Signal Processing 109 (2015) 317–333

Contents lists available at ScienceDirect

Signal Processing

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

Generalized random grids-based threshold visual cryptography with meaningful shares

Xuehu Yan [a,*], Shen Wang [a,*], Xiamu Niu [a], Ching-Nung Yang [b]

[a] School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin, China
[b] Department of CSIE, National Dong Hwa University, Hualien 974, Taiwan

ARTICLE INFO

Article history:
Received 1 July 2014
Received in revised form
20 November 2014
Accepted 1 December 2014
Available online 9 December 2014

Keywords:
Visual cryptography
Visual secret sharing
Random grid
Threshold
Meaningful shares

ABSTRACT

The meaningful share in visual cryptography (VC) is a desired feature because it can increase the efficiency of management and decrease the suspicion of secret image encryptions. Although the traditional user-friendly random grid (RG)-based VC can produce meaningful shares, with the advantages of no pixel expansion and no need for codebook design, current user-friendly RG-based VCs fail to support the general (k, n) threshold and the complementary shares might be required. In this paper, a generalized RG-based VC with meaningful shares is proposed. Besides inheriting the good features of no pixel expansion and no codebook design, the proposed scheme can support (k, n) threshold and provide adaptive visual quality, at the cost of slightly decreasing visual quality of shared images. Our main contribution is to propose a meaningful VC for case (k, n) with no pixel expansion and codebook design. To the best of our knowledge, the proposed scheme is the first method with all of these good features. Both the theoretical analysis and simulation results demonstrate the effectiveness and security of the proposed scheme.

1. Introduction

Along with the wide application and development of internet and multimedia technology, digital images are easily obtained, transmitted and manipulated. Security of digital images protects the sensitive information from the malicious behavior in transmission [1–3]. An alternative method to ensure the confidentiality and high level of security is cryptography [4]. Cryptography deals with the techniques that transform the data between comprehensible and incomprehensible forms by encryption/decryption operations under the control of key(s). It provides the content confidentiality and access control [4]. Even if one bit of the data is destroyed and the whole secret information is not leaked, the data is not available in cryptography. Therefore, retrieving the original data without any distortion is a matter of importance in case of a certain amount of data is lost in the transmission.

Secret image sharing has solved this problem since the method encodes the user data into different secret shadows (shares) and distributes them to multiple participants. Therefore, it has attracted more attention of scientists and engineers. Shamir's polynomial-based scheme [5–8] and visual cryptography(VC) [9–12], are the primary branches in secret sharing.

A (k,n) -threshold secret sharing scheme was first proposed by Shamir in 1979 [5] through encrypting the secret into the constant coefficient of a random $(k-1)$−degree polynomial. The secret image can be perfectly reconstructed using Lagranges interpolation. Inspired by Shamir's scheme. The advantage of Shamir's polynomial-based scheme [5–8] is the secret can be recovered losslessly. Although Shamir's polynomial-based scheme only needs k shares for reconstructing the distortion-less secret image, while it requires

* Corresponding authors.
Tel.: +86 451 86402861; fax: +86 451 86402861 861.
E-mail addresses: ictyanxuehu@163.com, xuehu.yan@ict.hit.edu.cn (X. Yan), shen.wang@hit.edu.cn (S. Wang).

http://dx.doi.org/10.1016/j.sigpro.2014.12.002
0165-1684/© 2014 Elsevier B.V. All rights reserved.

more complicated computations, i.e., Lagrange interpolations, for decoding and known order of shares.

VC was first introduced by Naor and Shamir [9]. VC is a kind of secret sharing scheme [9–12] that allows the decryption of the secret images without cryptographic knowledge and computational devices. In a general (k, n) threshold VC scheme, a secret image is generated into n random shares (also called shadows) which separately reveals nothing about the secret other than the secret size. The n shares are then printed onto transparencies and distributed to n associated participants. The secret image can be visually revealed based on human visual system (HVS) by stacking any k or more shares, while any $k-1$ or less shares give no clue about the secret [9]. VC can be applied in many scenes [12], such as information hiding, watermarking [13], authentication and identification, and transmitting passwords.

The next we will review some traditional VC schemes first, then extended VC(EVC) is discussed which can be divided into two classifications, depending on the pixel expansion is appeared or not.

Inspired by Naor and Shamir's work, the associated VC problems such as contrast, different formats, and pixel expansion were extensively studied by researchers worldwide. Blundo et al. [14] showed an optical threshold VC with perfect black pixels reconstructions. Ateniese et al. [15] proposed a general VC access structure. Color schemes are considered by Krishna et al., Luo et al., Hou et al., and Liu et al. [16–19]. Multiple secrets sharing was given by Shyu et al. [20]. Threshold VC for different whiteness levels was proposed by Eisen [21]. Step construction was proposed by Liu et al. [22] to improve the visual quality in VC. Ito et al. [23] proposed the probabilistic VC by equally selecting a column from corresponding basic matrix. Probabilistic VC for different thresholds was presented by Yang [24]. Cimato et al. [25] further extended the generalization probabilistic VC.

The aforementioned VC schemes all suffer from disadvantage that the shares consisting of noise-like patterns do not take any visual information, which might lead to suspicion of secret image encryption and decrease the shadow management efficiency. To reduce the suspicion of secret information encryption, and to manage the shares efficiently, EVC [26–28], and halftone VC (HVC) [29,11] were presented. Based on the special design of the dithering matrix, Liu et al. [27] proposed an embedded EVC by embedding random shares into meaningful covering shares. To insert the pixels carrying secret information into preexisting encoded halftone shares, Zhou et al. [29] developed HVC based on void and cluster dithering. Furthermore, an error diffusion-based HVC was proposed by Wang et al. [11]. In Wang et al.'s HVC, the secret information is encoded into the halftone images when the grayscale images are halftoned. Since the shares carry both the secret information and visual information with a codebook design in EVC or HVC, they have the limitation that the pixel expansion is large.

Random grid (RG)-based VC maybe an alternative method to overcome the drawbacks, since RG-based VC has no pixel expansion and requires no codebook design. RG-based VC was first presented by Kafri and Keren [30], which encrypts the secret image into two meaningless RGs. To illustrate the principles of RG-based VC, one of the three distinct encryption algorithms presented by Kafri and Keren is shown in Fig. 1. Each secret pixel taken from a secret binary image is encrypted into one subpixel in each of the two RGs. The subpixels are randomly selected from the two columns tabulated under the certain secret pixel. The selection is random so that each column is selected with the same probabilities (50%). Then, the first subpixel is assigned to RG 1 and the following subpixel is assigned to RG 2. Thus, an individual share gives no clue about the secret image. When the subpixels are stacked, the opaque (black) pixels will cover the transparent (white) pixels. The black secret pixel will be decoded into black pixel, and the white secret pixel will be decoded into white pixel or black pixel with the same probabilities (50%). As a result, the secret could be revealed by HVS. Fig. 2 shows an application example of RG-based $(2, 2)$ VC. The secret is encrypted into two random shares which have the same size as the secret image. The revealed image is clearly identified, although some contrast loss occurs.

Secret pixel	□		■	
RG 1	□	■	□	■
RG 2	□	■	■	□
Probability	50%	50%	50%	50%
Stacking RG 1 & 2	□	■	■	■

Fig. 1. In a RG-based $(2, 2)$ VC, a secret pixel is encrypted into one pixel in each of the two shares (RGs).

Follow-up investigations on RG-based VC were discussed to extend the features of RG-based $(2, 2)$ VC [31], such as contrast [32,33], color images [34], $(2, n)$ threshold [35–37], (n, n) threshold [31,38] and (k, n) threshold [39,40]. Unfortunately, the previous RG-based VC does not support meaningful shares. To exploit meaningful shares in RG-based VC, Chen and Tsao [31] proposed a friendly RG-based $(2, 2)$ VC by designing a procedure of distinguishing different light transmissions on the two shares. However, in Chen and Tsao's user-friendly RG-based $(2, 2)$ VC, complementary shares are used to achieve adjustable visual quality. In addition, the method is not for (k, n) threshold, where $k < n$.

The main motivation of this paper is to propose a threshold meaningful VC with no pixel expansion and no codebook design, which can be used in wider applications than traditional VCs. In this paper, a generated RG-based VC with meaningful shares is proposed. The proposed scheme can support (k, n) threshold and provide adaptive visual quality based on RG-based $(2, 2)$ VC and RG-based $(2, n)$ VC, at the cost of slightly decreasing the visual quality of shared images. The proposed scheme exploits generated RG to gain different light transmissions on shares, thus meaningful shares are obtained. In addition, the proposed scheme requires no codebook design as well as has no pixel expansion. Simulations results and theoretical analysis are given to show the advantages and effectiveness of the proposed scheme.