Journal of Visual Languages and Computing 25 (2014) 243–250

Contents lists available at ScienceDirect

Journal of Visual Languages and Computing

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

A new visual cryptography with multi-level encoding ☆

Cheng-Chi Lee [a,b], Hong-Hao Chen [c], Hung-Ting Liu [d], Guo-Wei Chen [d], Chwei-Shyong Tsai [d,*]

[a] Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Road, Sinjhuang City, Taipei County 24205, Taiwan, R.O.C

[b] Department of Photonics and Communication Engineering, Asia University, No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C

[c] Department of Computer Science and Information Engineering, National Taiwan University, No. 1, Section 4, Roosevelt Road, Taipei 10617, Taiwan, R.O.C

[d] Department of Management Information Systems, National Chung Hsing University, 250, Kuo Kuang Road, Taichung City, Taiwan, R.O.C

ARTICLE INFO

Article history:
Received 3 September 2009
Received in revised form
6 November 2013
Accepted 8 November 2013
Available online 28 November 2013

Keywords:
Visual secret sharing
Halftone
Visual cryptography
Image
Security

ABSTRACT

Visual secret sharing (VSS) is a visual cryptography scheme which decodes secret messages into several enlarged shares, and distributes them to different participants. The participants can recover the secret messages by stacking their shares, and then secret message can be revealed by human visual sensitivity. Afterward some researchers start to research size invariant scheme, and apply to encode grayscale images such as scenic photos or pictures, not only binary messages. Owing to the gray values distribution of pictures are different, extreme distribution may cause blurred revealed image. In this paper, we proposed a size invariant VSS scheme which is suitable for different distribution of image's gray values. Experiment results show that the reconstructed images of our method, for brighter, darker, and normal images, have clearer and higher contrast, and without apparent artifact and unexpected contour.

1. Introduction

Visual secret sharing (VSS) was first proposed by Naor and Shamir in 1995 [1]. Differing from other techniques in this area of cryptography, the characteristic of visual cryptography need not any machine computation during disclosure of the secret message. The human visual system (HVS) plays the role of recovering the secret instead. Afterwards many variations are developed. Owning to the original VSS model is an expanding method; the output shares are larger than secret image. It increases the transmission cost or inconvenient for carrying. Several researchers devoted to develop size invariant schemes [14,17–26]. In addition to size invariant shares, sharing grayscale images is an interesting topic. Halftoning is a common technique applied in sharing grayscale images. Halftoning is a technique that transforms the continuous-tone image into a binary image [11–13,23]. The concept is using one of the levels of density of the pixels to represent the gray-scale value. If the pixels in a certain region are close together then this area looks darker and, conversely, a lower density region looks lighter. Based on this design, only two colors are needed to monitor a continuous-tone image. Several kinds of halftone techniques have been proposed one after another, such as ordered dither [14], error diffusion [15,16], blue noise masks, dot diffusion, etc.

In order to reach size invariant property, the adoption of the encoded unit varies in each paper. Block-wise and pixel-wise are two commonly-used units. In a pixel-wise strategy, one pixel is encoded at a time [17,19,21]. Image size expansion and the lost of contrast are usually attached to this strategy. Block-wise strategy, proposed later, encodes a block at a time [18]. It usually prevents image size expansion and maintains contrast.

Nevertheless, the size invariant shares actually represent less information of original secret image simultaneously.

☆ This paper has been recommended for acceptance by Shi Kho Chang.

* Corresponding author.
E-mail address: tsaics@nchu.edu.tw (C.-S. Tsai).

1045-926X/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jvlc.2013.11.001

The recovered secret images are obvious blurred, especially for grayscale images. Furthermore, the contrast of recovered secret is decreased through encryption process. For low contrast images, the recovered secret ought to be indistinct. There are few studies investigate encryption method with low contrast secret image. In this paper, we encrypt secret according to image properties, error diffusion halftoning technique and block-wise strategy were used to encode the original secret image.

1.1. General VSS encoding method

In general, cryptography can be simply categorized into two parts, encoding and decoding [2,3]. In the encoding step of VSS, the original image *OI* is divided into n share images$=\{S_1, S_2,\ldots, S_n\}$. As we mentioned earlier, the form of the share images ought to be indistinguishable to keep information from being intercepted so that the images are in noise form. After the images are successfully transmitted to the receiver, the secret can be decoded by stacking $S_1, S_2,\ldots, S_n$ in a specific method according to the encoding algorithm. The general implementation of VSS is by using transparencies. The black pixels are dark on the transparency and white pixels are transparent. The example of recovering rule is shown in Fig. 1.

In general, we define two nm Boolean matrices W^0 and W^1 to represent it and we take a block-wise strategy, for example. To encode a white/black block, one of the matrices in W^0/W^1 is chosen. $[W_{ij}]$ equals 1 if the jth pixel of the ith share is black, and $[W_{ij}]$ equals 0 if the jth pixel of the ith share is white. The structure of W^0 and W^1 depends on the VSS chosen algorithm. The design of two matrices varies depending on the effect that the designer would like to represent. In reality, most researches in VSS mainly focus on this part.

In the decoding phase, after n share images are created and delivered through the internet, superimposing these share images can reveal the secret that sender would like to convey. The gray level of a block in *RI* is determined by the Hamming weight $H(v)$ from which k rows doing an "or" operation result. A block in the *RI* is judged as black if $H(v)\geq d$ and as white if $H(v)\leq d-\alpha m$, for some regular constant d and relative difference α. The value of d is the threshold value that the reconstructed blocks be visually interpreted as black or white. The variable m represents the expansion of the share images toward the original image and the variable α stands for the contrast of black and white pixels in an image. Intuitively, a secret message is expected to be as clear as possible, so that we can expect the value of α to be larger; oppositely, the value of m tends to be smaller.

We give a simple example for the concept discussed above. We briefly divide the original image into two shares and each block contains four pixels; accordingly, n equals to 2. W^0 and W^1 are defined as followed:

$$W^0=\left\{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix}0&0&1&1\\0&0&1&1\end{bmatrix}\right\}$$

$$W^1=\left\{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix}0&0&1&1\\1&1&0&0\end{bmatrix}\right\}$$

We list all of the combinations in Fig. 2.

In 1979, Shamir proposed (t, n) threshold secret sharing [4]. It contains two major components, t and n. A secret dealer initially divides the original image into n share images and then dispatches the n share images to a set of n qualified chosen members, $P=\{P_1, P_2,\ldots, P_n\}$. The following principle best describes the so-called t-out of n secret sharing as follows: For the n qualified members, at least t share images are needed to disclose the secret. Conversely, less than t share image recovers nothing. The background knowledge of secret sharing is based on the Lagrange interpolating polynomial.

The advantage of (t, n) threshold secret sharing is evident. Because at least t members are needed, the secret can be protected, the loss of at most n-t share images is acceptable. Intuitively, a greater value of n indicates a higher security of the secret. As a result, the value of n is expected to be large.

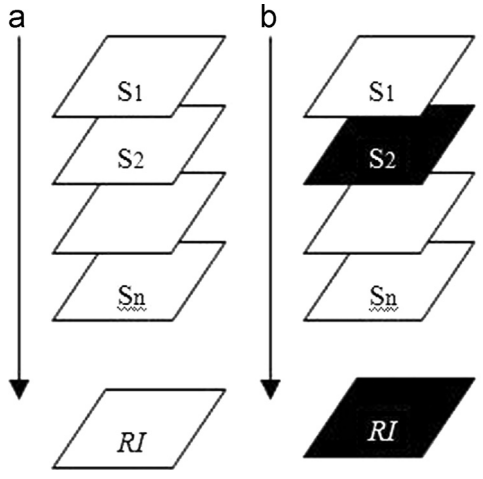

Fig. 1. Two cases of recovered image (*a*) *RI* is transparent if all of the pixels from shares are transparent. (*b*) *RI* is black if at least one of the pixels from shares is black.

Block in *OI*	**Blocks encoded in reconstructed image *RI***
White	
Black	
Probability	$\frac{1}{C_2^4}$ $\frac{1}{C_2^4}$ $\frac{1}{C_2^4}$ $\frac{1}{C_2^4}$ $\frac{1}{C_2^4}$ $\frac{1}{C_2^4}$

Fig. 2. The codebook of 2-out-of-2 visual cryptography.