



# A technique for sharing a digital image

Shih-Chieh Wei, Young-Chang Hou<sup>\*</sup>, Yen-Chun Lu

Department of Information management, Tamkang University, No.151, Yingzhuan Road, Tamsui District, New Taipei City 25137, Taiwan, ROC



## ARTICLE INFO

### Article history:

Received 16 September 2013

Received in revised form 3 November 2014

Accepted 27 January 2015

Available online 7 February 2015

### Keywords:

Visual cryptography

Secret image sharing

Color image

Information hiding

## ABSTRACT

A new information hiding scheme for color images based on the concept of visual cryptography and the Boolean exclusive-or (XOR) operation is proposed. Three different schemes with noise-like, meaningful and binary shares are presented. Meaningful shares may reduce suspicion that something is concealed there. Binary shares can achieve both the benefits of smaller share size and good visual quality. Our model can be easily extended from 256 colors to 65,536 or true color images simply by expanding the block size from  $3 \times 3$  to  $4 \times 4$  or  $5 \times 5$ , respectively.

© 2015 Elsevier B.V. All rights reserved.

## 1. Introduction

The combination of computer and communication technology has led to the rapid development and maturity of digital media usage. More and more digital data (text, voice, and image) are transmitted and exchanged over the Internet. It is now very easy to spread, duplicate, capture and modify multimedia data. However, the convenience of sharing digital data over the Internet has produced problems such as misappropriation of data, illegal data usage and other problems regarding intellectual property rights. How to protect important data from attacks becomes a very critical issue. A secure information sharing technique to protect transmitted data from illegal interceptors is needed. Recently, a number of intellectual property protection schemes have been proposed. In all of them, encryption is still the fundamental method used to protect important data files for the purpose of copyright protection, integrity checking and captioning. However, the computation needed for the encryption and decryption processes is quite complex and noise-like encrypted results may tempt an interceptor to break it. To avoid these problems, researchers have developed information hiding techniques to conceal the secret image in a cover image. The result is the so called stego image. The secret image can be delivered with the help of the stego image where the hidden information is not immediately apparent, which enhances the security of the secret information being transmitted. Even if the stego image is captured by illegal interceptors, there is still a good chance to avoid giving rise to suspicions that some secret information may be hidden inside.

Generally speaking, the research studies related to information hiding can be categorized into two schools – the spatial domain [1–6] and the frequency domain [7–12]. The spatial domain methods employ the property where a tiny change of pixels cannot be detected by the human eye; therefore, secret information is embedded by directly modifying the pixel's gray value. The Least Significant Bit (LSB) [1] is the simplest and the most commonly used of the spatial domain techniques. In the frequency domain methods, the host image is mainly turned into frequency space; the secret information is embedded by modifying the coefficients of the frequency space, and then transformed back to form a watermarked image. The main transformation techniques include the Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques.

Cryptography is a technology that transforms plaintext into meaningless or disordered messages through mass and complicated computing. As a result, ciphertext is produced. Without knowing the correct key, this transformation process cannot be reversed under confined resources (e.g., time) to ensure the safety of the secret data. In conventional cryptography, the encryption/decryption algorithms require complex computations, which mean that they are not suitable for an environment without computers. Naor and Shamir [13] introduced a perfectly secure method called visual cryptography (VC) for protecting the secret images. Compared with other traditional encryption/decryption processes, the visual secret sharing (VSS) scheme possesses the advantages of needing only human visual perception to decrypt the secret images, without the need of any complex mathematical operations. The basic model of VC consists of “splitting” the image or watermark into two transparencies (shares). One share can be regarded as the ciphertext and the other one as the secret key (called the key share). Each share looks like random noise, without any clue disclosing the outlines of the secret image. The original image can be revealed simply by superimposing

<sup>\*</sup> Corresponding author. Tel.: +886 2 26215656x3514; fax: +886 2 26209737.  
E-mail address: [yhou@mail.im.tku.edu.tw](mailto:yhou@mail.im.tku.edu.tw) (Y.-C. Hou).

these two shares. Due to its simplicity, the model can be used by anyone, even those without knowledge of cryptography and without the help of a computer to perform any complex computations.

The basic operation used to restore the secret image in VC is by stacking the shares [14–21]. The action of stacking transparencies works like a logical “OR” operation, in which 0 stands for a white pixel and 1 stands for a black pixel. When a black pixel appears in the corresponding position of any share of the stacked images, the result of stacking those pixels will be black. Only when the pixels of all shares for the corresponding position are white, will the result be white. Therefore, as long as the shares are arranged so that the stacked blocks corresponding to white pixels in the secret image remain half black and half white, and those corresponding to black pixels remain all black, the stacked blocks will provide enough contrast for the human eye to identify the secret image without the aid of a computer.

However, the OR operation is the main reason that the white pixels will be reconstructed as half-white-and-half-black blocks. The contrast in the stacked image is reduced to 50%. Therefore, some researchers [10,12,22–24] tried to change the default OR operation of VC into another operation, such as “XOR” to perfectly reconstruct the secret image during the decoding phase if a light-weight device is available. However such VC-like method can only handle pictures with limited colors.

In this study, a new VC-like scheme for digital color images based on XOR is proposed. Our scheme improves upon the drawbacks of [10,12,22–24], i.e., it can handle true color images, using only one operator (XOR) and a mask share is not needed to help in the generation of secured shares. The remainder of this paper is organized as follows. In the next section, we offer a concise introduction of related works. In Section 3, three different information hiding schemes with noise-like, meaningful and binary shares are presented. The experimental results are discussed in Section 4. Finally, a discussion and some conclusions are given in Section 5.

## 2. Literature review

### 2.1. Visual cryptography with the OR operation

In Naor and Shamir’s VC scheme [13], two  $n \times m$  matrices named  $C^0$  and  $C^1$  are used, in which  $n$  is the number of participants and  $m$  is the pixel expansion ratio;  $C^0$  represents the splitting and sharing model for the white pixels, and  $C^1$  for the black ones. Without loss of generality, we take the case where  $(k, n) = (2, 2)$ . Only two out of two shares are needed to recover the secret image in this example. The dispatch matrix is shown in Table 1. Each row of the matrix indicates the content dispatched (0 for white, 1 for black) to each participant. No matter what the pixel value is on the secret image, the blocks in each share appear as one-black-and-one-white blocks. The share’s safety is ensured because the interceptor cannot find any secret information from any one share. When sharing a white pixel, the block content in each share is the same type, otherwise it is a complementary type. After superimposing shares, the white pixels in the secret image will be half-white-and-half-black, while the black pixels will display as fully

black. Although the contrast in the stacked shares is reduced to 50%, it is still easy to decode the confidential data with the human visual system.

Look at the example in Fig. 1. A cartoon (Fig. 1a) is used as the secret image. The cartoon is decomposed into two noise-like transparencies, named share 1 and share 2 (Fig. 1c and d). The two transparencies are superimposed to obtain the restored image (Fig. 1b). Although there is a 50% degradation in the contrast of the restored image (Fig. 1b) compared to the original (Fig. 1a), the secret image can still be easily identified with the human eye.

If the shares are noise-like images, even though interceptors will not be able to obtain any information about the secret image from any single share, they will suspect that something might be concealed there, which increases the risk of being attacked. Therefore, having meaningful content on the shares provides a double layer of protection. The first layer of security is that attackers are not so likely to suspect that there is secret information concealed in the shares, so the possibility of attack is reduced. The second layer of security arises from the visual cryptographic mechanism itself. The attacker cannot perceive anything regarding the secret message from a single share because of the random dispatching scheme. Consequently, the adoption of meaningful-image shares can improve the security of secret information.

Ateniese, Blundo, Santis, and Stinson [14] extended the capability of the visual secret sharing mechanism and proposed a visual cryptography technique using an ordinary image as the cover image. In this dispatching model (Table 2), the shares have black and white contrast (e.g., a black pixel is replaced by a 3-black-and-1-white block, while white pixels are replaced by a 2-black-and-2-white block). Therefore, the shares show the contents of the cover image. When shares are stacked together, 4-black spots represent a black pixel, while 3-black-and-1-white stand for a white pixel. In this way, the contents of the secret images can be clearly identified (Fig. 2). However, in Ateniese’s sharing method, the secret image is limited to black and white.

Hou and Wu [15] extended Ateniese’s visual cryptography model by applying the color decomposition and halftone techniques to decompose a secret color image into three monochrome (cyan, magenta, and yellow) halftone images, to finally produce colored, meaningful shadow images.















Hwang and Chang [16] modified Ateniese’s visual cryptography model by extending each block from  $2 \times 2$  sub-pixels to  $3 \times 3$  sub-pixels. They use 5 and 7 black sub-pixels to represent the white and black pixels of the cover image; while 7 and 9 black sub-pixels are used to represent the white and black pixels of the restored secret image. Chang, Tai, and Lin [17] extended Hwang and Chang’s scheme [16] to a color image. The common drawback for both schemes is that the contrast in the shares and the recovered image is always  $2/9$  which is worse than with Ateniese’s method ( $1/4$ ). With the help of the halftone technique, Zhou, Arce, and Crescenzo [18] and Wang, Arce, and Crescenzo [19] produced better contrast in the recovered image, but the shares were at least four times larger in size than the secret image.

Tsai, Chen, and Horng [20] proposed a scheme that could generate meaningful shares, but the whole cover image could not be concealed from the stacked shares, which makes for a poor quality restored image. Nakajima and Yamaguchi [21] proposed an extended visual cryptography scheme for natural images. Unfortunately, the size of the shares was at least nine times larger than that of the secret image.

### 2.2. Visual cryptography with other operations

All the above research studies are related to visual cryptography, i.e., the decoding method is based on the human visual system, when  $k$  or more than  $k$  shares are stacked. The stacked image will display meaningful contrast to disclose the secret image, and hence no knowledge of cryptography is needed. However, the reconstruction ability of VC is not flawless because the white pixels are reconstructed as half-white-and-half-black blocks which reduce the contrast in the stacked

**Table 1**  
Sharing and stacking scheme for black and white pixels.

Secret image	Share 1	Share 2	Stacked image (OR operation)
			
			
			
			

Download English Version:

<https://daneshyari.com/en/article/454083>

Download Persian Version:

<https://daneshyari.com/article/454083>

[Daneshyari.com](https://daneshyari.com)