Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

# On the difficulty of aligning VSS random grids

Tzung-Her Chen [a,*], Yao-Sheng Lee [a], Chih-Hung Lin [b]

[a] *Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan, ROC*
[b] *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.

http://dx.doi.org/10.1016/j.image.2016.03.006
0923-5965/© 2016 Elsevier B.V. All rights reserved.

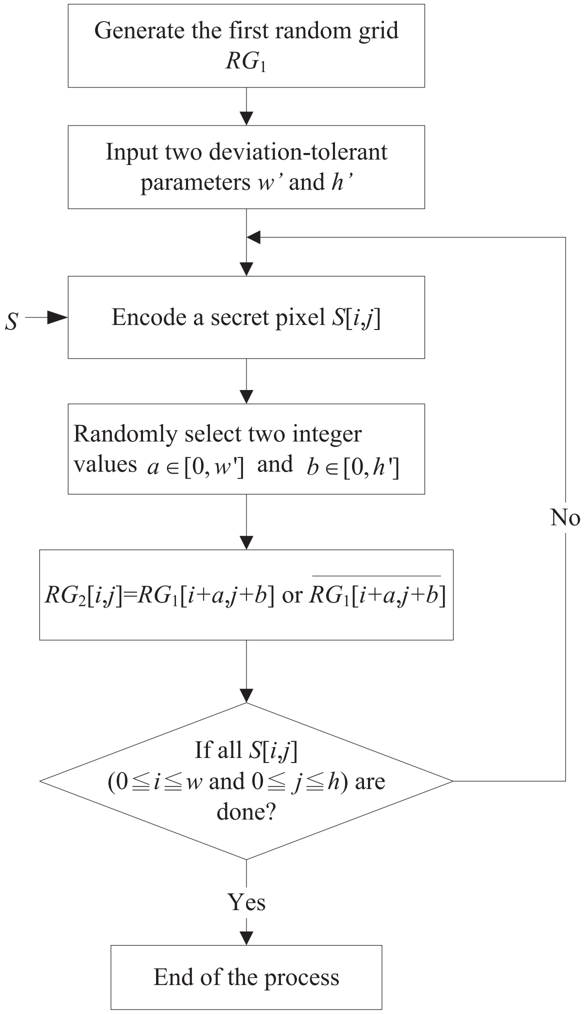
Generate the first random grid $RG_1$
Input two deviation-tolerant parameters $w'$ and $h'$
$S$
Encode a secret pixel $S[i,j]$
Randomly select two integer values $a \in [0, w']$ and $b \in [0, h']$
$RG_2[i,j]=RG_1[i+a,j+b]$ or $\overline{RG_1[i+a,j+b]}$
If all $S[i,j]$ ($0 \leqq i \leqq w$ and $0 \leqq j \leqq h$) are done?
No
Yes
End of the process

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

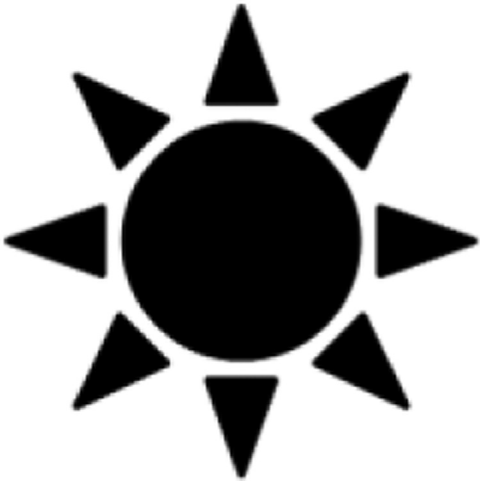

**Fig. 2.** Secret image with the size of 1024 × 1024.

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.

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 $S=\{S[i,j]|S[i,j]=0$ or $1, 1\leqq i\leqq w, 1\leqq j\leqq h\}$ 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 $RG_k=\{RG_k[i,j]|\ RG_k[i,j]=0$ or $1, 1\leqq i\leqq w, 1\leqq j\leqq h\}$ $(k=1,2)$ 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 $S=\{S[i,j]|S[i,j]=0$ or $1, 1\leqq i\leqq w, 1\leqq j\leqq h\}$ and
  two deviation-tolerant factors $w'$ and $h'$
Output: two meaningless random-grids $RG_k=\{RG_k[i,j]|\ RG_k[i,j]=0$ or $1, 1\leqq i\leqq w, 1\leqq j\leqq h\}$ $(k=1,2)$
$RG_1[i,j] \leftarrow$ 0 or 1 for all $i$ and $j$                 //Step 1
For $i=1$ to $w$, $j=1$ to $h$                                      //Step 3
Generate two random integers $a$ and $b$, where                   //Step 3.1
  $a \in [0, w'$ and $b \in [0, h']$.
If ($S[i, j]=0$)                                                   //Step 3.2
$RG_2[i,j] \leftarrow RG_1[i + a, j + b]$                           //Step 3.2.1
else
$RG_2[i,j] \leftarrow \overline{RG_1[i + a, j + b]}$                //Step 3.2.2
```

Download English Version:

https://daneshyari.com/en/article/537320

Download Persian Version:

https://daneshyari.com/article/537320

Daneshyari.com