Measurement 95 (2017) 480–493

Contents lists available at ScienceDirect

Measurement

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

Color transfer visual cryptography with perfect security

Ching-Nung Yang [a,*], Tzu-Chia Tung [a], Fu-Heng Wu [a], Zhili Zhou [b]

[a] Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan
[b] School of Computer and Software, NanJing University of Information Science & Technology, China

ARTICLE INFO

Article history:
Received 19 October 2015
Received in revised form 13 September 2016
Accepted 14 October 2016
Available online 17 October 2016

Keywords:
Visual cryptography
Secret sharing
Threshold scheme
Digital halftoning
Halftoned image
Color transfer

ABSTRACT

Recently, Luo et al. introduced the concept of the color transfer visual cryptographic scheme (CTVCS) by embedding the information of color channels *R*, *G* and *B* into the conventional (k, n)-VCS. Luo et al.'s (k, n)-CTVCS visually decoded the halftoned secret image by stacking any k shadow images similar to the conventional (k, n)-VCS and obtained a high-quality color image. However, Luo et al.'s (k, n)-CTVCS requires a key in the encoding and decoding phases and therefore it is, strictly speaking, not a threshold scheme with perfect security. In this study, we solved this security problem and proposed a (k, n)-CTVCS that does not require a key. This experiment indicated that the proposed solution achieves the same feature (obtaining the original color image) as Luo et al.'s (k, n)-CTVCS. In addition, we formally defined contrast and security conditions of a (k, n)-CTVCS and demonstrated that our constructions satisfied the contrast and security conditions of a (k, n)-CTVCS.

1. Introduction

The cryptographic technique for visually sharing secret images, denoted as visual cryptography scheme (VCS), was first proposed by Naor and Shamir [1]. For a (k, n)-VCS, a secret image is shared into n shadow images (referred to as shadows) by subdividing a secret pixel into m subpixels on shadows. This value m is referred to as pixel expansion. In (k, n)-VCS, any k participants may reconstruct the secret image by simply stacking together the shadows they own. However, $(k-1)$ or fewer shadows do not reveal any information. The VCS is beneficial because the reconstruction phase does not require any computation and is performed directly by the human visual system. This novel stacking-to-see property may be used in certain intended applications. For example, it is very suitable to securely and cheaply share short messages, e.g., passwords or safe combinations that are often represented by alphanumeric characters.

Naor and Shamir's VCS [1] separates the halftoned (black-and-white) secret image into shadows. Actually, there is no difference between the pixel and the subpixel except that the "pixel" is the secret pixel in a secret image and the "subpixel" is the pixel located in shadows. Therefore, the shadow size is expanded m times. Because the visual quality of a reconstructed image is degraded by large pixel expansion, most studies have proposed to reduce pixel expansion [2–7] and certain studies did not include any pixel expansion. To avoid the pixel expansion, Ito et al. [2] proposed a VCS with a non-expandable shadow size (i.e., $m = 1$). Yang [4] formally defined this scheme as the probabilistic VCS (PVCS) and provided various constructions. Afterwards, a generalized PVCS was introduced by Cimato et al. [5]. Because the conventional VCS uses the fixed m-pixel block to represent a secret pixel, the conventional VCS is referred to as deterministic VCS (DVCS). The invention of VCS is often credited to Naor and Shamir [1]. This is true, but we should note that a very similar concept, the random grid (RG), was introduced by Kafri and Keren [8]. RG [9–11] and VCS are identical with the exception of the terminology. Furthermore, similar to PVCS, RG does not include pixel expansion. In fact, researchers should not separate the study of DVCS, PVCS and RG. Recently, the authors in [12,13] have theoretically provided evidence that these models (DVCS, PVCS and RG) are related to each other but are different methods of approaching the same problem. Other VCSs with specific functions, such as sharing multiple secrets, providing misalignment tolerance, cheating prevention, achieving the ideal contrast, providing region incrementing property, providing progressive recovery, combining other secret image sharing and addressing continuous-tone image, were subsequently proposed [14–22].

VCS can also be applied to color images. One solution is to convert the color image into a halftoned color image by using a halftoning technique then processing each halftoned color plane using black-and-white VCS. Various color VCSs (CVCSs) have been analyzed [23–29]. Another concept of color-black-and-white VCS

* Corresponding author at: #1, Sec. 2, Da Hsueh Rd., Hualien, Taiwan.
E-mail address: cnyang@mail.ndhu.edu.tw (C.-N. Yang).

http://dx.doi.org/10.1016/j.measurement.2016.10.042
0263-2241/

(referred to as CBW-VCS) was introduced [30]. Similar to the CVCS, the CBW-VCS has color pixels on shadows but shares a black-and-white secret image.

The stacked result of CVCS is not the original color image. Recently, Luo et al. [31] proposed a (k, n) color transfer VCS (CTVCS) to add the color transfer ability into the conventional (k, n)-VCS. Luo et al.'s (k, n)-CTVCS includes black-and-white shadows (different from the CVCS and CBW-VCS) and visually decodes a halftoned image by stacking shadows (similar to VCS). Moreover, Luo et al.'s CTVCS can obtain the halftoned color planes R, G and B. In this study, we use the term "color bit" to represent "color plane" because the information of each halftoned R, G and B is binary. By recomposing these three halftoned color planes, we obtain a halftoned color image. The visual quality of halftoned color image is sufficient to be used in certain commercial products, e.g., the cholesteric liquid crystal display (ChLCD) used in electronic books and advertising boards.

However, Luo et al.'s CTVCS requires a key for the encoding and decoding phases. The key could be compromised. The color bits could be obtained even though the number of involved shadows does not reach the threshold. Therefore, Luo et al.'s CTVCS is, strictly speaking, not a threshold scheme because the security of recovering color bits requires a key. In this study, we use the inherent property of a digital image to propose a (k, n)-CTVCS that does not require a key. The remainder of this paper is organized as follows. In Section 2, we introduce the concepts of VCS and Luo et al.'s CTVCS. Motivation and design concept are described in Section 3. In Section 4, we formally define the contrast and security conditions of a (k, n)-CTVCS and provide two constructions: the proposed (k, n)-CTVCS and the enhanced (k, n)-CTVCS. Both (k, n)-CTVCSs correctly obtain the original color image similar to Luo et al.'s (k, n)-CTVCS. Meanwhile, the enhanced (k, n)-CTVCS improves the proposed (k, n)-CTVCS to achieve a better visual quality of the stacked halftoned image. In addition, we theoretically provide evidence that our CTVCSs are perfect secret sharing schemes that satisfy contrast and security conditions. Experiment, comparison and discussion are provided in Section 5. Finally, the conclusion is provided in Section 6.

2. Preliminaries

2.1. Naor and Shamir's (k, n)-VCS

Naor and Shamir's (k, n)-VCS is implemented by using $n \times m$ black and white Boolean matrices, B_1 and B_0. The collection C_1 (respectively, C_0) is a set obtained by permuting the columns of B_1 (respectively, B_0) in all possible ways. When sharing a black (respectively, white) secret pixel, the dealer randomly selects one matrix in C_1 (respectively, C_0) and selects a row for a relative shadow. Each h black subpixels and $(m - h)$ white subpixels (denoted as hB$(m - h)$ W) and lB$(m - l)$ W, where $0 \leqslant l < h \leqslant m$ in a m-pixel block represents a black and white secret pixel. The values of h and l represent the blackness of black color and white color.

The corresponding m subpixels in n shadows may be represented by an $n \times m$ Boolean matrix $S = [s_{ij}]$, where the element s_{ij} is the j-th subpixel in the i-th shadow. A black subpixel is represented by "1" and a white subpixel is represented by "0." When stacking r shadows together, the gray-level of each secret pixel (m-subpixel block) is proportional to the Hamming weight $w(v)$, where the vector v is the OR-ed vector of the selected r rows. Consider that M is an $n \times m$ matrix. Let $(M|r)$ be an $r \times m$ matrix selecting any r rows from M. In addition, the notation add$(M|r)$ denotes the OR-ed vector of all r rows in $(M|r)$ and the notation $D(M|r)$ denotes a set that includes all matrices obtained by permuting all columns in $(M|r)$. The formal definition of a VCS is provided as follows.

Definition. A (k, n)-VCS is obtained by $n \times m$ black and white base matrices, B_1 and B_0, that satisfy the following two conditions.

> (V-1) We obtain $w(\text{add}(B_1|k)) \geqslant h$ and $w(\text{add}(B_0|k)) \leqslant l$.
> (V-2) The collections $D(M_1|r)$ and $D(M_0|r)$ are indistinguishable in the sense that they include the identical matrices with the identical frequencies, where $M_1 \in C_1$ and $M_0 \in C_0$, for $r \leqslant (k - 1)$. For simplicity, we state that both collections are equivalent, i.e., $D(M_1|r) = D(M_0|r)$.

The first condition (V-1) is the contrast condition, and the second condition (V-2) is the security condition. In [1], the contrast is defined as the difference in blackness between a black pixel and a white pixel in the reconstructed image, i.e., $\alpha = \frac{(h-l)}{m}$.

For the conventional VCS, we always use a deterministic method, hB$(m - h)$W block and lB$(m - l)$W block, to represent a black secret pixel and a white secret pixel, respectively. Thus, the conventional VCS is referred to as deterministic VCS (DVCS). By randomly selecting a column from the corresponding base matrix, we can construct a PVCS. The PVCS has no pixel expansion; however, the PVCS is reconstructed in a probabilistic manner and its visual quality is degraded. Although the shadow of the DVCS is m times that of PVCS, it has a superior reconstructed image. We provide an example to illustrate VCS.

Example 1. Construct (2, 2)-VCS by $B_0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$.

From B_0 and B_1, we obtain $h = 2$, $l = 1$ and $m = 2$. By permuting all columns in B_0 and B_1, we obtain the collections $C_0 = \left\{ \begin{bmatrix} 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \end{bmatrix} \right\}$ and $C_1 = \left\{ \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \end{bmatrix} \right\}$. It is observed that $w(\text{add}(B_1|2)) = 2 \geqslant h$ and $w(\text{add}(B_0|2)) = 1 \leqslant l$ and that $D(M_0|1) = D(M_1|1) = \{[10], [01]\}$. Thus, both conditions (V-1) and (V-2) are satisfied. Let the notation n_1Bn_2 W represent n_1 "1" and n_2 "0" and its permutations. In a reconstructed image, the black color is 2B0W and the white color is 1B1W. Because every 2-subpixel block in two shadows is always 1B1W, the shadows are noise-like. The contrast of this (2, 2)-VCS is $\alpha = \frac{h-l}{m} = 1/2$. □

2.2. Notation

Notations used in this study and their descriptions are listed in Table 1. These notations are used to describe all the schemes (Luo et al.'s (k, n)-CTVCS, the proposed (k, n)-CTVCS and the enhanced (k, n)-CTVCS) throughout this study.

2.3. Luo et al.'s (k, n)-CTVCS

Luo et al.'s scheme uses the stacking-to-see property that visually decodes the black-and-white secret image without the use of a computer. Using a simple logic operation aided by a computer, the R, G and B halftoned images may be obtained for high resolution applications. Luo et al.'s scheme includes two input secret images, the gray-level image GI and the color image CI. Using the digital halftoning technique, the halftoned image HI and three halftoned color images H_R, H_G, and H_B may be obtained from GI and CI. Expand HI to HI' (see definition in Table 1). Then, encode every pixel in HI' by the collections C_{xy}, where x is the secret pixel in HI and y is the color pixel in H_R, H_G, and H_B and $x, y \in \{0, 1\}$. The stacked results from C_{1y} and C_{0y} are black color and white color, respectively. Meanwhile, we use C_{x0} and C_{x1} to represent the white color and the full-intensity