Signal Processing 97 (2014) 64–82

Contents lists available at ScienceDirect

Signal Processing

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

Improved tagged visual cryptography by random grids

Xiaotian Wu [a], Wei Sun [b,*]

[a] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510006, China
[b] School of Software, Sun Yat-Sen University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 18 July 2013
Received in revised form
24 September 2013
Accepted 23 October 2013
Available online 4 November 2013

Keywords:
Visual cryptography
Visual secret sharing
Random grid
Tagged-share
Cheat preventing

ABSTRACT

Tagged visual cryptography (TVC) is a brand new type of visual cryptography (VC) in which additional tags are concealed into each generated share. By folding up each single share, the associated tagged pattern is visually revealed. Such additional tag patterns greatly enrich extra abilities of VC, such as augmented message carried in a single share, user-friendly interface to manage the shares, and/or evidence for verifying consistency among those shares cooperating in a decryption instance. However, reported (k, n) TVC proposed by Wang and Hsu still suffers from the defects such as pixel expansion, code book required in the encoding phase and low image quality. In this work, a (k, n) TVC by adopting the concept of random grid (RG) is introduced. The proposed method can solve the pixel expansion and code book needed problems. Further, cheating activity can be prevented by the proposed algorithm. Superior visual quality of both the recovered secret image and reconstructed tag image is provided as well according to the theoretical analysis and demonstrated experiments.

1. Introduction

Visual cryptography (VC), which is also called visual secret sharing (VSS), is a secret sharing paradigm for images in which the decryption is done by superimposing the stacked shares via human visual system. An initial model of (k, n) VC was proposed by Naor and Shamir [1], where a binary secret image is encrypted into n meaningless shares. The secret image can be visually revealed by stacking any k or more shares together. Whereas, any $k-1$ or less shares give no clue about the secret.

Taking a (2, 2) VC experiment for example, a code book comprising all the code words being of the size 2×2 subpixels is adopted, as demonstrated in Fig. 1. A secret image is encrypted by the code book and two shares are generated, where every share is four times as big as the original secret image. Specifically, when the secret pixel is white (resp. balck), one of the six columns in the white (resp. black) group is randomly chosen and assigned to the two shares. When the two shares are stacked, the reconstructed black pixel is represented by four black subpixels. Whereas, the reconstructed white pixels is denoted by two black and two white subpixels. An example by using the (2, 2) VC code book is illustrated in Fig. 2, where the secret image is shown in Fig. 2(a) and the two shares are illustrated in Fig. 2(b) and (c). Fig. 2 depicts the stacked result by two shares.

Wide studies on VC and its associated properties such as meaningful appearance of the shares, sharing different format of secret image, contrast and pixel expansion are conducted based on the pioneer work [1]. Constructions of VC for general access structure are discussed in [2–4]. Extended VC [4,5] and halftone VC [6,7] are proposed for constructing shadows with meaningful contents, so that users can identify the shares by the meaningful appearance. Moreover, the chance of leading to suspicion on secret image encryption is further reduced. Investigation on achieving optimal contrast is provided in [8,9]. VC methods, such as probabilistic VC and random grid-based

* Corresponding author. Tel.: +86 13380062669.
E-mail addresses: wxt.sysu@gmail.com (X. Wu), sunwei@mail.sysu.edu.cn (W. Sun).

0165-1684/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.10.023

VC, for constructing non-expansible shares, are introduced as well.

For probabilistic VC, Ito et al. [10] introduced a methodology that encodes a black/white secret pixel by using a column which is selected from the corresponding black/white basis matrix. Yang [11] proposed a probabilistic model for constructing VSS without pixel expansion. Different threshold VC schemes were discussed. Further, a generalization of Yang's model [11] was introduced by Cimato et al. [12]. For big enough value of pixel expansion m, their model reduces to the classical deterministic model. For $m=1$, their model reduces to one of Yang's methods. In these probabilistic VC schemes, code book is still required to construct the shares in the encryption phase. Sometimes, designing such a code book is complicated.

Random grid (RG) is another technique to construct VC shares without pixel expansion. Major advantages of RG-based VC are that code book is not required in the encryption phase, and pixel expansion problem is solved. The initial idea of RG was first introduced by Kafri and Keren [13]. Three distinct methods for sharing a binary secret image into two RGs were presented as well. Inspired by Kafri and Keren, Shyu [14] presented the enhanced schemes to encrypt grayscale/color images for the (2, 2) case, as well as the (n, n) case [15]. Chen and Tsao [16] proposed algorithms to construct RG-based VC for (2, n) and (n, n) cases. Further, the same authors introduced a (k, n) threshold VSS [17]. A more generalized RG-based VC for access structure was presented in [18,19]. Other researches on RG-based VC can be found in [20–26].

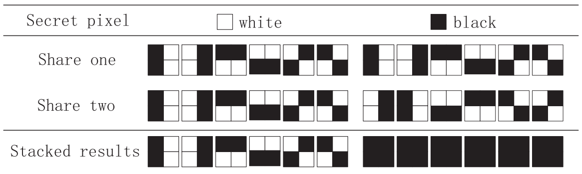

Fig. 1. Code book of a (2, 2) VC.

In the above-mentioned VC, useful information to users are not carried in the random-looking shares. Recently, Wang and Lee [27] introduced a RG-based VC, where certain patterns are tagged into each single share. By folding up a share, the associated tagged image is visually reconstructed. Such additional revealed information in a share provides extra abilities for a VC scheme such as augmented message carried in a single share, user-friendly interface to manage the shares, and/or evidence for verifying consistency among those shares cooperating in a decryption instance. But Wang and Lee's method [27] is limited in (2, 2) scheme and the patterns hiding in each share are constrained and depend on the content of the original secret image. Later, an improved tagged VC (TVC) was proposed by Wang and Hsu [28], where matrix-based VC and probabilistic VC are adopted for the tagged-share construction. However, some deficiencies still remain in their work, as described in the following:

- Pixel expansion. The shares are expanded when matrix-based VC are used.
- Code book needed. No matter matrix-based VC or probabilistic VC is applied, a code book is required in the encryption phase. Sometimes, designing a code book is not trivial.
- Reduced visual quality. Secret image with reduced visual quality reveals due to the tag image stamping procedure. Moreover, the visual quality of reconstructed tagged image is unsatisfactory as well.

In this work, a (k, n) RG-based TVC is proposed to solve the above-mentioned problems. In the proposed method, each share is non-expansible and code book is not required in the encryption phase. More significantly, better visual quality is provided by our approach and the cheating activity [20,29–31] can be prevented as well. The remaining part of this paper is organized as follows. RG-based VC is briefly described in Section 2. Section 3 introduces the (k, n) RG-based TVC. Experimental results and discussions are provided in Section 4. Section 5 gives some concluding remarks.

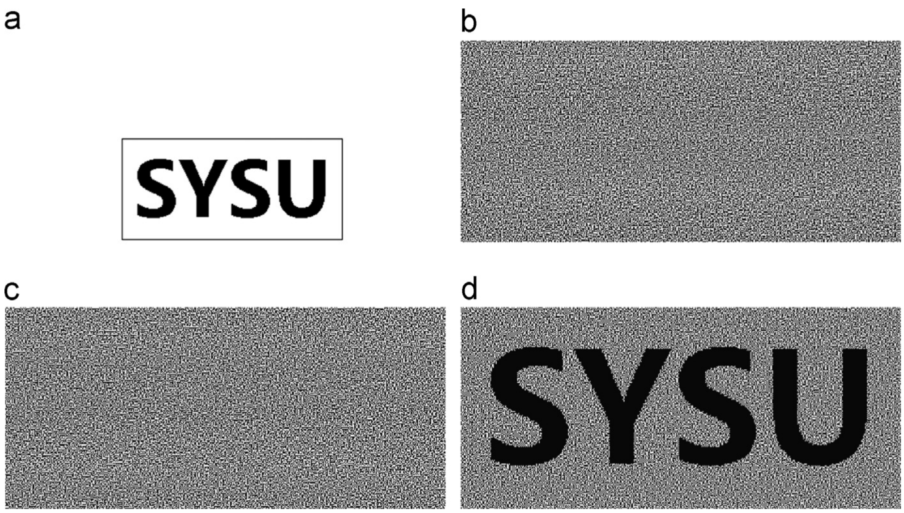

Fig. 2. An example of (2, 2) VC. (a) The secret image, (b) and (c) two generated shares and (d) stacked result of the two shares.