The Journal of Systems and Software 86 (2013) 1267–1274

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

# Quality-adaptive visual secret sharing by random grids

Tzung-Her Chen[a,*], Yao-Sheng Lee[a], Wei-Lun Huang[a], Justie Su-Tzu Juan[b], Ying-Yu Chen[b], Ming-Jheng Li[b]

[a] *Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan, ROC*
[b] *Department of Computer Science and Information Engineering, National Chi Nan University, Puli, Nantou 54561, Taiwan, ROC*

ARTICLE INFO

*Article history:*
Received 2 January 2012
Received in revised form 6 December 2012
Accepted 7 December 2012
Available online 17 December 2012

*Keywords:*
Visual cryptography
Random grid
Visual secret sharing
Quality adaptive

ABSTRACT

Visual secret sharing (VSS), classified into visual-cryptography (VC)-based and random-grid (RG)-based, suffers from the contrast problem that the reconstructed secret with low visual quality is not easy to recognize. Even worse, the more share images stacked, the lower visual quality of reconstructed secrets revealed. Therefore, it is promising to remove this innate drawback. In this paper, with security still kept, the light transmission of share images generated by the proposed scheme is redesigned to be higher than before such that the better visual quality of reconstructed secrets is obtained. To demonstrate the feasibility, the experimental results show the reconstructed secrets are visually recognizable and the goal that the more share images stacked, the better quality of reconstructed secrets we have is achieved.

## 1. Introduction

Visual secret sharing (VSS) [1,2] is a technique to share a secret, in which a secret image is turned into several meaningless share images and reconstructed by superimposing the share images. Compared with traditional encryption such as DES and AES, VSS offers unbreakable encryption if a meaningless share contains truly random pixels such that it can be seen as a one-time pad system. Furthermore, VSS provides the decryption operations without the needs of cryptographic knowledge and computational devices. Hence, VSS is suitable for the applications of high-security needed and without computational devices given.

Visual cryptography (VC), a well-known VSS technique, is proposed by Naor and Shamir [3] in 1995. Naor and Shamir proposed the concept of $t$-out-of-$n$ threshold secret image sharing scheme which encodes a secret into $n$ share images by a codebook and recovers the secret by recognizing the stacked result of at least $t$ share images ($2 \leqq t \leqq n$).

Generating a tailor-made VC codebook for some application is usually considerably difficult [4,5]. Moreover, it makes pixel expansion worse and, thus, causes more data transmission burden.

Recently, another VSS approach by adopting random-grid algorithm (RG-based VSS), first proposed by Kafri and Keren [6] in 1987, gained attention in academia again. Inspired by Kafri and Keren, Shyu [7] presented the new RG-based VSS schemes to encode gray-level and color images in 2007. Since then, a growing number of RG-based VSS schemes are presented in the literature [8–12].

In 2009, a multiple RG-based VSS scheme was proposed by Shyu [12] to deal with the situation that more than two share images are required to generate. Almost simultaneously, Chen and Tsao [10] also proposed $(2,n)$ and $(n,n)$ algorithms to remove the limitation of (2,2)-RG-based VSS [6,7].

However, the aforementioned VC-based or RG-based VSS schemes can reveal the original secrets, but cannot achieve the goal of progressive image sharing. In 2005, Jin et al. [13] proposed the first progressive VC-based VSS schemes, in which the secret image can be revealed with multilevel quality. That is, someone who holds more share images can recover the secret image with better visual quality. Unfortunately, the method needs extra computation, which violates the essential assumption of VSS.

Later, several researchers have paid attention to the progressive image sharing property for achieving flexible decoding. Fang and Lin [14] proposed another VC-based progressive VSS scheme with the disadvantage of pixel expansion. Here, pixel expansion means that a certain pixel in secret images will be turned into more than one sub-pixels in share images, so that the extra load of storage and transmission bandwidth is needed. In 2009, Chen and Lee [8] proposed a progressive RG-based VSS scheme to overcome the drawbacks of share image size expansion and codebook design.

However, all above-mentioned schemes still suffer the problem that the visual quality of the reconstructed secret images is low and, moreover, it becomes worse if more share images are stacked. This is because that the light transmission of each share image in previous VC-based VSS [3–5] or RG-based VSS [6,7,10,12] is equal or greater than 1/2. That is, the white pixels in the secret image

[*] Corresponding author. Tel.: +886 5 2717723; fax: +886 5 2717741.
*E-mail address:* thchen@mail.ncyu.edu.tw (T.-H. Chen).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.12.022

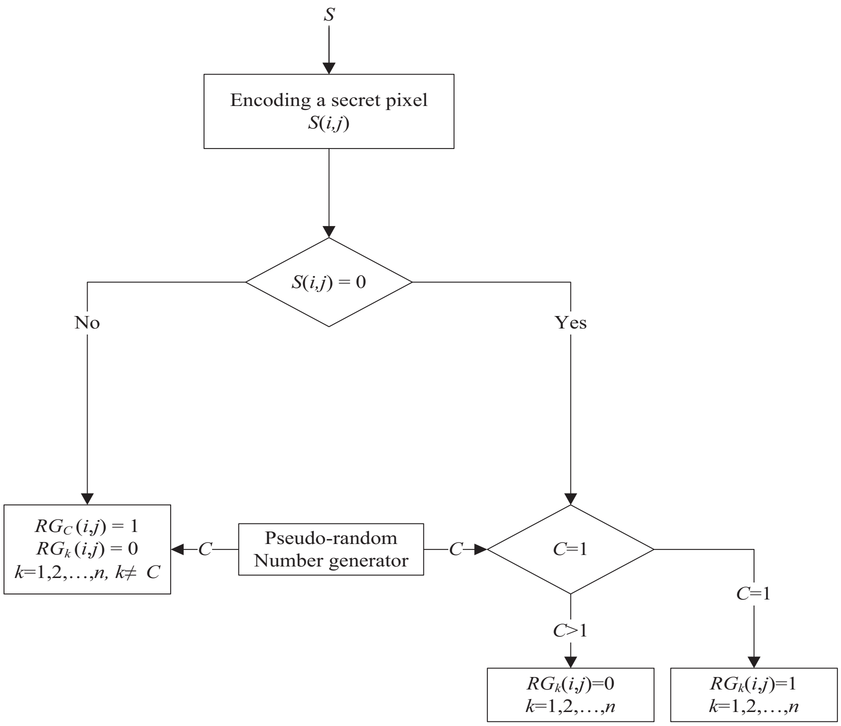

**Fig. 1.** The processes of encoding a secret pixel.

have the probability of 1/2 to misinterpret into black pixels in the reconstructed image.

To obtain the better visual quality of reconstructed images, the area of the stacked image corresponding to the white pixels in the secret image must be designed to include fewer black random-pixels than white, and the area of the stacked image corresponding to black pixels in the secret image must be totally black after stacking.

Inspired by Chen and Tsao's $(2,n)$ RG-based VSS [10], we propose the quality-adaptive RG-based VSS scheme which alters the light transmission of each random grid for improving the visual quality of reconstructed images upon keeping the security. In the past decade, many VSS techniques for halftone images, gray-level images, and color images [7,10,12,13,15–17] have been developed. To meet this trend, the experimental results demonstrate the feasibility of the proposed scheme by means of encoding not only binary secret images but also gray-level and color secret images.

The rest of this paper is organized as follows. The present scheme is described in Section 2. Sections 3 and 4 demonstrate the performance and the experimental results, respectively. Further discussions and conclusions are given in Sections 5 and 6.

## 2. Proposed scheme

A binary secret image $S$ with the size of $w \times h$ are determined as inputs. The proposed scheme outputs $n$ random-grids $RG_k$ ($k = 1, 2, \ldots, n$) with the same size of secret.

Firstly, a secret image is encoded into $n$ meaningless random-grids. On the decoding phase, staking any two of the random grids can reveal the secret image again. In addition, stacking more random grids can obtain the better quality. In the proposed scheme, the parameter $n$ is designed to control both the light transmission of random-grids and the quality of reconstructed images. The larger value of $n$, the higher light transmission of each random-grid and the better contrast of the reconstructed image when stacking $n$ random-grids.

The pixel values "0" and "1" are used to represent the transparent and the opaque pixels, respectively. The processes of encoding a secret pixel are demonstrated in Fig. 1. In the proposed scheme, the random integer $C$, computed by a pseudo-random number generator, is designed to control the light transmission of each random-grid. Precisely, $C$ determines which random-grid, i.e., one of $n$, is assigned a black random-pixel. For example, if a secret black pixel $S(i,j)$ is chosen as an input, the generated black random-pixel is assigned to $RG_C(i,j)$and the $n - 1$ white ones are distributed to the other $(n - 1)$ $RG_k(i,j)$ where $k = 1, 2, \ldots, n$ and $k \neq C$. Otherwise, the generated $n$ black or $n$ white random-pixels are distributed to $n$ random-grids with the probability of $1/n$ or $n - 1/n$, respectively.

The encoding process encompasses the following two main steps. Assume the secret pixel $S(i,j)$ is chosen first.

Step 1: generate an integer number

To encode one secret pixel, a random number $C$, where $1 \leq C \leq n$, is generated by a pseudo-random number generator.

Step 2: encode a secret pixel $S(i,j)$

By the generated value $C$ and the secret pixel $S(i,j)$, the random-pixels of each random grid $RG_k$ ($k = 1, 2, \ldots, n$) can obtained as follows:

$$RG_k(i,j) = \begin{cases} 1, & S(i,j) = 0 \text{ and } C = 1 \\ 1, & S(i,j) = 1 \text{ and } C = k \\ 0, & \text{otherwise} \end{cases}$$

where $k = 1, 2, \ldots, n$.

Step 3: Repeat Steps 1 and 2 until all random-pixels $RG_k(i,j)$ are obtained.

On the decoding phase, the secret information can be recognized by the human visual system when directly stacking two or more random-grids. The more random-grids stacked, the clearer of the original secret revealed.