Digital Signal Processing 38 (2015) 53–65

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality

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:
Available online 16 December 2014

Keywords:
Visual cryptography
Visual secret sharing
Extended visual cryptography
Halftone visual cryptography
Meaningful shares

ABSTRACT

In halftone visual cryptography scheme (HVCS), a secret image can be embedded into halftone shares with meaningful information of the cover images. Meaningful shares are significant since the efficiency of shares management will be increased and the suspicion of secret image encryption will be decreased. In this paper, we propose an HVCS construction method with minimum auxiliary black pixels (ABPs) distributed homogeneously, which is realized via embedding secret image into meaningful shares in the halftoned processing of the cover images by error diffusion. Secret information pixels (SIPs) are fixed in parallel and separated maximally from each other before the halftoned processing. The proposed scheme obtains admirable visual quality and some preferable advantages compared with related meaningful VC schemes (VCSs). Simulations and comparisons show the advantages and effectiveness of the proposed scheme.

1. Introduction

Naor and Shamir [1] first introduced visual cryptography (VC). VC is one branch of secret sharing scheme [1–4] whose decryption of the secret images is without cryptographic knowledge and computational devices. In a (k, n) threshold VC scheme (VCS), a secret image is encoded into n noise-like shares (also called shadows). Each share gives no clue about the secret except for the secret size. The n shares are then printed onto transparencies and distributed to n participants. The secret image can be visually revealed based on human visual system (HVS) by superimposing any k or more shares, while any $k-1$ or less shares reveal nothing about the secret [1]. VC [4] can be applied not only in information hiding, but also transmitting passwords, watermarking [5], etc.

Following Naor and Shamir's work, researchers studied the related VC problems such as contrast, different formats and the pixel expansion. An optical threshold VC with perfect black pixels reconstruction was presented by Blundo et al. [6]. Ateniese et al. [7] showed a general VC access structure. Color images schemes were studied by Liu et al. [8], Hou et al. [9], Luo et al. [10] and Krishna et al. [11]. Shyu et al. [12] proposed multiple secrets sharing. Threshold VC for different whiteness levels was proposed by Eisen [13]. Liu et al. [14] introduced step construction to improve the visual quality in VC. Through choosing a column from corresponding basic matrix equally, Ito et al. [15] proposed probabilistic VC. Yang [16] presented probabilistic VC for different thresholds. In addition, the generalization probabilistic VCS was further extended by Cimato et al. [17].

The above mentioned VCSs all have the shortcoming that the shares carry noise-like information rather than meaningful information, which might lead to suspicion of secret image encryption and affect the shares management. Extended VCS (EVCS) was introduced by Ateniese et al. [18], where the shares take both the visual information of the cover images and the secret information. Unfortunately, the method suffers from low image quality of the shares. To improve the image quality, a $(2, 2)$ EVCS for grayscale images was proposed by Nakajima et al. [19]. Two EVCS were presented by Tsai et al. [20] and Wang et al. [21], respectively, by modifying the basic matrices and substituting the subpixels. To exploit meaningful shares, Chen and Tsao [22] proposed a friendly $(2, 2)$ VC by designing a procedure of distinguishing different light transmissions on the two shares. Yang and Yang [23] enhanced the image quality of traditional EVCS through using the range distribution instead of the fixed pattern. The major drawbacks of these methods are unsatisfied security or contrast conditions, no (k, n) threshold, low visual quality, large pixel expansion, or cross interference from the share images [19,21,20,22].

Based on the special design of the dithering matrix, Liu et al. [24] proposed an embedded EVCS by embedding the SIPs into meaningful shares. In Liu et al.'s EVCS [24], to satisfy the contrast

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

http://dx.doi.org/10.1016/j.dsp.2014.12.002
1051-2004/

condition, the cover images are darkened before halftoning which may affect the visual quality of the shares. In addition, there might be slight grid patterns in the shares due to the use of the patterning dithering.

In order to embed secret into the shares, halftone visual cryptography scheme (HVCS) was introduced by Zhou et al. [25] based on dithering. However, in Zhou et al.'s HVCS, the embedding scatter of secret information pixels (SIPs) relies on the content of the cover images, which may decrease the visual quality of the recovered secret image. Moreover, a pair of complementary images are used and some participants may save more than one shares, which may increase the suspicion of secret image encryption and the bandwidth.

Furthermore, three HVCSs were developed by Wang et al. [3] based on error diffusion. In Wang et al.'s methods [3], the SIPs are encoded into meaningful shares in the halftoned processing of the cover images. Unfortunately, the SIPs are generated based on error diffusion of a constant-value grayscale image, which might lead to distortion in the reconstructed secret image. In Wang et al.'s first method, a pair of complementary images are also used. Wang et al.'s second method is only for (k, n) threshold and introduces more auxiliary black pixels (ABPs) to satisfy the contrast condition. The weakness of Wang et al.'s third method is that the input cover images may be given in a selected way.

In this paper, a HVCS with minimum ABPs is proposed. To avoid the distortion and obtain visually satisfactory halftone shares, SIPs are fixed in parallel and separated maximally from each other before the halftoned processing. The proposed scheme embeds these SIPs into meaningful shares in the halftoned processing of the cover images by error diffusion, which is a simply and widely applied halftone technology [26]. We discuss the factors affecting the share image quality and the reconstructed secret image quality. When inserting the ABPs, four factors are considered to obtain a homogeneous scatter of ABPs, including halftone error, global ABPs number, local ABPs number and local density. The extra error introduced by ABPs and SIPs is diffused away by error diffusion. As a result, visually satisfactory halftone shares will be obtained.

With less restrictions on error diffusion, admirable visual quality and some advantages will be obtained by the proposed scheme compared with related meaningful VCSs. We cannot reveal any visual information of the cover images from the reconstructed secret image. The security of the proposed HVCS is ensured by the security of the underlying VC. Simulations are given to show the advantages and effectiveness of the proposed scheme.

The rest of the paper is organized as follows: Section 2 introduces some preliminaries for the proposed scheme. In Section 3, the proposed scheme is presented in detail. Section 4 gives the further extension and comparison with different methods. Section 5 is devoted to experimental results and image quality comparisons. Finally, Section 6 concludes this paper.

2. Preliminaries

First some definitions on VCS and HVCS are presented, which are partially borrowed from [1,7,24,25] and [3]. Furthermore, we give an introduction of error diffusion.

2.1. Definitions of traditional VCS and HVCS

In this paper, only binary secret image is considered, where the white pixel (resp. black pixel) is denoted by 0 (resp. 1).

We denote all the participants as $\mathcal{V} = \{1, 2, \cdots, n\}$. An access structure is denoted by $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$, where Γ_{Qual} (resp. Γ_{Forb}) denotes the superset of qualified subsets (resp. the superset of forbidden subsets), and $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$. In this paper, we will only focus on the access structure with $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = 2^{\mathcal{V}}$.

Generally, a VCS is composed by a pair of matrices collections $(\mathbb{C}_0, \mathbb{C}_1)$, among which the matrices are called share matrices, where each share matrix contains $n \times m$ subpixels.

Definition 1 *(Basic matrix VCS).* (See [7,24].) The boolean $n \times m$ matrices M^0 and M^1 are the basic matrices in a VCS. If we have values $\{h_X : \text{for } X \in \Gamma_{\text{Qual}}\}$ and α $(\alpha > 0)$ satisfy:

1) Contrast condition: If $X = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{\text{Qual}}$, then we can obtain vectors v_0 and v_1 based on superposing (OR) on rows $i_1, i_2, \cdots, i_p$ of M^0 and M^1, respectively, satisfy $w(v_0) \le h_X - \alpha m$ and $w(v_1) \ge h_X$.

2) Security condition: If $F = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{\text{Forb}}$, then we can obtain the $p \times m$ matrices based on restricting M^0 and M^1 to rows $i_1, i_2, \cdots, i_p$, which are equal up to a column permutation.

where,

1. The hamming weight of a vector v is denote as $w(v)$.
2. m is the pixel expansion in the traditional VCS.
3. α is called the contrast of the recovered secret image.
4. h_X indicates the threshold of a qualified subset.

We can permute in all possible ways the columns of the corresponding basic matrix $M^0(M^1)$ [18] to construct the matrix collections $\mathbb{C}_0(\mathbb{C}_1)$.

Refs. [27] and [7] gave the methods to constitute the basic matrices. As examples [27,7], M^0 and M^1 in a $(2, 2)$ VCS are shown as follows:

$$M^0 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \qquad M^1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1}$$

Furthermore, M^0 and M^1 for case $(3, 3)$ are given as follows:

$$M^0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad M^1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{2}$$

The (k, n) threshold can be viewed as a special case of the general access structure. A (k, n) threshold satisfies:

$$\Gamma_{\text{Qual}} = \left\{B \subseteq \mathcal{V} : |B| \ge k\right\} \quad \text{and}$$
$$\Gamma_{\text{Forb}} = \left\{B \subseteq \mathcal{V} : |B| = k - 1\right\}$$

In addition, we introduce the formal definition of HVCS first in this paper as follows:

Definition 2 (*HVCS*). (See [25,3,24].) Aiming to encrypt a secret image S, the dealer inputs n grayscale cover images $\{C_1, C_2, \cdots, C_n\}$, and utilizes halftone technology to generate them into n shares which are partitioned into nonoverlapping halftone blocks of size q $(q > m)$. The HVCS outputs n shares $\{SC_1, SC_2, \cdots, SC_n\}$ through embedding one row of M^0 or M^1 (after permuting their columns randomly) into one block according to $S(i, j)$ at every location (i, j). If we have values $\{h_X : \text{for } X \in \Gamma_{\text{Qual}}\}$ and α greater than zero satisfy:

1. Contrast condition 1: A secret pixel can be reconstructed by the stacking result of each block for a qualified subset of shares. If $X = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{\text{Qual}}$, the blocks at the same position of the shares $SC_{i_1}, SC_{i_2}, \cdots, SC_{i_p}$ are denoted as $B_{i_1}, B_{i_2}, \cdots, B_{i_p}$. Then we can obtain vectors v_0 and v_1 based on superposing (OR) $B_{i_1}, B_{i_2}, \cdots, B_{i_p}$ for a white secret pixel and a black secret pixel, respectively, satisfy $w(v_0) \le h_X - \alpha q$ and $w(v_1) \ge h_X$.
2. Contrast condition 2: No visual information of the cover images can be revealed by the superposing result of each block for a qualified subset of shares.