The Journal of Systems and Software 92 (2014) 107–114

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A secure Boolean-based multi-secret image sharing scheme

Chien-Chang Chen*, Wei-Jie Wu

Department of Computer Science and Information Engineering, Tamkang University, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 19 April 2013
Received in revised form 29 August 2013
Accepted 2 January 2014
Available online 8 January 2014

Keywords:
Multiple secret images
Boolean
XOR

ABSTRACT

An (n, n) multi-secret image sharing scheme shares n secret images among n shared images. In this type of schemes, n shared images can be used to recover all n secret images, but the loss of any shared image prevents the recovery of any secret image. Among existing image sharing techniques, Boolean-based secret schemes have good performance because they only require XOR calculation. This study presents a secure Boolean-based secret image sharing scheme that uses a random image generating function to generate a random image from secret images or shared images. The proposed function efficiently increases the sharing capacity on free of sharing the random image. The use of a bit shift subfunction in the random image generating function produces a random image to meet the random requirement. Experimental results show that the proposed scheme requires minimal CPU computation time to share or recover secret images. The time required to share n secret images is nearly the time as that required to recover n secret images. The bit shift subfunction takes more computation load than the XOR subfunction needs.

1. Introduction

The popularity of digital images has increased security problems in storing or transmitting vital images. Secret image sharing techniques preserve image securely by sharing secret image among shared images and then recovering the secret image from shared images.

Since Thien and Lin (2002) adopted the Shamir–Lagrange technique to share image secretly, researchers have proposed functional secret image sharing schemes based on sharing among host images (Lin et al., 2009; Guo et al., 2012; Wu et al., 2012; Ulutas et al., 2013), sharing with authentication (Chang et al., 2008; Yang et al., 2012), cheater identification (Chen and Suen, 2010), sharing by Boolean operations (Wang et al., 2007), progressive sharing (Fang, 2008; Huang et al., 2010; Dhara and Chanda, 2012), visual cryptography and secret image sharing (Lin and Lin, 2007; Yang and Ciou, 2010), and scalable sharing (Wang and Su, 2006).

Most of these secret image sharing schemes only share one secret image. However, when multiple secret images are secretly shared simultaneously, a more efficient method can improve performance and security. Chen and Chien (2008) used extra storage to reduce the load incurred by sharing multiple images. Lin et al. (2010) presented theoretical calculations on sharing two secret images among shared images. In this method, stacking or flipped stacking acquires the two reconstructed images. Chen et al. (2005) used a fixed-angle segmentation technique to create circular shared images, and stacked shared images at various angles to reveal different secret messages. Wu and Chang (2005) used a circular shared image with various rotation angles to share secrets. Hsu et al. (2007) presented a multi-secret sharing scheme to share secrets in outer and inner rings. Shyu et al. (2007) encoded circular secret images in two circular shared images such that secret images can be obtained individually by stacking the first share and rotating the second share at a different angle. Chen and Wu (2011) presented an (n, n) secret image sharing scheme that uses Boolean operations to encode $n-1$ secret images among n shared images.

This paper presents a secure Boolean-based (n, n) multi-secret image sharing scheme that shares n secret images among n shared images and recovers all n secret images using only these n shared images. The proposed scheme uses a random image generating function, which includes XOR and bit shift subfunctions to generate a random image from secret or shared images. Therefore, the random image no longer requires secret sharing, and one more secret image can be shared, increasing the sharing capacity. The proposed scheme uses the XOR result of odd secret and random images to preserve the randomness of the shared images. The proposed scheme improves upon the method proposed by Chen and Wu (2011) by increasing the sharing capacity and randomizing shared images. The theoretical analysis and experimental results of this study show the properties of the proposed scheme.

This paper is organized as follows. Section 2 presents a review of relevant literature regarding the Chen and Wu (2011)

* Corresponding author. Tel.: +886 2 26215656x3303.
E-mail address: ccchen34@mail.tku.edu.tw (C.-C. Chen).

0164-1212/$ – see front matter © 2014 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2014.01.001

method. Section 3 presents the proposed scheme. Sections 3.1 and 3.2 present the sharing and recovery procedures, respectively. Section 3.3 discusses the properties of the proposed random image generating function. Section 4 presents experimental results and a comparison of the proposed scheme with other methods. Section 5 provides a conclusion and suggestions for future research.

2. The scheme proposed by Chen and Wu

Chen and Wu (2011) presented a Boolean-based secret image sharing scheme to share $n-1$ secret images among n shared images. This section introduces the scheme proposed by Chen and Wu and provides a discussion of the special properties of their scheme. The algorithm of this secret image sharing scheme is described as follows:

1. Assume that G_i ($i=1,\ldots,n-1$) and R represent $n-1$ secret images and a random image, respectively.
2. Calculate $B_i=G_i \oplus R$ ($i=1,\ldots,n-1$).
3. Use Eq. (1) to calculate shared images S_i

$$\begin{aligned} S_1 &= B_1 \\ S_i &= B_{i-1} \oplus B_i \qquad \text{for } 2 \le i \le n-1 \\ S_n &= B_{n-1} \oplus G_1 \end{aligned} \tag{1}$$

The recovery algorithm is described as follows.

1. Perform the XOR calculation $S_1 \oplus S_2 \oplus \ldots \oplus S_n$ to acquire G_1 and $S_1 \oplus G_1$ to obtain the random image R.
2. Calculate $B_i \oplus R=G_i$ to obtain secret images G_i.

Chen and Wu used a random image R to randomize secret images G_i in Step 2 of their sharing algorithm. They also used Eq. (1) to fulfill the $(n-1, n)$ threshold criterion. Although their scheme can share $n-1$ multiple images among n shared images, some shortcomings can be improved.

First, a shared image S_i is acquired by $B_i \oplus B_{i-1}=(G_i \oplus R) \oplus (G_{i-1} \oplus R)=G_i \oplus G_{i-1}$, when $2 \le i \le n-1$. A scheme that uses only XOR calculations for two meaningful images cannot produce a randomized image. Fig. 1 shows the results of performing an XOR calculation on Lena and House test images. Therefore, performing XOR calculations on natural images with odd random images is needed to randomize the shared image.

Second, the scheme proposed by Chen and Wu has a sharing capacity of $(n-1)/n$. This sharing capacity is defined by dividing the number of secret images by the number of shared images. Because the random image R used to randomize meaningful secret images must be shared among shared images, only $n-1$ secret images can be shared with n shared image. The proposed scheme overcomes these two drawbacks to acquire a more secure Boolean-based secret image sharing scheme.

3. Proposed scheme

This section introduces the proposed (n, n) Boolean-based secret image sharing scheme. The proposed scheme generates the random image from secret images. This generation does not need to preserve the random image among shared images. Sections 3.1 and 3.2 show the proposed sharing and recovery procedures, respectively. Section 3.3 presents a discussion of properties of the proposed random image generating function.

3.1. Proposed sharing procedure

The proposed scheme uses a random image generating function F to generate the required random image. The term F consists of two subfunctions F_1 and F_2, as defined by $F=F_2(F_1)$. The term F_1 calculates the XOR result of images $G_i(i=1,\ldots,k)$. as shown in $F_1(G_1, G_2, \ldots, G_k)=G_1 \oplus G_2 \oplus \ldots \oplus G_k$, where $\oplus$ represents bitplane XOR calculation. The term $F_2(G)$ is defined by $bit\_shift(G(x, y), (x+y) \bmod 8)$, where bit_shift applies circular shift $((x+y) \bmod 8)$ bits to each pixel $G(x, y)$. The proposed sharing procedure is illustrated as follows:

1. Assume that $G_1, G_2, \ldots, G_n$ denote n secret images.
2. Use Eq. (2) to calculate a random image R

$$\begin{aligned} R &= F(G_1, \cdots, G_{k-1}, G_k) = F_2(F_1(G_1, \cdots, G_{k-1}, G_k)) \\ &= F_2(G_1 \oplus \cdots \oplus G_{k-1} \oplus G_k) \end{aligned} \tag{2}$$

$$\text{where} \quad k = 2 \cdot \left\lfloor \frac{n}{2} \right\rfloor .$$

3. Acquire the noised secret image N_i by $N_i=G_i \oplus R$, where $i=(1, 2, \ldots, n)$.
4. Use Eq. (3) to calculate each shared image S_i from all N_i for participant i

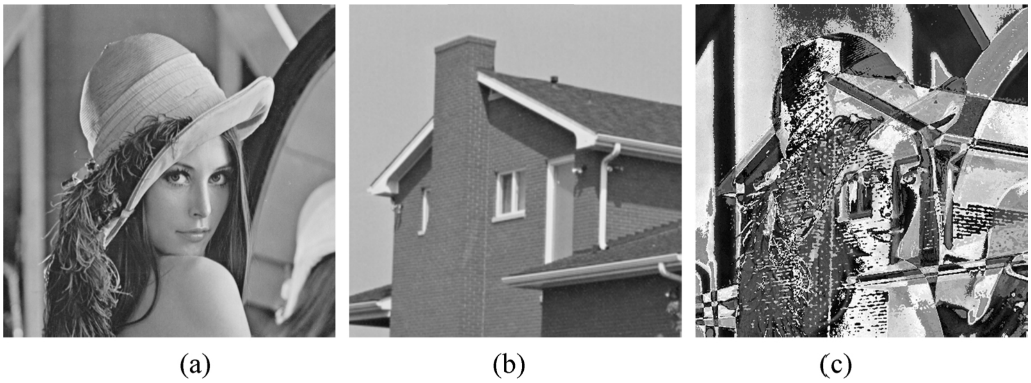

Fig. 1. XOR calculation results for (a) Lena image, (b) House image, and (c) XOR result image.