Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

Image sharing method for gray-level images

Wei-Kuei Chen*

Department of Computer Science and Information Engineering, Chien Hsin University of Science and Technology, Chungli, Taoyuan 320, Taiwan, ROC

ARTICLE INFO

Article history:
Received 16 June 2012
Received in revised form 9 September 2012
Accepted 27 September 2012
Available online 23 October 2012

Keywords:
Visual secret sharing
Hill cipher
Random grid
Pixel expansion
Distortion

ABSTRACT

In 1994, Naor and Shamir firstly proposed the concept of visual secret sharing. By using a codebook to encode a binary image into sharing images, nobody can obtain the original information from any one of the shared images unless superimposing all shared images. Although the above method can protect the security of the binary image, pixel expansion and lossy recovery are two unsolved problem. To improve the disadvantages mentioned above, a new image sharing method is proposed in this paper. The proposed method firstly use linear equations of Hill cipher to divide an image into several sub-images. Then the concept of the random grid is applied to the sub-images and to construct the shared images. Experimental result shows that the proposed scheme can effectively improve the above drawbacks.

1. Introduction

Due to the convenience of the Internet, digital information can be transmitted quickly among users' computers. Although the transmission speed has greatly improved, the security of the information is an unsolved problem. By using the leak of the Internet, many adventurers can smoothly intrude computers and steal the important information. Hence, how to effectively protect the security of the information has become an important issue nowadays.

Cryptography is an ancient technique that has been applied to protect the security of the secret message. By encrypting the secret message into disordered code, the encrypted message can be transmitted securely via the Internet and cannot be understood even though they are stolen. Furthermore, it is necessary to consume much time to decrypt the encrypted message. In recent years, information hiding technique has attracted many people's attention due to the feature of imperceptibility, security, and high capacity. By embedding the secret message into cover-media (such as images, videos, and texts), the secret message cannot be perceived by adventurers. Another feature of information hiding technique is reversibility. That is to say after the secret message is extracted, the original media can be recovered without distortion (Umamageswari et al., 2011). The above method is very suitable for some applications, such as the protection of medical, military, forensic, and art images.

A technique of simple and easy implementation was secret sharing method firstly proposed by Shamir (1979) and Blakley (1979). The basic concept is encoding a secret message into n shares. Less than k ($k \leq n$) shares cannot recover the original information unless more than or equal to k shares are obtained. If a director worries the security of a secret document, the director can encode the document into n parts and submit to different participant. Only when more than k parts are obtained, the original document can be recovered. As you can see, the method provides a good solution in many real-life applications (Wu et al., 2011).

Naor and Shamir firstly proposed a visual sharing method for protecting the security of digital images in 1994 (Lukac and Plataniotis, 2005). The basic concept is using a codebook to encode a binary image and the constructed shared images can be transmitted to different participant. We take a (2, 2) sharing method as an example. First, an image (shown as Fig. 1(a)) is encoded into two shared images by using a codebook (shown as Table 1). If a pixel is white, two blocks will be selected randomly from the left side of the codebook. On the contrary, if a pixel is black, two blocks will be selected randomly from right side of the codebook. Based on the rule, finally two shared images, as shown in Fig. 1(b) and (c), will be constructed and transmitted to different participant.

To obtain the original image, the two shared images are collected firstly. Then after superimposing two shared images, the original information can be retrieved and recognized directly by human eyes (as shown in Fig. 1(d)). As you can see, no one can obtain any message of the original image from any one of the shared images. Only if two shared images are superimposed, the information of the original image will appear. The disadvantages of the above method are the problem of pixel expansion and lossy recovery.

* Tel.: +886 3 4581196x7704.
E-mail addresses: wkchen@cyu.edu.tw, wkchen@uch.edu.tw

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.09.040

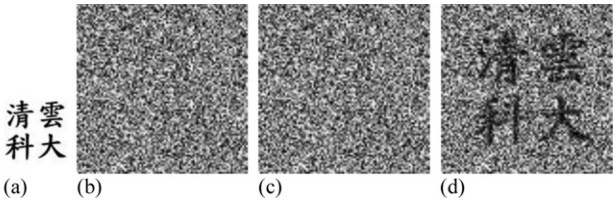

Fig. 1. (a) The secret image, (b) and (c) the shared images and (d) the reconstructed image.

In recent years, many improved methods have been proposed (Lukac and Plataniotis, 2005; Fang, 2008; Shyu, 2007; Kafri and Keren, 1987; Chen and Tsao, 2009; Ito et al., 1999; Yang, 2004; Cimato et al., 2006; Shyu, 2009; Chen and Tsao, 2011; Hsu and Hou, 2006; Thien and Lin, 2003). Lukac and Plataniotis (2005) proposed a bit-level based visual sharing method in 2005. A gray-level image is firstly decomposed into 8 bit-planes where every bit-plane can be regarded as a binary image. Then every binary image is encoded into two shared images respectively by the codebook as Table 1. Finally two gray-level sharing images will be obtained by combining the binary shared images.

To recover the original image, the two gray-level images are decomposed into 8 bit-planes respectively. Then every bit-plane is used to recover the bit-plane of the original image by the following rule.

$$\begin{array}{ll} \text{If} & \mathrm{s}^{\mathrm{b}}_{1(2i-1,2j-1)} = \mathrm{s}^{\mathrm{b}}_{2(2i-1,2j-1)} \quad \text{Then} \\ & \mathrm{o}^{\mathrm{b}}_{(i,j)} = 1 \\ \text{Else} & \\ & \mathrm{o}^{\mathrm{b}}_{(i,j)} = 0 \\ \text{End} & \end{array} \tag{1}$$

where $\mathrm{s}^{\mathrm{b}}_1$ and $\mathrm{s}^{\mathrm{b}}_2$ represent the bit-plane pixel of sharing image s_1 and s_2 respectively, o^{b} represents bit-plane pixel of the original image. Successively processing all pixels, finally the original image will be obtained by performing bit-plane reconstruction process. Although the method can recover the original image without distortion, the constructed sharing images have the problem of pixel expansion.

Fang (2008) proposed a progressive secret sharing method. The main concept of the method is encoding an expanded secret image and a cover image into n meaningful shared images. To recover the secret image, only if collecting any two shared images, rough information of the secret image can be recovered. When all shared images are superimposed, the secret image can be recovered without distortion. However, the problem of the pixel expansion is still unsolved.

Shyu (2007) proposed a random grid method based on Kafri and Keren algorithm (Kafri and Keren, 1987). Shyu's scheme can deal with binary, gray-level, and color secret images. Firstly a user randomly generates a random image consisting of 0 and 1. Then a random grid algorithm is applied to the random image and secret images. Finally two random shared images with the same size can be obtained. The method removes the problem of pixel expansion. However, the quality of the recovered image is necessary to be improved. Chen and Tsao (2009) also proposed two random grid methods based on Kafri and Keren algorithm. When more shared images are collected, the secret image can be clearly recovered. However, how to completely obtain the original image is an unsolved.

Table 1
The codebook of (2, 2) secret sharing method.

Pixel	□				■			
Shares 1	▄	▀	▚	▞	▄	▀	▚	▞
Shares 2	▄	▀	▚	▞	▀	▄	▞	▚
Superimposing results	▄	▀	▚	▞	█	█	█	█

The methods mentioned-above have the disadvantages of pixel expansion and image distortion. In real application, reducing the size of the shared images can provide fast transmission speed in network and save storage space in computer. Completely images without distortion can provide the accurate judgment for authenticators. In this paper, an image sharing method using Hill cipher and random grid is proposed. Firstly linear equations of Hill cipher are used to divide a secret image into several sub-images with the smaller size than the original secret image. Then the concept of random grid is applied to the sub-images and to construct the shared images. No one can obtain the original image unless the authorized person. Collecting all shared images can completely recover the original secret image without distortion.

The rest of the paper is organized as follows. Section 2 briefly introduces some related techniques. In Section 3, the proposed scheme is described in detail. The experimental results and discussions are shown in Section 4. Finally, the conclusions are drawn in Section 5.

2. Preliminary

Some of the related works are reviewed in this section. The Hill cipher is introduced in Section 2.1. The random grid is introduced in Section 2.2.

2.1. Hill cipher

Hill cipher was proposed by the mathematician Lester Hill in 1929 (Hill, 1929). The main concept of the algorithm is using m ciphertext letters to substitute m successive plaintext letters, where m belongs to positive integer. First, each letter is assigned a numerical value, such as $a=0$, $b=1$, . . ., $z=25$. Then m linear equations are used to determine m substituted letters (Acharya et al., 2009). Assume $m=2$, the ciphertext can be obtained by the following equations:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2) \bmod 26. \end{aligned} \tag{2}$$

The above equation can also be represented as Eqs. (3) and (4).

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} K_{11}K_{12} \\ K_{21}K_{22} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \bmod 26. \tag{3}$$

$$C = KP \mod 26, \quad \text{where } C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \quad K = \begin{bmatrix} K_{11}K_{12} \\ K_{21}K_{22} \end{bmatrix}, \quad P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \tag{4}$$

Furthermore C, P and K denote ciphertext, plaintext and encryption key respectively.

Although the inverse of the matrix K can be used to decrypt the ciphertext, it is not always existence. That is to say, if the matrix K is not invertible, the ciphertext cannot be decrypted. The plaintext can be obtained by the following equation:

$$P = K^{-1}C \mod 26. \tag{5}$$

Hill cipher can be used to encrypt gray-level images. For gray-level images, the modulus will be 256 (Acharya et al., 2009).