Information Sciences 301 (2015) 61–74

Contents lists available at ScienceDirect

Information Sciences

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

Prevention of cheating in visual cryptography by using coherent patterns

Pei-Yu Lin [a], Ran-Zan Wang [a,b,*], Yu-Jie Chang [c], Wen-Pinn Fang [d]

[a] Department of Information Communication, Innovation Center for Big Data and Digital Convergence, Yuan Ze University, Taiwan
[b] Department of Computer Science & Engineering, Yuan Ze University, 135 Far-East Rd., Chung-Li, Taoyuan 320, Taiwan
[c] Department of Computer Simulation & Design, Shih Chien University, Taiwan
[d] Department of Computer Science & Engineering, Yuan Pei University, Taiwan

ARTICLE INFO

Article history:
Received 18 June 2014
Received in revised form 19 December 2014
Accepted 29 December 2014
Available online 5 January 2015

Keywords:
Visual cryptography
Visual secret sharing
Secret sharing
Image sharing
Cheating prevention visual cryptography

ABSTRACT

This paper proposes a simple method for establishing a visual cryptographic (VC) scheme with the ability to prevent cheating. Given the n base-shares generated in a conventional (t,n), $2 \leqslant t \leqslant n$, VC scheme, an authentication pattern stamping process was designed to encode the n base-shares to get n verifiable shares that exhibit the following properties: (1) knowledge of less than t verifiable-shares gets no secret information, (2) the secret can be revealed by completely superimposing t or more verifiable-shares, and (3) the authentication pattern can be revealed by partially superimposing any pair of verifiable-shares. Theoretical proof and computer simulation for the proposed method are provided. The proposed method has smaller pixel expansion than previous cheating prevention VC schemes, and the verification process is fulfilled without resorting to any additional dedicated verification share. It can be attached easily to any reported VC scheme to endow legitimate users with the capability of detecting faked shares provided by malicious participants.

1. Introduction

Visual cryptography (VC) is an image-based secret sharing scheme that was first introduced by Noar and Shamir [8] in 1995. In a conventional (t,n)-threshold VC scheme [1,8,14], the input image is encoded in n transparent shares in such a way that any subset of t $(2 \leqslant t \leqslant n)$ or more shares can disclose the secret message, but no information about the secret can be revealed from any $t-1$ or fewer shares. The decryption action in a VC scheme is conducted by carefully aligning and superimposing the gathered shares, and the secret is displayed on the superimposed share. The user can inspect and recognize the secret exhibited on the superimposed share using the naked eye without any computation.

The unique property of decoding the secret without any computer computation makes VC a good tool for sharing secrets in environments with insufficient computing power. It has attracted many researchers' interest in the past two decades, and many proposals of the VC schemes have been made to improve the efficiency and/or the displaying effects of the revealed secrets. In general, pixel expansion and contrast of the superimposed result are considered the two most important properties in measuring the efficiency of a VC scheme. Pixel expansion m refers to the number of pixels in a share used to encode a

* Corresponding author at: Department of Computer Science & Engineering, Yuan Ze University, 135 Far-East Rd., Chung-Li, Taoyuan 320, Taiwan. Tel.: +886 3 4638800 3003; fax: +886 3 4638850.

E-mail address: rzwang@saturn.yzu.edu.tw (R.-Z. Wang).

http://dx.doi.org/10.1016/j.ins.2014.12.046

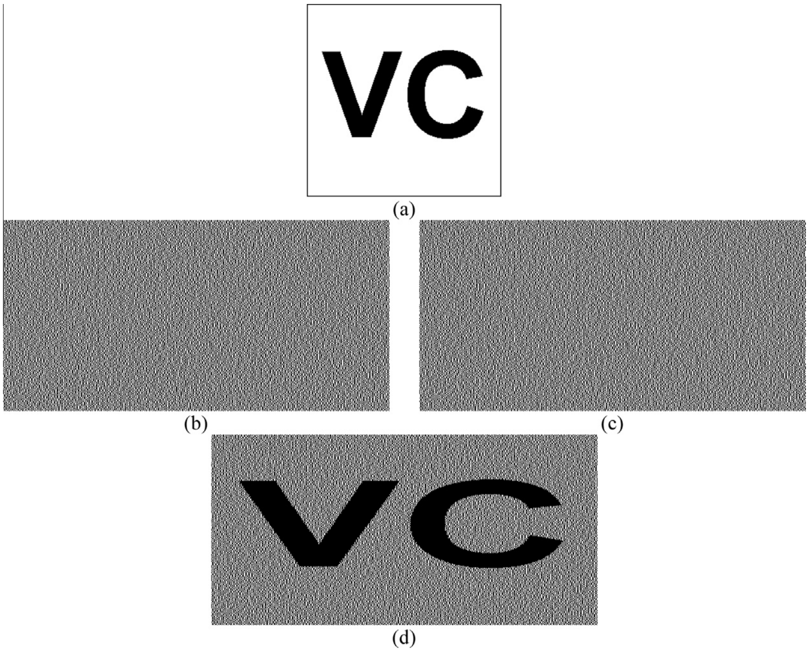

Fig. 1. Computer simulation of Shamir's (2,2) VC scheme: (a) secret image; (b) share 1; (c) share 2; (d) superimposing result of the two shares.

pixel of the secret image. The contrast α is the relative luminance difference between regions on the superimposed share that come from a white pixel and a black pixel in the original image, which can be expressed by the following equation:

$$\alpha = \frac{|n_w - n_b|}{m}, \tag{1}$$

where n_w and n_b are the numbers of pixels in the region of a white pixel and the region of a black pixel, respectively. For example, the pixel expansion m in the sharing example shown in Fig. 1 is $m = 2$, and the contrast of the disclosed secret is $\alpha = 1/2$. Smaller pixel expansion and higher contrast are usually considered good properties for a VC scheme, and they are the main research topics explored in the field of VC schemes [1,2,9,10,14,15,18].

Some other VC schemes have been developed to display diverse revealing effects to the secret. Extended VC schemes [23,24] encode the secret image in natural-looking shares to decrease the chance of attracting attention to the secret image. Multi-secret VC schemes [16,18] encode more than one secret among the shares to increase the payload in a sharing instance. The progressive VC scheme [6,19] displays the perceptual quality of the secret image gradually. Incrementing VC scheme [11] discloses a larger number of secrets when more shares are superimposed, and the Tagged VC scheme [12] exhibits an extra tag message in each share singly to provide users with supplementary information.

In 1999, Yang and Laih [5] presented two cheating prevention VC (CPVC) schemes to break the misleading secrets forged by dishonest participants. The first method generates an additional verification share to verify the genuineness of each share, in which the verification share is held by a trusted authority (TA) to check the validity of each share. The second method transforms a conventional VC scheme to another CPVC scheme in which the pixel expansion of the generated shares in the CPVC is larger. Superimposing any two shares reveals the verification image, which can be inspected by the user to check the validity of the shares.

In 2006, Horng et al. [7] also demonstrated a process of collusive cheating by $n + 1$ participants to the other user in $(2, n)$ VC schemes, and they presented two possible solutions to the problem. The first solution was to generate a dedicated verification share for each participant, which the participant can use to investigate the genuineness of the shares gathered from other participants. The second solution uses a $(2, n + l)$, $l \geqslant 1$, VC scheme instead of $(2, n)$ scheme in a 2-out-of-n sharing instance, and this impairs the malicious user's ability to predict the structure of the shares possessed by other participants. Later, Hu and Tzeng [4] presented three robust methods to improve the weaknesses of the above cheating prevention VC schemes [5,7]; two of the robust methods were for conventional VC schemes, and the other method was for the extended VC scheme. Based on Hu and Tzeng's scheme, the CPVC schemes [20–22] generate extra n verification shares to verify the genuineness of shares. Other cheating prevention VC schemes have been proposed using hybrid codebooks or efficient pixel expansion [3,17]. However, the previous CPVC schemes require an additional verification share [4,20,22] and/or greater pixel expansion [4,5,22] to make it possible to resist cheating by malicious participants.

In this paper, a simple method is proposed to endow conventional VC schemes with the ability to prevent cheating. It enables a participant to check the genuineness of the shares gathered from other participants, and it ensures the correctness