2-out-of-3 Secret Sharing Scheme Using Visual Cryptography

Hnin Thiri Zaw, Khin Than Mya
University of Computer Studies, Yangon
h.thirizawucsy@gmail.com

Abstract

With the rapid advancement of network technology, the security of secret data is threatened because anyone may tend to intrude the system or eavesdrop via the communication channel. Most secret sharing schemes are based on cryptography such that the encryption and decryption processes need high computation costs. Visual cryptography, a kind of secret sharing schemes, differs from traditional secret sharing in terms of the efficient decryption process. It encrypts a secret image into several shares and then it can be recovered not only computer but also human visual system. This paper presents 2-out-of-3 secret sharing method by using bit-level decomposition which can be applied to binary, gray-scale and color images. The secret is reconstructed by stacking the encrypted shares the secret image becomes clearly visible. Secret image is divided into three image shares. These shares are distributed to each of three users. Any two or all image shares can be stacked together to recover the original image perfectly.

Keywords: Visual Cryptography, 2-out-of-3 secret sharing scheme, bit-level decomposition

1. Introduction

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin providing information security, rather one of the techniques.

In a secret sharing scheme, each participant gets a piece of secret information, called a share. When the allowed coalitions of participants pool their shares, they can together recover the shared secret; on the other hand, any other subsets, namely non-allowed coalitions, cannot recover the secret information by pooling their shares.

Visual Cryptography (VC), proposed by Naor and Shamir in 1994, is a new type of secret sharing scheme for protecting image-based secrets that has a computation-free decryption process [2]. The simplest form of visual cryptography separates an image into two shares so that either share by itself conveys no information, but when the layers are combined the image is revealed.

This paper proposes 2-out-of-3 secret sharing scheme using visual cryptography with bit-level decomposition. Bit-level decomposition breaks the color of a pixel into binary representation and encrypts the secret image at the bit-level using 2-out-of-3 scheme.

The rest of this paper is organized as follows: Section 2 is related works. Section 3 describes conventional (2, 3) secret sharing scheme and bit-level decomposition in background theory. Section 4 presents overview system design. Section 5 is the experimental results. Final conclusions are presented in Section 6.

2. Related Works

Young-Chang Hou proposed the techniques of halftone technology and color decomposition to construct three methods that can deal with both gray-level and color visual cryptography. Based on the theory of color decomposition, every color on a color image can be decomposed into three primary colors: (C, M, and Y) [7]. Z. Wang and G.R. Arce presented an algorithm for halftone visual cryptography which relied on the simple operation of error diffusion [8]. Sang-Su Lee et al. proposed a method for a visual cryptography scheme that uses phase masks and an interferometer. This method encrypted only gray-level images [6]. The authors presented a multi-pixel encoding called pixel-block aware encoding. It worked for both threshold access structure and general access structure and well for both gray-scale and chromatic images without pixel expansion [3]. M. Nakajima and Y. Yamaguchi focused on the (2, 2) scheme and the method to deal with the natural images with intermediate gray levels. It also showed how to enhance the contrast of the recovered secret [4]. A. Sreekumar and Dr. S. Babu Sundar presented a method to construct an n-out-of-n secret sharing scheme based on a new number system, called Permutation Ordered Binary Number System (POB number system). This scheme provided an efficient way to hide secret information in different shares. Furthermore, the size of shares is less than the size of the secret [1]. This paper presents the 2-out-of-3 secret sharing scheme using bit-level decomposition method. Color image or gray-scale image can be encoded by this system to generate three shared images useful for secure distribution over the public networks. The secret sharing scheme proposed here the secret sharing encryption which differs significantly from traditional image sharing schemes. The original secret image can be recovered perfectly by stacking any two or all shared images.

3. Background Theory

Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an untrusted communication channel [9]. It exploits the human visual system to read the secret image from some overlapping shares thus overcoming the disadvantages of complex computation required in the traditional cryptography. The threshold scheme makes the application of visual cryptography more flexible. With the t-out-of-n threshold scheme ($t \leq n$), the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any t of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than t, the content of the secret image will remain hidden [7].

3.1. Conventional 2-out-of-3 Secret Sharing Scheme

In (2, 3) secret sharing scheme, each pixel of original image is divided into three sub pixels. Each pixel of the original image appears in three modified versions called shares.

Table 1. (2, 3) visual secret sharing (VSS) scheme

Pixel	□	■
Share 1	■□□ □■□ □□■ ■□□ □■□ □□■	■□□ ■□□ □■□ □□■ □□■ □■□
Share 2	■□□ □■□ □□■ ■□□ □■□ □□■	□■□ □□■ ■□□ ■□□ □■□ □□■
Share 3	■□□ □■□ □□■ ■□□ □■□ □□■	□□■ □■□ □□■ □■□ ■□□ ■□□
Stack	■□□ □■□ □□■ ■□□ □■□ □□■	■■■ ■■■ ■■■ ■■■ ■■■ ■■■

$$C_0 = \left[\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right]$$

$$C_1 = \left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right]$$

To share a white pixel, the dealer randomly chooses one of the matrices $C_{0,}$ and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the black and white colors of the three sub pixels in each one of the three transparencies. Decryption process is done by stacking three shares. If the original pixel is white, the sub pixels of recovered image are one black and two white (grey level). If the original pixel is black, the sub pixels of recovered image are all black.

3.2. 2-out-of-3 Secret Sharing Scheme using Bit-level Decomposition

Assume a digital $N_1 \times N_2$ input image (B-bit image) with a B-bit per pixel representation. For example, the 8-bit representation can describe 256 gray-scale levels. For this representation, each integer pixel value of input image can be expressed equivalently in a binary form using

$$I_{(i,j)} = I_{(i,j)} 2^7 + I^2_{(i,j)} 2^6 + I^3_{(i,j)} 2^5 + \ldots\ldots + I^7_{(i,j)} 2 + I^8_{(i,j)} \quad (1)$$

Where (i, j) denotes the spatial location and $I^b_{(i,j)}$ indicates the bit value at the bit levels b = 1, 2,...,8 with $I^1_{(i,j)}$ corresponding to the most significant bit (MSB). After achieving 8 bit binary planes, the 2-out-of-3 secret sharing scheme (Table 1) is utilized to generate the three binary shares S^b_1, S^b_2, S^b_3 using the reference pixel $r_{(i,j)} = I^b_{(i,j)}$. Assuming that $s'^b_{(u,v)} \in S^b_1$, $s''^b_{(u,v)} \in S^b_2$ and $s'''^b_{(u,v)} \in S^b_3$ for u = 1, 2,..., $3N_1$ and v = 1, 2,..., N_2, denote the pixels in three binary shares S^b_1, S^b_2 and S^b_3 respectively, the 8 bit share pixels $s'_{(u,v)} \in S_1$, $s''_{(u,v)} \in S_2$ and $s'''_{(u,v)} \in S_3$ are constituted by bit-level stacking as follows:

$$s'_{(u,v)} = s'_{(u,v)} 2^7 + s'^2_{(u,v)} 2^6 + s'^3_{(u,v)} 2^5 + \ldots\ldots + s'^7_{(u,v)} 2 + s'^8_{(u,v)} \quad (2)$$

$$s''_{(u,v)} = s''_{(u,v)} 2^7 + s''^2_{(u,v)} 2^6 + s''^3_{(u,v)} 2^5 + \ldots\ldots + s''^7_{(u,v)} 2 + s''^8_{(u,v)} \quad (3)$$

$$s'''_{(u,v)} = s'''_{(u,v)} 2^7 + s'''^2_{(u,v)} 2^6 + s'''^3_{(u,v)} 2^5 + \ldots\ldots + s'''^7_{(u,v)} 2 + s'''^8_{(u,v)} \quad (4)$$

Due to the encryption function and the random choice of sub pixels pattern from table (1) is applied, the original pixel $I_{(i,j)}$ and the integer valued share pixels: $s'_{(i,j)}, s'_{(2i,j)}, s'_{(3i,j)}$, $s''_{(i,j)}, s''_{(2i,j)}, s''_{(3i,j)}$ and $s'''_{(i,j)}, s'''_{(2i,j)}, s'''_{(3i,j)}$ can differ significantly [5].

As the decryption function used XOR operation, it can get the perfect reconstruction, a property unavailable in conventional 2-out-of-3 scheme.

4. Proposed Method

This system encrypt the image by using bit-level decomposition method and 2-out-of-3 secret sharing scheme. There are two parts in this system. They are encryption and decryption process.

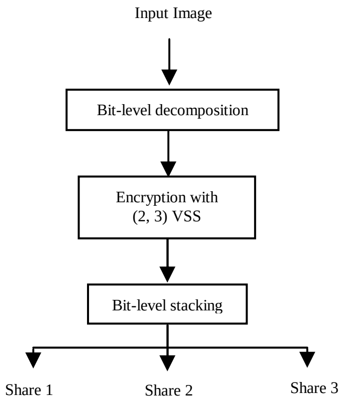


Figure 1. Encryption Process

The encryption process encodes the original image using three steps. Firstly, the input image (pictures and texts) is applied to the system. Every pixel in the input image is divided by the bit-level decomposition (equation 1). Secondly, each bit of 8-bit representation of the original pixel is encrypted by the use of 2-out-of-3 secret sharing scheme (Table 1) to generate three binary shares. Finally, binary sequence in every binary shares are stacked according to the bit levels by producing the share pixels differ from original pixel using equation 2, 3 and 4. Each share pixels are assigned to three shadow images, called shares are formed from the original image. Figure 1 describes the encryption process of the proposed system.

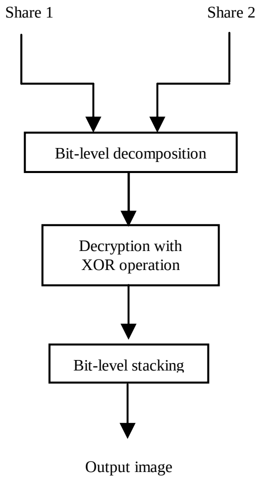


Figure 2(a). (2, 3) Decryption Process

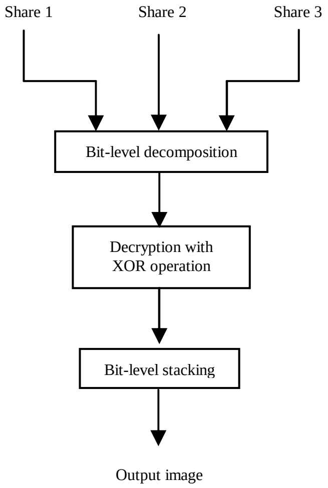
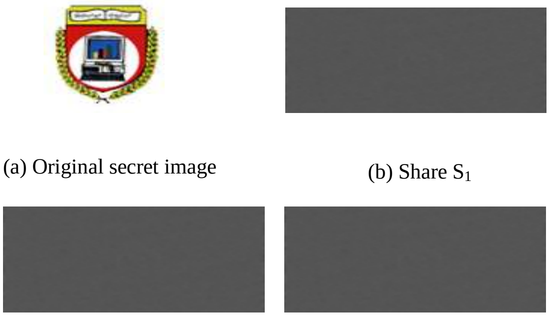


Figure 2(b). (3, 3) Decryption Process

The decryption process consists of three steps. First, any two or three users who received shares applied their shares to the bit-level decomposition process. Second, bit level representations of three shares are transformed by using XOR operation to form the recovered binary image. Finally, bit-levels of recovered binary image are stacked to produce the original secret image. In decryption, any two shares can be recovered the original image with free noise as shown in Figure 2(a). All of three shares can also be recovered the secret with faithful recovery as shown in Figure 2(b).

5. Experimental results

As the proposed secret sharing scheme operates directly on the bit planes of the input image, the proposed method differs significantly from conventional (2, 3) secret sharing scheme. Figure 3(a) is encrypted using proposed system. Three image shares are shown in Figure 3(b), 3(c), and 3(d). Figure 3(e), 3(f) and 3(g) show the recovered image with stacking two shares. Figure 3(h) displays the restored image by combining three shares.

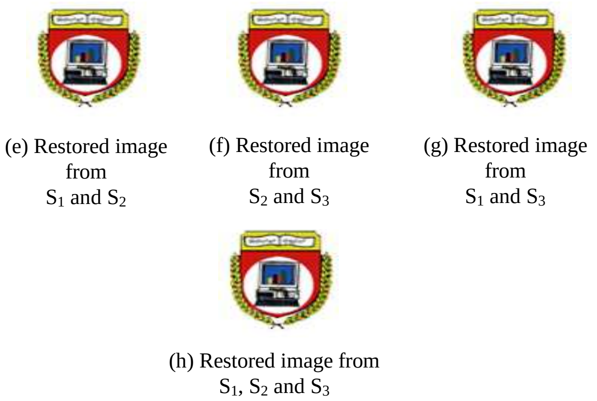


(a) Original secret image

(b) Share S_1

(c) Share S_2

(d) Share S_3



(e) Restored image from S_1 and S_2

(f) Restored image from S_2 and S_3

(g) Restored image from S_1 and S_3

(h) Restored image from S_1, S_2 and S_3

Figure 3. Encryption and decryption process of the proposed system

This paper is implemented using C# programming language and the execution of the developed tool on a personal computer equipped with an Intel® Core™ 2 Duo 2.00GHz CPU, 2G RAM, Windows XP operating system.

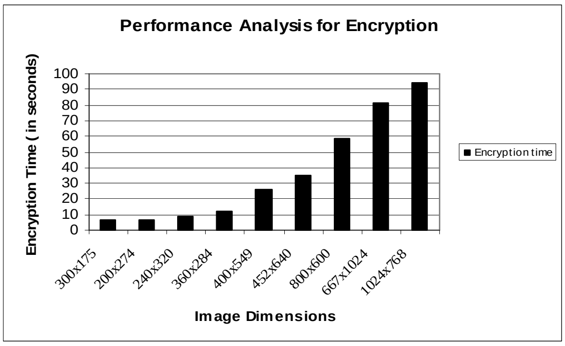


Figure 4. Performance Analysis of Encryption Time

This system is tested with various types of image such as jpg, bmp, png, tif and gif files. Figure (4) shows the performance analysis for encryption process of various types of image with different dimensions. Figure (5) represents the processing time for (2, 3) and (3, 3) decryption process.

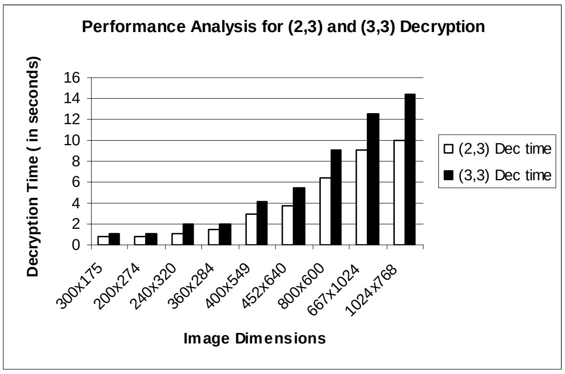


Figure 5. Performance Analysis of (2, 3) and (3, 3) Decryption Time

6. Conclusions

This system shows the method which encrypts the image operating at the bit-levels. The sensitive document (financial, medical, signature, images, military maps) can be encrypted into three shares and the secret information is revealed only when any two or three shares are stacked by computer. Although the size of each shared image is three times larger than that of the original secret image, the reconstructed image is the same size as the original image. Due to the decryption function uses Boolean XOR operation, decryption time is faster than the encryption time in this system. Gray-scale images and color images can be applied to this system and perfect reconstruction is achieved by performing decryption through simple logical operations.

References

[1] A. Sreekumar and Dr. S. Babu Sundar, “An Efficient Secret Sharing Scheme using POB-number system”, Department of Computer Applications Cochin University of Science and Technology, Kochi, Kerala, India

[2] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., “An overview of visual cryptography”, International Journal of Computational Intelligence Techniques, ISSN: 0976-0466 & E-ISSN: 0976-0474, Volume 1, Issue 1, 2010, PP-32-37

[3] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, “Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding”, Journal of Computer, vol.3, No. 12, December 2008.

[4] Mizuho NAKAJIMA, Yasushi YAMAGUCHI, “Extended Visual Cryptography For Natural Images”, Department of Graphics and Computer Sciences Graduate School of Arts and Sciences, University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan.

[5] Rastislav Lukac, Konstatinos N. Plataniotis, “Bit-level based secret sharing for image encryption”, Pattern Recognition 38 (2005) 767-772

[6] Sang-Su Lee, Jung-Chan Na, Sung-Won Sohn, C.Park, Dong-Hoan Seo, and Soo-Joong Kim, “Visual Cryptography Based on an Interferometric Encryption Technique”, ETRI Journal, Volume 24, Number 5, October 2002.

[7] Young-Chang Hou, “Visual Cryptography for color images”, Pattern Recognition 36 (2003) 1619-1629, Received 6 June 2002: accepted 26 August 2002.

[8] Zhongmin Wang and Gonzalo R. Arce, “ Halftone Visual Cryptography Through Error Diffusion”, Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, ICIP 2006.

[9] http://www.fianl-yearprojects.co.cc/

http://troubleshoot4free.com/fyp/