Information Sciences 271 (2014) 246–263

Contents lists available at ScienceDirect

Information Sciences

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

New extended visual cryptography schemes with clearer shadow images

Ching-Nung Yang *, Yao-Yu Yang

Department of Computer Science and Information Engineering, National Dong Hwa University, #1, Sec. 2, Da Hsueh Rd., Hualien, Taiwan

ARTICLE INFO

Article history:
Received 17 March 2009
Received in revised form 14 August 2013
Accepted 15 February 2014
Available online 25 February 2014

Keywords:
Image secret sharing
Visual cryptography
Visual secret sharing
Shadow image
Digital halftoning

ABSTRACT

Visual cryptography scheme (VCS) encodes a visual information (pictures, text, etc.) into several noise-like shadow images. In VCS, each shadow image can be made on a transparency. By stacking transparencies and stack them on an overhead projector, we can visually decode the secret through human visual system without the assistance of any hardware or computation. However, noise-like shadows of VCS were suspected to censors and difficult for identification and management. Therefore, the extended VCS (EVCS) with meaningful shadow images had been proposed to address this problem of suspicion. In this paper, we employ a digital halftoning technology to propose a new EVCS whose shadow images are clearer in comparing with existing EVCSs.

1. Introduction

In (k,n) visual cryptography scheme (VCS), where $k \leqslant n$, a visual secret image is divided into n shadow images (referred to be shadows). In (k,n)-VCS, each shadow image can be made on a transparency. By stacking any k transparencies on an overhead projector, we can visually decode the secret through human visual system without the assistance of any hardware or computation. In stacking $k-1$ or fewer shadows, we cannot recover the secret image. This novel decoding property may serve to securely and cheaply share alphanumeric characters (e.g., passwords or safe-combinations) where users hope to recover the key without using computer for some security reasons or when no computer is temporarily available. Recently, this stacking-to-see property has attracted attention. VCS is not only an important and active research area, but also can provide practical applications in combining watermark, fingerprint, Google street view, and bar code [32,25,36,42]. More applications of VCS can be found in Chapter 12 "Applications of Visual Cryptography" in [7]. The following briefly surveys the VCS framework.

The first VCS was proposed by Naor and Shamir [27], which uses whiteness to distinguish black color from white color. A black-and-white secret image is shared into noise-like shadows by subdividing a secret pixel into m (referred to as the pixel expansion) subpixels in each of n shadows. The shadow size is m times expanded, and thus the visual quality of a reconstructed image is degraded by this pixel expansion. Most research papers have been published to reduce the pixel expansion [18,19,39,40,43,6,34]. Some of them can even have no pixel expansion ($m = 1$) [18,39,6,34]. Another secure imaging technology is random grid [12,35,13], which is similar to VCS with non-expanded shadow size. Accordingly, VCSs with specific features, such as sharing multiple secrets [3,11,49,29,31,51], cheating prevention [14,15], solving misalignment problem [48,23], achieving the ideal contrast [5,47], keeping aspect ratio invariant [41,44], sharing gray/color image

* Corresponding author. Tel.: +886 3 8634025; fax: +886 3 8634010.
E-mail address: cnyang@mail.ndhu.edu.tw (C.-N. Yang).

http://dx.doi.org/10.1016/j.ins.2014.02.099
0020-0255/

[33,38,16,21,2,4,46,20,34], providing progress recovery [17], providing region incrementing property [30,50], and language letter based VCS [22] were proposed.

VCSs have noise-like shadows with black and white random dots, which are suspected to censors and difficult for identification and management. A VCS with meaningful shadow (often being a natural image) is referred to as extended VCS (EVCS) were given in [27,1,45,37,24] to address this problem of suspicion. Some VCS-like schemes [8,9,26] also had such "extended capability" (meaningful shadow). In [26], the authors used circle subpixels to design an EVCS. Other two methods [8,9] provided the high-quality meaningful shadows but they needed an optical interferometer [8] and a 3-D viewer [9] for decoding.

In this paper, we adopt the digital halftoning technology and arrange the black dots on shadows according to the specific patterns of digital halftone image to retain a high-quality cover image shown on shadows. Three constructions are proposed. *Construction 1* is an extension of Naor and Shamir's (2,2)-EVCS. *Construction 2* is a (k,n)-EVCS and *Construction 3* is a (2,2)-EVCS, and these two constructions loosen the contrast condition of EVCS to improve the visual quality of shadow quite substantially. However, the halftone cover image remains on a reconstructed image and diminishes the clearness of a secret. The rest of this paper is organized as follows. Section 2 describes the previous EVCSs. Three constructions based on the digital halftoning technology are introduced in Section 3. Experiment and comparison are given in Section 4. Finally, Section 5 concludes the paper.

2. Preliminaries

2.1. VCS with noise-like shadows

Naor–Shamir's VCS used a whiteness to distinguish the black color from the white color – i.e., "$m-h$"B"h"W (respectively, "$m-l$"B"l"W) represents a white (respectively, black) secret pixel – where h and l are referred to as the whiteness of white and black colors, respectively, and $0 \leqslant l < h \leqslant m$.

A (k,n)-VCS can be designed using two basis $n \times m$ matrices B_1 and B_0 with elements "1" and "0" denoting black and white subpixels, respectively. When sharing a black (respectively, white) secret pixel, the dealer randomly chooses one row of a matrix in the set which includes all matrices obtained by permuting the columns in B_1 (respectively, B_0) to a relative shadow. Let OR $(B_i|r)$, $i = 0, 1$, denote the OR-ed vector of any r rows in B_i, and $H(\cdot)$ be the Hamming weight function. Then, basis matrices of (k,n)-VCS should satisfy the following conditions.

(1–1) $H(\text{OR}(B_1|r)) = H(\text{OR}(B_0|r))$ for $r \leqslant (k-1)$.
(1–2) $H(\text{OR}(B_1|r)) \geqslant (m-l)$ and $H(\text{OR}(B_0|r)) \leqslant (m-h))$ for $r = k$, where $0 \leqslant l < h \leqslant m$.

Condition (1–1) is often referred to as the security condition and assures a (k,n)-VCS of perfect secrecy. Condition (1–2) is the contrast condition, in which the different contrasts of the black and white colors are defined so that a secret image can be recognized.

Example 1. Construct a (2,2)-VCS of $h = 2$, $l = 0$ and $m = 4$ by using $B_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ and $B_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$. The secret is an alphanumeric image 3.

This (2,2)-VCS has $H(\text{OR}(B_1|2)) = 4$, $H(\text{OR}(B_0|2)) = 2$, and $H(\text{OR}(B_1|1)) = H(\text{OR}(B_0|1)) = 2$, which satisfy (1–1) and (1–2) conditions. In a reconstructed image, the black color is 4B0W and the white color is 2B2W. We use xByW to represent $(\overbrace{1\cdots1}^{x},\overbrace{0\cdots0}^{y})$ and its permutations. Because all 4-subpixel blocks in shadows are 2B2W, shadows are noise-like. Fig. 1(a) shows two noise-like shadows (S_1 and S_2), and the reconstructed image for stacking two shadows ($S_1 + S_2$) is shown in Fig. 1(b). A secret 3 is revealed.

2.2. EVCS with meaningful shadow images

In [27], the authors also showed a (2,2)-EVCS with a meaningful cover image on shadows. The contrast and security conditions of EVCS are formally defined in [1]. Also, an optimal (k,k)-EVCS and a general (k,n)-EVCS were proposed. The EVCS in [1] is described by a general access structure, which is a specification of all qualified and forbidden subsets of participants that define which combinations can reveal the secret image. Let $\{\Gamma_{Qual}, \Gamma_{Forb}\}$-VCS be a VCS of a general access structure. A qualified set Γ_{Qual} and a forbidden set Γ_{Forb} are non-empty subsets of a set $P = \{1,2,\ldots,n\}$, where $i \in \{1,n\}$ is a participant "i", $\Gamma_{Qual} \subseteq 2^P$, $\Gamma_{Forb} \subseteq 2^P$ and $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. Any set $X = \{i_1,i_2,\ldots,i_r\} \in \Gamma_{Qual}$, where Participants $\{i_1,i_2,\ldots,i_r\} \in P$, can reveal a secret image; but any set $X \in \Gamma_{Forb}$ cannot recover the secret image. For example, a simple (2,2)-VCS can be represented by a $\{\Gamma_{Qual}, \Gamma_{Forb}\}$-VCS, where $\Gamma_{Qual} = \{1,2\}$ and $\Gamma_{Forb} = \{\{1\},\{2\}\}$.

A $(\Gamma_{Qual},\Gamma_{Forb})$-EVCS with a general access structure can be described by $2^{(n+1)}$ basis $n \times m$ Boolean matrices $\{B_s^{c_1\cdots c_n}\}$. The corresponding sets are $\{C_s^{c_1\cdots c_n}\}$ including all matrices obtained by permuting the columns in $B_s^{c_1\cdots c_n}$, where $c_i \in \{0(\text{white}), 1(\text{black})\}$, $1 \leqslant i \leqslant n$, denotes the color on i-th cover image C_i, and $s \in \{0,1\}$ is the color of a secret image. For example, the B_0^{11} of a (2,2)-EVCS is a matrix that the pixels of both cover images c_1 and c_2 are all black colors, and their stacked result