_{(1)}]$	176759	176449	176498	176290
# of white pixels in $R[S_{(1)}]$	40259	40569	40520	40728
# of black pixels in $R[S_{(0)}]$	571838	572180	571577	571605
# of white pixels in $R[S_{(0)}]$	259720	259378	259981	259953
$L(R[S_{(1)}])$	0.185510	0.186938	0.186713	0.187671
$L(R[S_{(0)}])$	0.312329	0.311918	0.312643	0.312610
Experimental $\sigma$	0.106975	0.105296	0.106117	0.105196
Theoretic $\sigma$	$\frac{2}{19} = 0.1053$	$\frac{2}{19} = 0.1053$	$\frac{2}{19} = 0.1053$	$\frac{2}{19} = 0.1053$

$RG \oplus RG$ , where the operation  $\oplus$  is denoted as bit-wise OR operation, the result of  $RG \oplus RG$  is identical to  $RG$ .

- (2) When superimposing two inverse random-grids denoted  $RG \oplus \overline{RG}$ , where  $\overline{RG}$  is the bit-wise complement of  $RG$ , the result of  $RG \oplus \overline{RG}$  is fully black.

**Lemma 2.** If superimposing two independent grids  $RG_1$  and  $RG_2$ , which are generated by a coin-flip function to form a stacked image  $RG_{1 \oplus 2}$ , the expected average light transmission of  $L[RG_{1 \oplus 2}]$  is  $(\frac{1}{2})^2$ .

**Proof.** Let  $p_1$  be a certain pixel of random grid  $RG_1$ , and  $p_2$  be the corresponding pixel at the same position in  $RG_2$ . If each pixel in  $RG_1$  or  $RG_2$  is generated by a coin-flip function, its probability of generating a black or white pixel is  $\frac{1}{2}$ . If superimposing two grid-pixels  $p_1$  and  $p_2$  as  $p_{1 \oplus 2}$ , the probability of obtaining a white pixel is  $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ , so  $L[RG_{1 \oplus 2}] = \frac{1}{w \times h} \sum_{i=1}^w \sum_{j=1}^h (\frac{1}{2} \times \frac{1}{2}) = \frac{1}{4}$  by Definition

**Table 2**

Comparison between related works and the proposed scheme.

Schemes	Kernel technique	Pixel expansion	Need to align precisely	Misalignment tolerance
Naor and Shamir [10]	VC	4	Yes	N/A
Zhou et al. [18]	VC	4	Yes	N/A
Droste [6]	VC	4	Yes	N/A
Ateniese et al. [1]	VC	4	Yes	N/A
Jin et al. [7]	VC	4	Yes	N/A
Chang et al. [2]	VC	9	Yes	N/A
Tu and Hou [14]	VC	1	Yes	N/A
Yang [16]	VC	1	Yes	N/A
Kafri and Keren [8]	RG	1	Yes	N/A
Shyu [11]	RG	1	Yes	N/A
Chen and Tsao [3]	RG	1	Yes	N/A
Shyu [12]	RG	1	Yes	N/A
Yan et al. [15]	VC	4	Yes	N/A
Shyu [13]	VC	> 1	Yes	N/A
Chen and Tsao [4]	RG	1	Yes	N/A
Chen and Tsao [5]	RG	1	Yes	N/A
Liu et al. [9]	VC	$m$	No	$m-1$
Yang et al. [17]	VC	4	No	$< \alpha, \alpha >$
Proposed scheme	RG	1	No	$< w', h' >$

$\alpha$  – the ratio of the size of “big block” subpixel to that of “small block” subpixel.

$m$  – the ratio of pixel expansion.

1.

**Assumption 1.** Two random-grids  $RG_1$  and  $RG_2$  generated by the proposed scheme are assumed to divide into  $(w' + 1) \times (h' + 1)$  sub-random-grids  $RG_k^i$ , where  $k=1,2$  and  $i=1,2,\dots,(w' + 1) \times (h' + 1)$ . More precisely,

$$RG_k = RG_k^1 \cup RG_k^2 \cup \dots \cup RG_k^{(w'+1) \times (h'+1)} = \bigcup_{i=1}^{(w'+1) \times (h'+1)} RG_k^i$$

and

$$RG_k^1 \cap RG_k^2 \cap \dots \cap RG_k^{(w'+1) \times (h'+1)} = \emptyset.$$

The expected number of pixels in  $RG_k^i$  is  $\frac{w \times h}{(w' + 1) \times (h' + 1)}$ , and the parameters  $w'$  and  $h'$  affect the visual quality of the reconstructed image. The larger the value of  $w' \times h'$ , the worse the visual quality of the reconstructed image.

**Lemma 3.** Superimposing a pair of sub-random-grids  $RG_1^i$  and  $RG_2^i$ , the expected contrast of the superimposed result  $R^i = RG_1^i \oplus RG_2^i$  is  $\frac{1}{2}$ , which is high enough to reveal the secret information of the secret image  $S$ .

**Proof.** By Assumption 1,  $RG_1$  and  $RG_2$  are divided into  $(w' + 1) \times (h' + 1)$  sub-random-grids, respectively. Each sub-random-grid is encoded to deal with a deviation. Since the encoding process for each secret pixel is done according to the traditional random-grid VSS algorithm, we have:  $R^i[S_{(0)}^i] = RG_1^i[S_{(0)}^i] \oplus RG_2^i[S_{(0)}^i] = RG_1^i[S_{(0)}^i] \oplus RG_1^i[S_{(0)}^i] = RG_1^i[S_{(0)}^i]$  by Lemma 1(1) and  $R^i[S_{(1)}^i] = RG_2^i[S_{(1)}^i] \oplus RG_2^i[S_{(1)}^i] = RG_2^i[S_{(1)}^i]$ , meaning it is fully black by Lemma 1 (2). Hence, the expected average light transmissions of the corresponding areas in  $R^i$  with respect to the white and black

$$\text{areas in } S^i \text{ are } L[R^i[S_{(0)}^i]] = \frac{1}{\frac{w \times h}{(w' + 1) \times (h' + 1)}} \sum_{i=1}^{(w'+1)} \sum_{j=1}^{(h'+1)} \left(\frac{1}{2}\right) = \frac{1}{2} \text{ and}$$

$$L[R^i[S_{(1)}^i]] = \frac{1}{\frac{w \times h}{(w' + 1) \times (h' + 1)}} \sum_{i=1}^{(w'+1)} \sum_{j=1}^{(h'+1)} 0 = 0, \text{ respectively. Here,}$$

$$\text{the contrast of } R^i = \frac{L[R^i[S_{(0)}^i]] - L[R^i[S_{(1)}^i]]}{1 + L[R^i[S_{(1)}^i]]} = \frac{\frac{1}{2} - 0}{1 + 0} = \frac{1}{2} > 0.$$

**Lemma 4.** The average light transmission  $L[RG_k]$  of binary random-grids  $RG_k$  is  $\frac{1}{(w' + 1) \times (h' + 1)} \times L[RG_k^i] + (1 - \frac{1}{(w' + 1) \times (h' + 1)}) \times L[RG_k^j]$ , where  $RG_k^j = RG_k - RG_k^i$ .

**Proof.** By Definition 1, the average light transmission of binary random-grids  $RG_k$  is  $\frac{1}{w \times h} \sum_{rg_k \in RG_k} l(rg_k)$ . By Assumption 1,  $RG_k^i$ , with the respective size of  $(w' + 1) \times (h' + 1) - 1$  times of  $RG_k^i$ , is known, so

$$\begin{aligned} L[RG_k] &= \frac{1}{w \times h} \left( \sum_{all rg_k \in RG_k^i} l(rg_k) + \sum_{all rg_k \in RG_k^j} l(rg_k) \right) \\ &= \frac{1}{\frac{w \times h}{(w' + 1) \times (h' + 1)}} \sum_{all rg_k \in RG_k^i} l(rg_k) \\ &\quad + \frac{1}{((w' + 1) \times (h' + 1) - 1) \times \frac{w \times h}{(w' + 1) \times (h' + 1)}} \sum_{all rg_k \in RG_k^j} l(rg_k) \\ &= \frac{1}{(w' + 1) \times (h' + 1)} \times L[RG_k^i] + \left( 1 - \frac{1}{(w' + 1) \times (h' + 1)} \right) \\ &\quad \times L[RG_k^j]. \end{aligned}$$

**Theorem 1.** (Contrast)

The expected contrast of the reconstructed result from stacking two random-grids, for example,  $R = RG_1 \oplus RG_2$ , in the proposed scheme is greater than zero.

**Proof.** Reconstructing the secret image  $S$  has the probability of  $\frac{1}{(w' + 1) \times (h' + 1)}$  to disclose the secret and the probability of  $1 - \frac{1}{(w' + 1) \times (h' + 1)}$  to deal with the shift problem when pixels shift.

In the proposed scheme,  $\frac{w \times h}{(w' + 1) \times (h' + 1)}$  pixels in each sub-random-grid are used to disclose the reconstructed secret since the encoding process for each secret pixel was done according to the traditional random-grid VSS algorithm. When the secret pixel is white (black), the expected light transmission of the stacked pixel is  $\frac{1}{2}$  (0) by Lemma 3. The remaining  $w \times h - \frac{w \times h}{(w' + 1) \times (h' + 1)}$  pixels are encoded to deal with the misalignment operations. Without losing the generality, assume the sub-random-grid  $RG_k^x$  ( $1 \leq x \leq (w' + 1)(h' + 1)$ ) is used to reveal the secret when superimposing the two sub-random-grids precisely. The pixels in  $RG_2^x$  and those in  $RG_1^x$  are independent when one random grid shifts.

Likewise, it has  $w \times h - \frac{w \times h}{(w' + 1) \times (h' + 1)}$  unallied pixels when two random grids are stacked by the proposed scheme. Therefore, its expected average light transmission is  $\frac{1}{4}$  by Lemma 2. The random grid  $RG_k$  is divided into  $(w' + 1) \times (h' + 1)$  sub-random-grids, and one pair of sub-random-grids—say,  $RG_1^i$  and  $RG_2^i$ —is used to reveal the secret image while the other  $(w' + 1) \times (h' + 1) - 1$  pairs—say,  $RG_1^j$  and  $RG_2^j$ —are used to deal with deviations. The size of  $RG_k^i$  is  $(w' + 1) \times (h' + 1) - 1$  times the size of  $RG_k^j$ . The average light transmission can be obtained by Lemma 4.

$$\begin{aligned} L[R[S_{(0)}]] &= \frac{1}{(w' + 1) \times (h' + 1)} \times L[RG_k^i[S_{(0)}]] \\ &\quad + \left( 1 - \frac{1}{(w' + 1) \times (h' + 1)} \right) \times L[RG_k^j[S_{(0)}]] \\ &= \frac{1}{(w' + 1) \times (h' + 1)} \times \frac{1}{2} + \left( 1 - \frac{1}{(w' + 1) \times (h' + 1)} \right) \times \frac{1}{4} \\ &= \frac{(w' + 1) \times (h' + 1) + 1}{4(w' + 1) \times (h' + 1)} \end{aligned}$$

$$\begin{aligned} L[R[S_{(1)}]] &= \frac{1}{(w' + 1) \times (h' + 1)} \times L[RG_k^i[S_{(1)}]] \\ &\quad + \left( 1 - \frac{1}{(w' + 1) \times (h' + 1)} \right) \times L[RG_k^j[S_{(1)}]] \\ &= \frac{1}{(w' + 1) \times (h' + 1)} \times 0 + \left( 1 - \frac{1}{(w' + 1) \times (h' + 1)} \right) \times \frac{1}{4} \\ &= \frac{(w' + 1) \times (h' + 1) - 1}{4(w' + 1) \times (h' + 1)} \end{aligned}$$

Therefore, we have the contrast

$$\begin{aligned} \sigma &= \frac{L[R[S_{(0)}]] - L[R[S_{(1)}]]}{1 + L[R[S_{(1)}]]} = \frac{\frac{(w' + 1) \times (h' + 1) + 1}{4(w' + 1) \times (h' + 1)} - \frac{(w' + 1) \times (h' + 1) - 1}{4(w' + 1) \times (h' + 1)}}{1 + \frac{(w' + 1) \times (h' + 1) - 1}{4(w' + 1) \times (h' + 1)}} \\ &= \frac{2}{4(w' + 1) \times (h' + 1) + (w' + 1) \times (h' + 1) - 1} \\ &= \frac{2}{5(w' + 1) \times (h' + 1) - 1} > 0. \end{aligned}$$



Finally, the proof is obtained.

### Theorem 2. (Security)

The proposed scheme is secure because no random-grid,  $RG_1$  or  $RG_2$ , alone reveals information about the secret  $S$ .

**Proof.**  $RG_1$  is divided into  $(w' + 1) \times (h' + 1)$  sub-random-grid  $RG_1^i$  ( $i=1,2,\dots,(w' + 1) \times (h' + 1)$ ). By Assumption 1, each pixel in  $RG_1^i$  is generated by a coin-flip function with the probability of generating a black or white pixel being  $\frac{1}{2}$ . The average light transmission of the corresponding area in  $RG_1^i$ , with respect to the white (black) area in the secret image  $S^i$ , is  $L[RG_1^i[S^i_{(0)}]] = \frac{1}{2}$  ( $L[RG_1^i[S^i_{(1)}]] = \frac{1}{2}$ ). Consequently, with the random-grid  $RG_1$  alone, the contrast of  $RG_1$  is  $\frac{L[RG_1[S_{(0)}]] - L[RG_1[S_{(1)}]]}{1 + L[RG_1[S_{(1)}]]} = \frac{\frac{1}{2} - \frac{1}{2}}{1 + \frac{1}{2}} = 0$ . By Definition 2,  $RG_1$  is meaningless, so no secret information can be visually recognized by only  $RG_1$ . According to Assumption 1,  $RG_2$  is divided into  $(w' + 1) \times (h' + 1)$  groups  $RG_2^i$ . By Step 3.2.1,  $RG_2^i[S^i_{(0)}]$  is equal to  $RG_1^i[S^i_{(0)}]$ , the average light transmission of  $RG_2^i[S^i_{(0)}]$  is  $L[RG_2^i[S^i_{(0)}]] = L[RG_1^i[S^i_{(0)}]] = \frac{1}{2}$ , the  $RG_2^i[S^i_{(1)}]$  is generated by Step 3.2.2, and the average light transmission of  $RG_2^i[S^i_{(1)}]$  is  $L[RG_2^i[S^i_{(1)}]] = \overline{L[RG_1^i[S^i_{(1)}]]} = \frac{1}{2}$ , where  $RG_1^i$  and  $RG_2^i$  are located in the same positions in  $RG_1$  and  $RG_2$ , respectively. Each sub-random-grid encoded with the same algorithm by Step 3.2. has the same average light transmission in every sub-random-grid. We can obtain the average light transmission  $L[RG_2[S_{(0)}]] = L[RG_2[S_{(1)}]] = \frac{1}{2}$ . With the random-grid  $RG_2$  alone, the contrast of  $RG_2$  is  $\sigma = \frac{L[RG_2[S_{(0)}]] - L[RG_2[S_{(1)}]]}{1 + L[RG_2[S_{(1)}]]} = \frac{\frac{1}{2} - \frac{1}{2}}{1 + \frac{1}{2}} = 0$ . By Definition 2,  $RG_2$  is also meaningless.

## 4. Experimental results

To demonstrate the method's feasibility, the experimental results are compared with results from related work.

A secret image  $S$ , shown in Fig. 2, of size  $1024 \times 1024$  pixels is encoded by the proposed method to generate two random-grids  $RG_1$  and  $RG_2$  with the same size as  $S$ .

**Simulation 1.** Comparison between the related work and the proposed.

Figs. 3 and 4 show the comparison in terms of various visual quality between the proposed scheme and Yang et al.'s scheme [17], using 50% big blocks and 50% small blocks. In Fig. 3 and Fig. 4,  $x$  is the horizontal deviation and  $y$  is the vertical deviation. Two experiments with  $\langle w', h' \rangle = \langle 1, 1 \rangle$  and  $\langle w', h' \rangle = \langle 2, 2 \rangle$  are conducted. If one share shifts within the pre-defined deviation, the reconstructed secret image is still recognizable without pixel expansion. The present scheme is superior to Yang et al.'s in terms of the size of share images.

Although Yang et al.'s experimental results and the proposed experimental results illustrate that the secrets can be visually recognizable, the former suffer some problem illustrated below.

### 4.1. Problem of the related work

In Yang et al.'s scheme, it is clear that the reconstructed secrets appear like a white sun (Fig. 4(d)–(f)) instead of the original black

one (Fig. 4(a)–(c)). This drawback comes from the “small block” design. Taking (2,2)-VC as an example, there are six cases for encoding a white secret pixel and a black one, as shown in Fig. 5(a). It is evident that the stacked results in the white cases are all brighter than those in the black cases. We use the horizontal deviations with one pixel to test the misalignment tolerance, as shown in Fig. 5(b). The stacked results in the white cases are, on average, darker than those in the black cases such that the color of the reconstructed secrets changes by mistake.

The design of “big” blocks in [17] was aimed at increasing the misalignment tolerance, but it decreased the quality of reconstructed secrets. From Fig. 4(a–c) and (d–f), the visual quality of the reconstructed secrets worsens slightly.

The experimental results of the proposed scheme illustrate the following advantages: (1) no pixel expansion, (2) fixed visual quality, and (3) correct reconstruction of the secret. However, Yang et al.'s scheme reconstructs the wrong secret, i.e., reconstructs a different color, unless the design of “big” blocks is adopted.

### Simulation 2. Correctness of Theorem 1

To examine the correctness of theoretical contrast by Theorem 1, the experimental contrast is computed. Table 1 shows that the values of the experimental and theoretical contrast in the first experiment, with the size of  $1024 \times 1024$ , are nearly identical in the last two rows. Indeed, the theoretical value of contrast is an approximate value, not possible maximum, if the pseudo randomness is achieved under generating random-grids. In Table 1,  $R$  refers to the stacked result of superimposing random grids to reconstruct the secret, and the notation # denotes the number of pixels in a specific area. The value  $\langle x, y \rangle$ , where  $0 \leq x \leq w'$  and  $0 \leq y \leq h'$ , means that one of the share images shifted to the right by  $x$  pixels and down by  $y$  pixels during decoding.

## 5. Discussion

The main advantages of the proposed scheme, as compared with related work, are depicted in Table 2. The superiority of the proposed scheme includes that the size of the generated random-grids is identical to that of the original secret and that it has high misalignment tolerance in the decoding phase.

Inspired by Kafri and Keren's [8] and Shyu's [11] schemes, the kernel technique of the proposed scheme is built upon the RG-based VSS. In this situation, the proposed scheme can still satisfy the advantages of RG-based VSS. Moreover, Kafri and Keren's [8] and Shyu's [11] schemes can be regarded as a special case of the proposed scheme when  $\langle w', h' \rangle = \langle 0, 0 \rangle$ .

Furthermore, inspired by Chen and Tsao's threshold scheme [4], the proposed scheme can be extended the (2,2) case to the  $(k, n)$ .

## 6. Conclusion

This paper proposes an effective random-grid-based VSS scheme that can reconstruct the secret when one share is not aligned precisely. The proposed scheme demonstrates superiority to related work. To the best of our knowledge, this is the first attempt in academia to achieve the goal of solving the alignment problem without suffering the pixel expansion problem.

## References

- [1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended capabilities for visual cryptography, *Theor. Comput. Sci.* 250 (2001) 134–161.
- [2] C.C. Chang, W.L. Tai, C.C. Lin, Hiding a secret colour image in two colour images, *Imaging Sci. J.* 53 (2005) 229–240.
- [3] T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, *Pattern Recognit.* 42 (2009) 2203–2217.
- [4] T.H. Chen, K.H. Tsao, Threshold visual secret sharing by random grids, *J. Syst. Softw.* 84 (2011) 1197–1208.
- [5] T.H. Chen, K.H. Tsao, User-friendly random grid-based visual secret sharing, *IEEE Trans. Circuits Syst. Video Technol.* 21 (2011) 1693–1703.
- [6] S. Droste, New results on visual cryptography, in: *Proceedings of Advances in Cryptology: CRYPTO 96, Lecture Notes in Computer Science*, vol. 1109, 1996, pp. 401–415.
- [7] D. Jin, W.Q. Yan, M.S. Kankanhalli, Progressive color visual cryptography, *J. Electron. Imaging* 14 (2005) 033019.
- [8] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, *Opt. Lett.* 12 (1987) 377–379.
- [9] F. Liu, C.K. Wu, X.J. Lin, The alignment problem of visual cryptography schemes, *Des., Codes Cryptogr.* 50 (2009) 215–227.
- [10] M. Naor, A. Shamir, Visual cryptography, in: *Proceedings of Advances in Cryptology: EUROCRYPT94, Lecture Notes in Computer Science*, vol. 950, 1995, pp. 1–12.
- [11] S.J. Shyu, Image encryption by random grids, *Pattern Recognit.* 40 (2007) 1014–1031.
- [12] S.J. Shyu, Image encryption by multiple random grids, *Pattern Recognit.* 42 (2009) 1582–1596.
- [13] S.J. Shyu, M.C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes, *IEEE Trans. Inf. Forensics Secur.* 6 (2011) 960–969.
- [14] S.F. Tu, Y.C. Hou, Design of visual cryptographic methods with smooth looking decoded images of invariant size for grey-level images, *Imaging Sci. J.* 55 (2007) 90–101.
- [15] W.Q. Yan, D. Jin, M.S. Kankanhalli, Visual cryptography for print and scan applications, in: *Proceedings of the International Symposium on Circuits and Systems, ISCAS*, vol. 5, 2004, pp. 572–575.
- [16] C.N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognit. Lett.* 25 (2004) 481–494.
- [17] C.N. Yang, A.G. Peng, T.S. Chen, MTVSS: misalignment tolerant visual secret sharing on resolving alignment difficulty, *Signal Process.* 89 (2009) 1602–1624.
- [18] Z. Zhou, G.R. Arce, G.D. Crescenzo, Halftone visual cryptography, *IEEE Trans. Image Process.* 15 (2006) 2441–2453.
- [19] D. Wang, L. Dong, X. Li, Towards shift tolerant visual secret sharing schemes, *IEEE Trans. Inf. Forensics Secur.* 6 (2011) 323–337.
- [20] X. Wu, W. Sun, Random grid-based visual secret sharing with abilities of OR and XOR decryptions, *J. Vis. Commun. Image Represent.* 24 (2013) 48–62.