Digital Signal Processing 40 (2015) 131–139

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Preserving user-friendly shadow and high-contrast quality for multiple visual secret sharing technique

Jung-San Lee [a,*], Chin-Chen Chang [a,b], Ngoc-Tu Huynh [a,d], Hsin-Yi Tsai [c]

[a] Department of Information Engineering and Computer Science, Feng Chia University, Taichung, 40724, Taiwan, ROC
[b] Department of Computer Science and Information Engineering, Asia University, Taichung, 41354, Taiwan, ROC
[c] Department of Computer Science, National Tsing Hua University, 30013 No. 101, Section 2, Kuang-Fu Road, Hsinchu, 30013, Taiwan, ROC
[d] College of Information Technology, The University of Danang, Danang University Village, Luu Quang Vu Street, Danang, Vietnam

ARTICLE INFO

Article history:
Available online 5 March 2015

Keywords:
Visual secret sharing
Visual cryptography
Pixel expansion
User-friendly

ABSTRACT

Traditional secret sharing scheme that encrypts secret image based on mathematical calculation to construct shadows often requires the complicated computation to extract the secret. Later on, conventional visual cryptography scheme was developed to deal with the perplexed calculation in encryption and extraction of previous schemes. The stack-to-see technique can be used easily to reveal the secret by human visual system, which can shorten computation time. However, the expansion of image size and the noise-liked shares of previous schemes lead to the difficulty in transmission and storage. This study uses a pre-defined codebook to encode two secret images into two meaningful transparencies without pixel expansion. According to the turning mechanism, two secret images can be embedded into two shares simultaneously. The decryption process allows the user to get two secrets via turning and stacking. A notable feature of our scheme is that the black pixel value of the secret image can be completely extracted and the vision quality of stacking results can be identified clearly.

1. Introduction

Visual cryptography (VC) was first proposed by Naor and Shamir in 1994 [1]. The concept of visual cryptography technique was based on the secret sharing scheme presented by Shamir in 1979 [2]. The main idea of secret sharing is that more than a predefined number of participants can cooperate to reveal the original ciphertext; otherwise nothing about the secret can be extracted.

In fact, to conceal or reveal the original secret in a secret sharing mechanism needs the adoption of complicated computation. The completion of the computation requires the help of computers. But in the real world, we often face the situation that we cannot access to a computer to figure out any secret information. So, the new thought of reducing the computation was studied.

The idea of visual cryptography is to encrypt a binary secret image into k noise-like shadows which exhibit no private message [2,5–14]. As similar as (k, n)-threshold secret sharing scheme, the visual cryptography mechanism follows the regulation which requires k $(k \leq n)$ shadows to decode confidential information by superimposing these shadows through human visual system (HVS). Nevertheless, $k-1$ or fewer shadows are insufficient to generate confidential message or to leak any private information.

In traditional visual cryptography, the original gray-level secret image needs to be transformed into a halftone image. Then it is encoded by expanding the halftone secret image to achieve the goal of camouflaging the original secret image without any information leaked out. The following is a simple example. A white pixel □ can be encoded into two shadows by randomly choosing one row of white-pixel in Table 1; whereas a black pixel ■ is selected from the row of black-pixel in Table 1 randomly. Since each pixel in secret can be encoded into one block of the combination of black and white pixel, the shadows are cluttered to achieve the confusion of visibility. Extracting the secret by stacking two shadows, we can acquire similar outcome of the original secret. As the human vision is not sensitive to the contrast that makes human eye be able to identify the content of secret from the stacking result. Fig. 1 shows the results of Naor and Shamir's visual cryptography scheme by expanding one pixel to two pixels. The result of Naor–Shamir's method clearly shows that an individual shadow reveals nothing, while the stacking result of two shadows can be used to identify the content of secret.

* Corresponding author.
E-mail address: leejs@fcu.edu.tw (J.-S. Lee).

http://dx.doi.org/10.1016/j.dsp.2015.02.012
1051-2004/

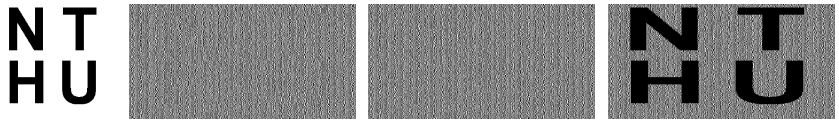

Fig. 1. Results of Naor and Shamir's visual cryptography scheme with pixel expansion = 2.

Table 1
Naor and Shamir's visual cryptography scheme with pixel expansion = 2.

Pixel in secret image	Block in shadow1	Block in shadow2	Block from stacking two shadows
□	■□	■□	■□
	□■	□■	□■
■	■□	■□	■■
	□■	□■	■■

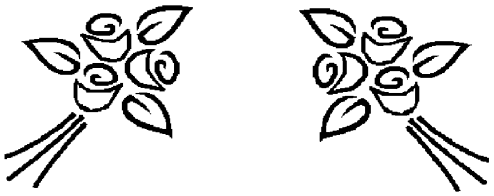

Fig. 2. An example of turning image over with horizontal mechanism.

Naor and Shamir's scheme is really practical for encrypting secret and decreasing the computing ability. Nevertheless, the burden of storage is heavy due to the expanding of original image size. In 2004, Yang [4] used the concept of pre-calculating the probabilities of white pixels in bright and dark areas of secret for encrypting secret without pixel expansion. Based on the probabilities of calculating the contrast difference, an encoding rule was used to create shadows. After stacking transparencies, the high contrast of stacking results is shown clearly. In 2009, Shyu [12] used the random grids technique to encrypt one halftone secret image without expanding pixels of secret. In 2010, Yang and Ciou [5] proposed a hybrid technique combining two different sharing methods: Visual cryptography scheme and polynomial-based image secret sharing scheme. The secret image can be revealed by the concept of stack-to-see, while the original secret can be extracted losslessly. In 2011, Hou and Quan [15] proposed a progressive visual cryptography scheme by using the secret sharing matrices. In Hou and Quan's scheme, N shadows are generated for different participants. The exhibition of ciphertext is proportional to the number of gathered shadows.

Although traditional visual cryptography refused any computation during decryption, its limitation is to hold a noise-like shadow. The meaningless transparencies are not user-friendly with difficulty for identification and management. Therefore, meaningful shadows become the trend of visual cryptography [3]. Fang [14] proposed a friendly progressive method by using a coded sharing codebook. In Fang's scheme, one pixel value is expanded into a 2×2 pixel block to get a meaningful transparency. The decoding way is to superimpose transparencies gradually so that the secret image can be revealed more and more clearly. In other hands, sharing only one confidential message is not efficient. In order to solve the shortcoming, many scholars have proposed multiple secret sharing methods [17,18], which increased the number of secrets to be shared at the same time. Wu and Chen [18] proposed a multiple secret sharing scheme to embed two secret images into two shadows. Two sets of secret can be embedded by rotating a specific shadow. To reveal the first secret, we stack two shadows. Second secret becomes visible if the first shadow is rotated counterclockwise, and stacked together with the second shadow.

Inspired by Feng et al.'s definition [16] and the above-mentions, to reduce the size of the expanded visual cryptography with meaningful shadows is the most important issue in our study. In addition, the new method aims to provide a high contrast of stacking results, which means the stacking result can show a complete black pixel value of secret images. Thus the secret image can be evidently recognized by the human vision. In this paper, the codebook is compiled for encoding meaningful transparencies without pixel expansion. Furthermore, two secret images are embedded into two shadows by the turning over mechanism. Note that the first secret image is displayed by superimposing the first and the second transparency, while the second secret image is extracted by turning the first transparency with horizontal technique to stack onto the second transparency. Fig. 2 illustrates an example of turning over mechanism.

The remainder of this paper is organized as follows. In Section 2, the meaningful visual cryptography scheme is described detailedly. Experimental results of the proposed scheme are shown in Section 3. Finally, Section 4 gives the conclusions of this paper.

2. The proposed method

First, we design an opaque visual cryptography codebook for two secret images (S_1 and S_2) to be embedded into two transparencies (T_1 and T_2). Opaque means the stacking result of two shared images can reveal complete black pixel in the secret. As to the decoding process, the decrypted secret image S'_1 can be revealed by stacking T_1 with T_2 and the decrypted secret image S'_2 is decoded by turning T_1 over and stacking onto T_2.

When two meaningful shared images (T_1 and T_2) are gathered, the *OR* operation is adopted to stack two pixel values in two transparencies. Here, we define the black pixel as 0 and white pixel as 1. The stacking operation for two meaningful shared images is symbolized by $\oplus$, where $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, and $1 \oplus 1 = 1$.

Here, Fig. 3 shows the decrypting operation of the proposed scheme and two secret images are revealed by stacking two transparencies. The size of each image is $M \times N$ and two pixel values in each image are called a symmetric pair which two pixels are turning over with horizontal in relative position. For two symmetric pairs in different decrypted secret images, four pixel values must be considered simultaneously to satisfy the following conditions:

$$\begin{aligned} &S_1(i,j) = T_1(i,j) \oplus T_2(i,j), \\ &S'_1(i,N-j+i) = T'_1(i,N-j+i) \oplus T'_2(i,N-j+i), \\ &S_2(i,j) = T'_1(i,N-j+i) \oplus T_2(i,j), \\ &S'_2(i,N-j+i) = T_1(i,j) \oplus T'_2(i,N-j+i), \end{aligned} \tag{1}$$

where $1 \le i \le M$ and $1 \le j \le \frac{N}{2}$.

Every four-pixel values of secret images $\vec{T} = [T_1(i,j), T'_1(i,N-j+i), T_2(i,j), T'_2(i,N-j+i)]$ should be encoded at the same time. To restrict the complete black pixel of stacking results, two halftone secret images are encoded into two transparencies by an opaque-oriented codebook. Table 2 shows all possible encoding sets for two transparencies that the corresponding results can be chosen for constructing an opaque codebook.