Measurement 51 (2014) 81–90

Contents lists available at ScienceDirect

Measurement

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

Color transfer in visual cryptography

Hao Luo [a], Hua Chen [a], Yongheng Shang [a,*], Zhenfei Zhao [b], Yanhua Zhang [b]

[a] School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China
[b] School of Electronics and Information, Zhejiang University of Media and Communications, Hangzhou 310018, China

ARTICLE INFO

Article history:
Received 16 September 2013
Received in revised form 14 December 2013
Accepted 27 January 2014
Available online 4 February 2014

Keywords:
(k, n) Visual cryptography model
Color transfer
Digital halftoning
Monochrome output device
Cheating prevention
Cholesteric liquid crystal display

ABSTRACT

Visual cryptography is an important technique for image encryption. This paper proposes a color transfer scheme which can be incorporated into the (k, n) visual cryptography model. In encoder, a color image is encrypted into n noise-like binary share images. When any k or more than k shares are collected, a high quality colorful version of the secret image can be reconstructed with low complexity computations. The principle is motivated to develop a color image secret sharing for output devices such as monochrome printer or fax machines. The generated share images are still binary transparencies which can be directly produced by these low cost output devices. Meanwhile, the security of a (k, n) visual cryptography model is perfectly preserved. When stacking a qualified set of transparencies, the gray level version of secret content can be revealed by human visual system. Nevertheless, the proposed paradigm is cheating immune. It also can be integrated into some emerging display technologies such as cholesteric liquid crystal display. Experimental results and related examples demonstrate the effectiveness and efficiency.

1. Introduction

As a powerful technique for image encryption [1–4] and secret sharing, the paradigm of visual cryptography scheme (VCS) is first introduced by Naor and Shamir [5]. In their (k, n) VCS model, a binary secret image is encrypted into n random noise-like shares (also called transparencies, shadows) and further printed on transparencies held by n participants. When superimposing a qualified set of k or more shares, the secret content is visible to human eyes. In other words, no computer participation or prior knowledge is required for secret decryption. Meanwhile, this VCS is perfectly secure for no secret information will be revealed when less than any k transparencies are overlaid.

In recent years, many various VCS methods are proposed in literatures. Most of them can be summarized as following three aspects. An extensive survey can be referred to [6].

(1) Extend the basic VCS model for grayscale and color image encryption. In these schemes, digital halftoning or its produced halftone images are usually involved [7]. The transparencies could be binary or color halftone images. In order to enhance the security, some transparencies are meaningful images which are jointly produced by VCS and a given camouflage image.
(2) Introduce computer participation for incorporating an extra ability into the conventional VCS. These abilities include progressive transmission, confidential data hiding for authentication, nearly lossless data reconstruction, etc. As a result, the applications of these VCS models are broadened in some specific scenarios.

[*] Corresponding author. Address: No. 38, ZheDa Road, Yuquan Campus, Zhejiang University, School of Aeronautics and Astronautics, Hangzhou 310027, PR China. Tel.: +86 15858259064.
E-mail address: luohao723@126.com (Y. Shang).

http://dx.doi.org/10.1016/j.measurement.2014.01.033
0263-2241/© 2014 Elsevier Ltd. All rights reserved.

(3) Reducing the size expansion of transparencies and enhancing the decrypted image quality [8]. The former work is beneficial to reducing the burden of limited transmission channel and saving storage space. The latter work is useful when a high fidelity secret image should be recovered. This is because the contrast and distortion of stacking decryption mechanism are not acceptable in most cases.

In [9], Hou proposed a VCS for color image secret sharing with following two properties. (1) To obtain a hardcopy of a color transparency, color printers must be available to convert it into cyan, magenta and yellow (CMY) space first (i.e., the complementary red, green and blue (RGB) space), and then adopt C, M, Y inks for color display. However, as the color inks are much more expensive, this scheme is not applicable in the cases where only a monochrome printer can be used. (2) The decrypted image quality is not satisfactory due to the stacking mechanism. In general, the contrast of the decrypted image is much lower in comparison with the original version. In addition, the color inks may be printed slightly out of register due to the mechanical tolerances and hence further visual distortions are introduced.

In Hou's and some other VCS methods, digital halftoning is involved. It is a process to transform a continuous-tone (e.g. 8-bit gray level) image into a two-tone (e.g. 1-bit binary) image. As a product, halftone image is a special kind of binary image for monochrome printing and low cost devices display. It resembles the continuous-tone version by the low-pass filtering of the human visual system (HVS) when viewed from an appropriate distance. So far, the popular halftoning techniques consist of ordered dithering, error diffusion, and iterative methods. Among these three categories, error diffusion achieves a better tradeoff between low complexity computations and moderate halftone image quality.

Generally speaking, the ordinary ink jets and laser printers are only able to apply or not apply ink at a given spatial location of paper or transparency. During gray level image printing, the ink dots were black; while in color image printing, a cyan, magenta, or yellow ink dot is possible at each location. In fact, many color printers can also produce a black ink dot. In digital products, the low cost liquid crystal displays (LCDs) have the same limitation in that they can only turn a pixel on or off.

As one of the most important image features, color has been used in a large quantity of applications [10] including image retrieval, object detection and recognition, target segmentation and tracking, etc. This paper proposes a (k, n) color transfer VCS (CTVCS for short) technique. It can improve the deficiencies of Hou's scheme due to an extra ability of color transfer is incorporated. Color transfer [11] means to recolorize a gray level image using its original color when captured by camera or generated by computer. In [12], a reversible color transfer technique is proposed based on wavelet transform. But it cannot be used in VCS. Actually, reversibility is also the key property of the proposed method. That is, the color information can be nearly recovered from the binary shares or their hardcopy transparencies. In particular, a color image is encrypted into n binary transparencies and the colors can be retrieved from any k or more than k transparencies at a later time.

The CTVCS is implemented by flattening the compressed color information into a single bit-plane with digital halftoning and color decomposition exploited. Specifically, the secret image is decomposed into three color channels (R, G, and B) and transformed into the grayscale version first. Then the digital halftoning is applied to convert the grayscale and three color channel images into halftone versions, respectively. Next, four halftones of the grayscale, R, G, B channels are integrated encrypted with a modified (k, n) VCS. In this way, the color information is also embedded into the transparencies during the processing. In the decoding stage, the inverse procedures are executed due to the reversibility is well preserved. To the best of our knowledge, CTVCS is the first VCS model with the ability of color transfer.

The remained part of this paper is organized as follows. Section 2 reviews the principles of the conventional VCS, secure color transfer techniques and error diffusion halftoning. Section 3 extensively describes the proposed scheme and gives some examples. Section 4 demonstrates the experimental results and discussions. Finally, conclusions are given in Section 5.

2. Related work

2.1. The conventional VCS

The conventional (k, n) VCS consists of two collections of $N \times M$ Boolean (Basis) matrices C_0 and C_1. To share a white (black) pixel, the dealer randomly chooses one of the matrices in C_0 (C_1). Each row of the chosen matrix corresponds to a transparency's subpixels. The solution is regarded as valid if three conditions given in [5] are satisfied.

For description simplicity, an example of (2, 2) VCS principle is shown in Fig. 1. It divides each secret pixel into $M = 2$ subpixels. Each white (denoted by 0) or black (denoted by 1) pixel corresponds to two encryption modes. Each choice contains a pair of white and black pixels.

Three important factors are usually taken into account during a VCS construction. (1) Hamming weight. It refers to the number of non-zero symbols in a symbol sequence. (2) Pixel expansion. It is the number of the subpixels in a shared pixel. (3) Relative difference. It refers to the ratio of the maximum number of black subpixels in a reconstructed white pixel to the minimum number of black subpixels in a reconstructed black pixel.

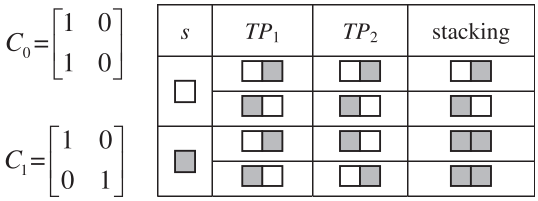
$C_0=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$
$C_1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$
s
TP1
TP2
stacking

Fig. 1. Encryption and decryption strategies of conventional (2, 2) VCS.