Available online at www.sciencedirect.com

ScienceDirect

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

Visual multi secret sharing by cylindrical random grid

Saman Salehi[*], *M.A. Balafar*

Dept. of Computer, Faculty of Engineering, University of Tabriz, Tabriz, East Azerbaijan, Iran

ARTICLE INFO

Article history:
Available online 14 July 2014

Keywords:
Visual cryptography
Secret sharing
Data hiding

ABSTRACT

Visual secret sharing (VSS) is the process of encoding a secret image into several share images in which the original secret image can be reconstructed and recognized by stacking all of the share images together. VSS has two categories: visual cryptography (VC) and Random Grid (RG). The VC is affected by various drawbacks such as: enlarging the size of original image, need for a codebook and the limitation to encode only one secret image at a time. RG solves the first two drawbacks of VC. To solve the third drawback and provide a solution to optimize recent algorithms, we propose a novel RG-based VSS scheme which encodes several secret images at a time. Instead of using only (2, 2) visual secret sharing, (2, *n*) and (*n*, *n*) is employed. This scheme has the ability to encode one or multiple secret images into multiple shares in place of two shares. In our proposed scheme, instead of Circular Random Grid, a new algorithm named Cylindrical Random Grid is used. It encrypts multiple secret images into two or more shares. To decrypt the first secret image, shares are stacked together. For decrypting of other secret images, one of the stacked shares is rotated in a fixed size over other shares based on the number of secret images which are encrypted. This algorithm is simple to implement and less time consuming.

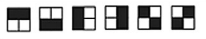
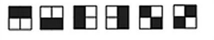
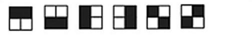
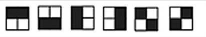
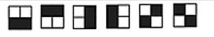
1. Introduction

Visual secret sharing (VSS), so-called visual cryptography, aims to provide a perfect-security cryptosystem in which the decryption operation employs the human visual system (HVS) with no computational cost. VC first was introduced by Naor and Shamir (1995a) in which a secret image such as text, note and binary picture was encrypted into two shares in a secure way that could not be detected by HVS. These shares are printed on transparency such that all pixels that have information about secret image in two shares are inter-correlated. When two shares superimposed together the secret image is revealed. Naor and Shamir used codebook table to create share images (S_1) that is a noise like images. The codebook is a binary matrix of '0' or '1' ('0' for transparent and '1' for opaque). In codebook, every pixel of secret image is presented by a block that two of them are white and the other two are black (Table 1 white for "transparent", black for "opaque"). The VC algorithm has three steps. In the first step, to create S_1 (first share), $w \times h$ (w is width and h is high of secret image) blocks of codebook is selected randomly. The S_1 has equal number of white and black pixel. In second step, to create S_2 (second share), *SI* (secret image) is converted to a one dimensional binary secret image. Then, for every pixel of *SI* if $SI(i, j)$ was transparent therefore, corresponding block of $S_2(i, j)$ is set to $S_1(i, j)$ otherwise $S_2(i, j)$ is set to $\overline{S_2(i, j)}$. Finally, S_1 and S_2 are stacked together for decrypting original secret image.

[*] *Corresponding author.*
E-mail addresses: s.salehi90@ms.tabrizu.ac.ir (S. Salehi), Balafarila@tabrizu.ac.ir (M.A. Balafar).

http://dx.doi.org/10.1016/j.jisa.2014.05.003

Table 1 – The Codebook with 2 × 2 block (White for “transparent”, Black for “opaque”).

if SeIm(i,j)=	share *A*	share *B*	Stacking
white □			
black■			■ ■ ■ ■ ■ ■

Note that in RGVSS algorithm opaque pixel denoted by “1” and a transparent pixel by “0”. An example of running this algorithm is shown in Fig. 1.

One of the most critical concerns to design an effective visual secret sharing scheme is how to construct set of basis matrixes, which either achieves a smaller pixel expansion under some specific situation or improve the contrast in the reconstructed result. VC-based VSS scheme suffers from drawbacks such as: the pixel expansion, need for a codebook and limitation to encode only one secret image at a time. Several researchers attempted to overcome these drawbacks, for instance to overcome the single secret image encoding limitation at a time, Shyu et al. (2007) proposed a method to encrypt a set of $m \geq 2$ secrets into two circular shares so that m secrets can be recovered one by one, by stacking one share and rotating another share with m different rotation angles. The drawback of their scheme was the expansion of pixel ratio with 2 × m (Chen et al., 2005). To store two secret images with size 20 × 20, the share images size expanded to 4 × 20 × 20. In order to overcome pixel expansion and need for codebook problems (conventional VC), Kafri and Keren (1987a) proposed the VSS method known as RG (Random Grids) (Chen and Tsao, 2008; Shyu, 2007, 2009). In Kafri and Keren's method, binary image is encrypted into two cypher-grids with same size of the original image. Deciphering secret image is simple and is as same as VC deciphering process. But, these methods have still the problem of encoding only one secret image at a time.

To overcome these problems, Chen (Chen et al., 2008) proposed a method that encrypts multiple secret images into two rectangular grids which have the same size as the original image and needs no codebook, but this method can encrypt only up to four images by rotating RG in 0°, 90°, 180°, 270° degrees.

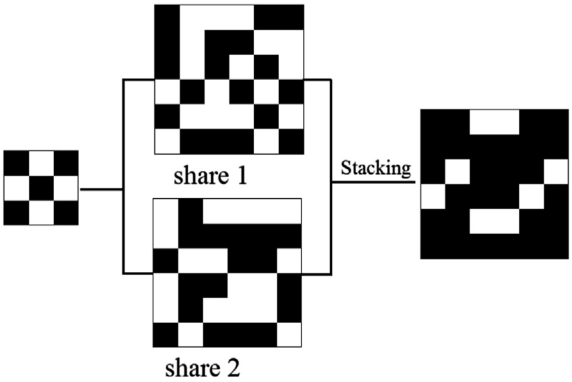


Fig. 1 – Three step for constructing VC (visual Cryptography): first step, S_1 (share 1) is created by randomly choosing block in Codebook Table, second step, S_2 (share 2) is created from S_1, third step, stack two S_1 and S_2 to reveal secret image.

With all these problems that VC based VSS has, an increasing number of researchers have applied VC to VC-related work, such as image encryption (Lukac and Plataniotis, 2005), image hiding (Chang et al., 2005; Fang and Lin, 2006) and visual identification (Naor and Pinkas, 1997), therefore VC-based VSS has played an important role in multimedia security.

In this paper a novel RG-based VSS scheme is proposed that encodes several secret images at a time and has the ability to encipher the secret image into several shares instead of two shares. In proposed method, cylindrical share is substitute with circular share. The cylindrical share has no pixel expansion and the process of creating shares and revealing secret image is less time complexities. In circular mode every share should be converted to circular shares. It means one pixel of the secret image must be converted to one sector-pixel of the circular cipher-grid. So, it causes time complexity and pixel expansion. Several researchers (Naor and Shamir, 1995b; Koga, 2001; Naor and Shamir, 1996) try to use visual secret sharing in multi shares. But their schemes can be used only for single secret sharing. The recent visual secret sharing which introduced as yet for (2, n) and (k, n) is only based on single secret image (Chen and Tsao, 2011). This means that only one secret image can be shared among the participants. Other researchers such as (Chen and Li, 2011) try to share multiple secret images in two shares. In this paper we introduce visual multi secret sharing based on (2, n) and (n, n). The scheme can be used in validating the authority of group of users to access a critical resource on which all users need in order to decrypt the secret code of this resource. The secret code is shared among each user and for decrypting secret code, the shares are superimposed together. The decoding process of this scheme is done by human visual system.

When two shares are stacked together, secret image is revealed from the random background duo to the light transmission. So, there is no need for any computation and no individual user can reveal information about secret image. We call the proposed method; Cylindrical Random Grid that has a simple implementation, a small time complexity and better results compared to the previous state of the art methods. Furthermore, it doesn't have the drawbacks of VC scheme.

The rest of the paper is organized as follows: in Section 2 we review the main techniques of conventional VSS by random grids briefly. In Section 3 the proposed scheme will be describe. Section 4 is discussion about VSS. Section 5 is about analysis. In Section 6 the experimental results are demonstrated and finally Section 7 presents the conclusion of this article.