J. Vis. Commun. Image R. 23 (2012) 677–684

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

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

Optimal (2,n) and (2,infinity) visual secret sharing by generalized random grids

Shang-Kuan Chen [a,*], Sian-Jheng Lin [b]

[a] Department of Computer Science and Information Engineering, Yuanpei University, Hsinchu, Taiwan
[b] Research Center for Information Technology Innovation, Academia Sinica, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 22 October 2010
Accepted 9 March 2012
Available online 21 March 2012

Keywords:
Contrast
Random grids
Visual cryptography
Visual secret sharing
Generalized random grids
Image sharing
Secret image sharing
Optimal contrast

ABSTRACT

Based on generalized random grids, this paper proposes two visual cryptography methods denoted as $(2,n)$ GRG and (2,infinity) GRG. The $(2,n)$ GRG is suitable for the pre-decided number of shares, and the (2,infinity) method is suitable for the adjustable number of shares. The proposed $(2,n)$ GRG achieves better contrast on the stacking result, and the proposed (2,infinity) GRG enables extending the number of shares anytime. Based on the definition of contrast in Shyu's work in 2007, we also demonstrate that the stacking result of $(2,n)$ GRG is close to the theoretical bound of the contrast, and the stacking result of (2,infinity) GRG achieves the theoretical bound of the contrast.

1. Introduction

Kafri and Keren [1] introduced a method for encrypting an image into two noise-like random grids in 1987. The size of each random grid is the same as that of the secret image. Without any computation, when we superimpose the two random grids, the input image can be revealed. Their method is called 2-out-of-2 visual secret sharing (VSS), denoted as (2,2) VSS, by random grids. In 2007, Shyu [2] adopted the encoding algorithm of Kafri and Keren [1] to accomplish encryption of gray and color images. Later in 2009, Shyu [3] generalized Ref. [2] to an (n,n) VSS method by random grids. In 2009, Chen and Tsao [4] proposed (n,n) and $(2,n)$ VSS methods by random grids. Their $(2,n)$ visual secret sharing method by random grids is a fault-tolerant version. Chen [5] generalized the idea of random grids to have each grid be either opaque or transparent in non-necessary equal probability. The method also generates meaningful shares. In this paper, we propose the $(2,n)$ visual secret sharing method by generalized random grids. With n as a pre-defined constant, the first subsystem achieves better stacking result than the second subsystem. Otherwise, the second subsystem that is suitable for n can be extended anytime. Finally, some theoretic demonstrations are shown for the two subsystems.

Another visual secret sharing system is called visual cryptography (VC) that was first proposed by Naor and Shamir [6] in 1995. VC is also a method for protecting image-based secrets. The secret image is shared into n noise-like transparencies, also called shares. Without computation, only stacking at least r $(r \leqslant n)$ shares together, the content of the secret image can be revealed. Therefore VC is fault-tolerant while protecting image-based secrets. However, different from the above methods using random grids, some related VC methods [7–12] use basis matrices for encoding shares, and the size of the generated shares are much larger than that of the secret image. When n or r increases, the pixel expansion becomes larger and larger. Thus, it may be impracticable for real application.

Without pixel expansion, Ito et al. [13] introduces the basic model of probabilistic visual cryptography scheme (PVCS). The PVCS is based on the basis matrices introduced by Naor and Shamir [6], but each secret pixel is coded by the randomly chosen column in the basis matrices. The PVCS generates transparencies with invariant size. The optimal contrast of (2,n) and (n,n) PVCS are constructed by Yang [14], and a generalized VCS with flexible size expansion is introduced by Cimato et al. [15].

In Section 2 of the paper, we introduce the related works. The proposed method is stated in Section 3. The experimental results are shown in Section 4. In Section 5, we present the discussion. Finally, the conclusions are made in Section 6.

2. Related works

The details of the VC method proposed by Naor and Shamir [6] and Shyu's random grids method [2] are demonstrated as follows.

Table 1 shows an example of (2,3) VC proposed by Naor and Shamir [6]. A binary pixel b is encoded into three pixel shares h_1, h_2, and h_3, respectively. $\otimes$ is defined as stacking operator, and the

* Corresponding author.
E-mail addresses: skchen@mail.ypu.edu.tw (S.-K. Chen), sjlin@citi.sinica.edu.tw (S.-J. Lin).

1047-3203/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jvcir.2012.03.004

Table 1
The encoding and decoding table of (2,3) VC by Naor and Shamir's method [6].

b	h_1	h_2	h_3	$h_1 \otimes h_2$	$h_1 \otimes h_3$	$h_2 \otimes h_3$	$h_1 \otimes h_2 \otimes h_3$	Probability
□	■□□	■□□	■□□	■□□	■□□	■□□	■□□	1/3
	□■□	□■□	□■□	□■□	□■□	□■□	□■□	1/3
	□□■	□□■	□□■	□□■	□□■	□□■	□□■	1/3
■	■□□	□■□	□□■	■■□	■□■	□■■	■■■	1/6
	■□□	□□■	□■□	■□■	■■□	□■■	■■■	1/6
	□■□	■□□	□□■	■■□	□■■	■□■	■■■	1/6
	□■□	□□■	■□□	□■■	■■□	■□■	■■■	1/6
	□□■	■□□	□■□	■□■	□■■	■■□	■■■	1/6
	□□■	□■□	■□□	□■■	■□■	■■□	■■■	1/6

basic operations are □ ⊗ □ = □, □ ⊗ ■ = ■, ■ ⊗ □ = ■, and ■ ⊗ ■ = ■. Each generated pixel refers to each row of the basis matrices defined as

$$M_{\text{white}} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad M_{\text{black}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where 1 represents the black pixel ■ and 0 represents the white pixel □. Hence, the size of each share is 3-fold the size of the secret image. Table 1 shows the results of permuting columns of M_{white} and M_{black} for the share's security. The white secret pixel refers to three encoding rules with each probability 1/3, and the black secret pixel refers to six encoding rules with each probability 1/6. However, for any three random pixels in a share, the probability that the corresponding pixel of the secret image is black or white is the same. Therefore, we cannot obtain any information about the secret image from a single share. Stacking any two shares together, the result of two whites and one black is corresponding to that of the white pixel of the secret image, and the result of one white and two blacks is corresponding to that of the black pixel of the secret image. The difference of the ratio of blacks in every three pixels, called contrast, enables us to see the content of the secret image. Using the (2,3) VC as an example, the contrast is 1/3 when two shares are stacked together, and the contrast is 2/3 when three shares are stacked together. Besides, any one of the shares damaged or lost is tolerant.

A random grid was defined as a two-dimensional array of binary pixels determined in a totally random way, 50% to 50%. Shyu proposed [2] a method for non-expansible visual secret sharing (VSS) system using two random grids. The method does not need encoding matrix for generating the shares. The basic Input and Output definitions and the three kernel algorithms are stated as follows.

Input: A binary image B
Output: Two shares H_1 and H_2 for revealing the content of B
[Algorithm K_1]
1. Generate H_1 that is full of random 0(white)/1(black) pixels.
2. For each entry $b \in B$, if $b = 0$, then $h_2 = h_1$, otherwise $h_2 = 1 - h_1$, where $h_1 \in H_1$, $h_2 \in H_2$.
[Algorithm K_2]
1. Generate H_1 that is full of random 0/1 pixels.
2. For each entry $b \in B$, if $b = 0$, then $h_2 = h_1$, otherwise h_2 = random 0/1 pixel.
[Algorithm K_3]
1. Generate H_1 that is full of random 0/1 pixels.
2. For each entry $b \in B$, if $b = 0$, then h_2 = random 0/1 pixel, otherwise $h_2 = 1 - h_1$.

3. The proposed method

The proposed visual secret sharing consists of two subsystems: (1) the system with fixed number of shares, also called $(2,n)$ generalized random grids (*GRG*) system; (2) the system with addible number of shares, also called (2,infinity) *GRG* system. Before describing the two subsystems, the definitions of stacking operation, the two important characteristics of VSS and random bit function are stated as follows.

Given a binary secret image B, for each $b \in B$, where $b = 0$ represents a white pixel and $b = 1$ represents a black pixel. The n shares $\{H_k | h_k \in \{0,1\},\ k = 0,\ 1,\ \ldots,\ n-1\}$ are generated, where $h_k = 0$ represents a transparent pixel and $h_k = 1$ represents an opaque pixel.

Definition 1. Given a binary secret image B of each pixel $b \in \{0,1\}$, the corresponding pixel h_k, where $k = 0,\ 1,\ \ldots,\ n-1$ must satisfy the following two conditions for meeting the definition of VC proposed by Naor and Shamir [6]:

(1) (Security condition). $P(h_k = 0|b = 0) = P(h_k = 0|b = 1)$, where $P(e_1|e_2)$ means the probability that event e_1 occurs given that event e_2 occurs.
(1) (Contrast condition). Refer to the definition of Shyu [2], stacking the corresponding pixel h_k and h_l, the contrast $\alpha (\alpha > 0)$ of the stacking result $s_{kl} = h_k \oplus h_l$ is defined as

$$\alpha = \frac{P(s_{kl} = 0|b = 0) - P(s_{kl} = 0|b = 1)}{1 + P(s_{kl} = 0|b = 1)}.$$

Definition 2. A random bit generator $g(x)$ is defined as a random bit of the value 0 or 1 by $g(x) = 0$ with probability x and $g(x) = 1$ with probability $1 - x$.

3.1. Image encryption by (2,n) generalized random grids

A binary image B is shared to obtain n shares $\{H_0, H_1, \ldots, H_{n-1}\}$, where $h_k \in \{0(\text{white}), 1(\text{black})\}$. Algorithm 1 shows the proposed $(2,n)$ GRG, where $B[i,j]$ and $H_k[i,j]$ represent the secret pixel b and the share pixel h_k at the position $[i,j]$, respectively. The constant c calculated in step 1 will be discussed in Theorem 3.

Algorithm 1: $(2,n)$ GRG

Input: an $h \times w$ binary secret image B, and a number n
Output: n shares $\{H_0, H_1, \ldots, H_{n-1}\}$.
Steps:
1. Calculate the constant $c = \arg\max_{c'} \left\{ \frac{c'/n - (c'/n)^2}{1 + (c'/n)^2 - 1/n(1 + c'/n)} \right|$, $c' \in \left\{ \left\lfloor n(\sqrt{2} - 1) \right\rfloor, \left\lceil n(\sqrt{2} - 1) \right\rceil \right\}. \}$.
2. Create an $h \times w$ matrix T of all entries are c.
3. **for** $i = 1$ **to** h, $j = 1$ **to** w
4. $H_0[i,j] \leftarrow g(c/n)$
5. **if** $B[i,j] = 1$ **and** $H_0[i,j] = 0$
6. $T[i,j] \leftarrow T[i,j] - 1$
7. **end if**
8. **end for**
9. **for** $k = 1$ **to** $n - 1$
10. **for** $i = 1$ **to** h, $j = 1$ **to** w