Information Sciences 288 (2014) 330–346

Contents lists available at ScienceDirect

Information Sciences

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

Distortionless visual multi-secret sharing based on random grid

Kai-Siang Lin [a], Chih-Hung Lin [b], Tzung-Her Chen [a,*]

[a] Department of Computer Science and Information Engineering, National Chiayi University, No.300 University Rd., Chia-Yi City 60004, Taiwan
[b] Graduate Institute of Mathematics and Science Education, National Chiayi University, No.85 Wenlong Vil., Minxiong Township, Chiayi County 62103, Taiwan

ARTICLE INFO

Article history:
Received 27 February 2013
Received in revised form 26 May 2014
Accepted 18 July 2014
Available online 5 August 2014

Keywords:
Visual secret sharing
Visual multi-secret sharing
Visual cryptography
Random grid
Secret distortion

ABSTRACT

Because visual secret sharing (VSS) has already been well defined, visual multi-secret sharing (VMSS) is more practical for various fields. In a VMSS scheme, N secret messages are encoded into two shares that appear to be noise and these are later stacked by rotating, flipping and turning to visually recognize the secrets. VMSS is generally classified as visual cryptography (VC) based VMSS or random grid (RG) based VMSS. However, VC-based VMSS has the three main drawbacks of pixel expansion, the cost of designing a complex codebook, and shape distortion in the decoded secret image. In order to stack shares at any angle during decoding, secrets are encoded into doughnut-shaped shares. However, the traditional doughnut share methods distort the secret after decoding, because the shape of each share is doughnut. This paper proposes a new RG-based VMSS scheme that defines the shape of each share as a pie-shaped share that does not distort secrets, so that multiple secrets are encoded into two pie shares and then decoded by stacking one pie share on another at different angles of rotation. Experimental results demonstrate the efficiency of the proposed method.

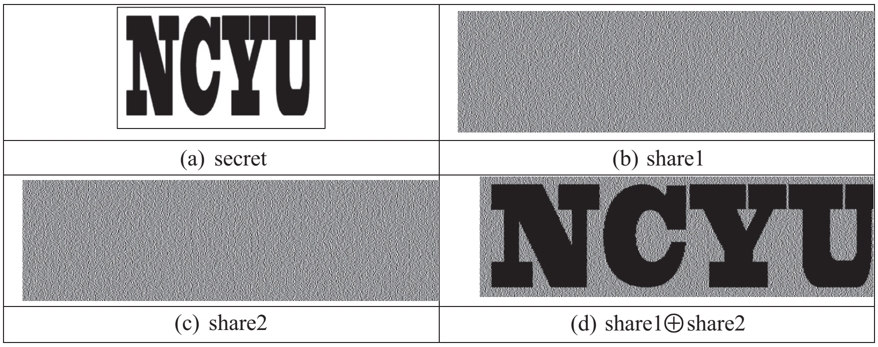
1. Introduction

In 1987 Kafri and Keren [13] proposed visual secret sharing (VSS) using random grids (RG) and in 1996 Naor and Shamir [16] proposed VSS using visual cryptography (VC). A comparison of RG-based VSS with VC-based VSS shows that the former avoids three main disadvantages of VC: pixel expansion, complex codebook design and shape distortion when decoding the secret image. As shown in Fig. 1 for VC-based VSS and Fig. 2 for RG-based VSS, the VSS encodes a secret message into two shares, which are both noise-like and unrecognizable. By stacking these two shares, the secret message is disclosed visually. Using VSS, secret image can be encoded and shared with participants, and the participants can decode the secret image by collecting the shares from other participants and stacking those shares to recover the secret image. Therefore, the participants only collect and stack the shares, so the secret is recognized visually with no complex calculations, computer assistance, or related background knowledge.

Many VSS applications have been proposed. Wu et al. [23] proposed a VC-based scheme for color images and Shyu [17] proposed a RG-based scheme for gray-level and color images. To expand usage of VSS, improving the visual quality is important, so VC-based schemes [10,11,14,24,25] and RG-based schemes [2,15,22] have been proposed. Extended from the simple VSS so that more shares could be generated, a study of visual secret sharing was undertaken by Shyu [18] and Chen and Tsao [4,6,7], both of whom used RG. In order to make the shares more meaningful during recognition, Fang [12] and Chen and Tsao [8] proposed a friendly-VSS, respectively based on VC and on RG. However, these studies only shared one secret in each VSS.

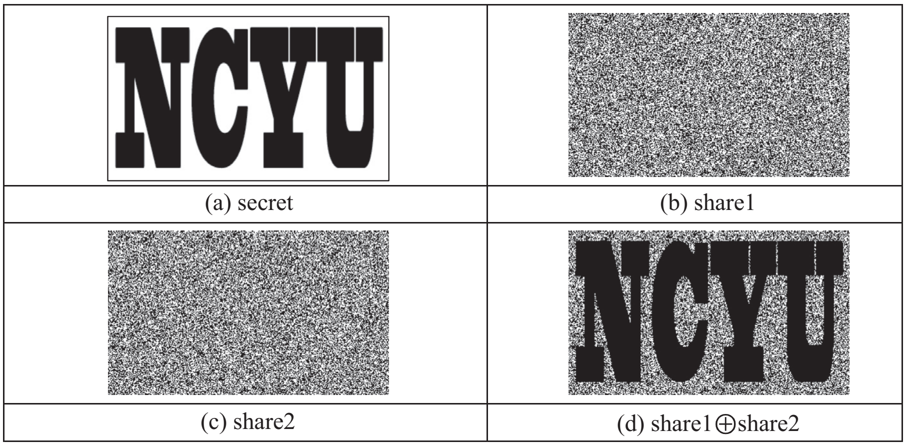
* Corresponding author. Tel.: +886 5 271 7723.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

http://dx.doi.org/10.1016/j.ins.2014.07.016



(a) secret (b) share1 (c) share2 (d) share1⊕share2

Fig. 1. VC-based VSS.



(a) secret (b) share1 (c) share2 (d) share1⊕share2

Fig. 2. RG-based VSS.

With the extensive development of networks, increased transmission performance is important. In order to rapidly promote communication, the sharing of multiple secrets on VSS is a novel and useful application. Consequently, visual multi-secret sharing (VMSS) technology has become more popular. In 1998, Wu and Chen [21] and Chen et al. [5] proposed VC-based VMSS and RG-based VMSS that could encode two secret messages into two shares and decode the secret by stacking the two shares immediately, to disclose the first secret, then rotating one shared image through 90° to disclose the other. In 2005, Wu and Chang [20] and Chen et al. [1] utilized the concept of a circle to encode two secrets, allowing an arbitrary rotation angle from 0° to 360° to disclose the secrets. In 2012, Chen et al. [9] proposed RG-based VMSS to increase the number of secrets to four, using limited rotation angles of 0°, 90°, 180° and 270°.

In 2007 and 2012, Shyu et al. [19] and Chen and Li [3] proposed VC-based VMSS and RG-based VMSS that encodes a set of N secrets ($N \geqslant 2$) into two doughnut shares. The N secrets are then decoded by stacking these two doughnut shares at N different rotation angles. Figs. 3 and 4 show the results of Chen and Li's RG-based VMSS scheme. Although making the share doughnut-shaped allows the sharing of more secrets, it still has two disadvantages. The first disadvantage is shown in Fig. 3, where it can clearly be seen that the disclosed secrets exhibit significant distortion, which is caused by the conversion into doughnut shares during encoding. The second disadvantage is caused by the hole of the doughnut share, so the type of secret is restricted. In Fig. 4, where the secret image is a message, the original secret is unrecognizable after decoding. Therefore, secret sharing is confined to text messages.

In VMSS studies, some schemes [5,9] have been shown to be more suitable than others [1,3,19,20], where shape distortion is caused by a VC basis or the shape of the doughnut. In schemes [3,19], although the doughnut shape results in distortion of the secret messages or images, VMSS can still be extended to share more secrets. In this paper, the proposed VMSS method shares any number of secret images. The traditional scheme is abandoned and the secret shape is firstly defined as a circle. With this restriction, the problem of secret distortion that is caused by a doughnut share is addressed. By using RG for VMSS, the proposed method avoids pixel expansion and complex codebook design. All of the VMSS schemes previously mentioned encode secret images into two shares. By extending the proposed method, a threshold VMSS scheme is proposed and the result of further extension is seen in the experimental results.

The remainder of this paper is organized as follows. The proposed method and a performance analysis are described in Section 2 and in Section 3, respectively. The experimental results and a discussion are provided in Section 4. Finally, Section 5 gives conclusions.