Available online at www.sciencedirect.com

SCIENCE DIRECT®

Pattern Recognition Letters 27 (2006) 551–555

Pattern Recognition Letters

www.elsevier.com/locate/patrec

Secret image sharing with smaller shadow images

Ran-Zan Wang *, Chin-Hui Su

Department of Computer and Communication Engineering, Ming Chuan University, 5 Der-Ming Rd., Kwei-Shan, Tau-yuan, 333 Taiwan, ROC

Received 9 August 2004; received in revised form 30 July 2005
Available online 26 October 2005

Communicated by Prof. G. Sanniti di Baja

Abstract

Secret image sharing is a technique for protecting images that involves the dispersion of the secret image into many shadow images. This endows the method with a higher tolerance against data corruption or loss than other image-protection mechanisms, such as encryption or steganography. In the method proposed in this study, the difference image of the secret image is encoded using Huffman coding scheme, and the arithmetic calculations of the sharing functions are evaluated in a power-of-two Galois Field GF(2^r). Experiment results show that each generated shadow image in the proposed method is about 40% smaller than that of the method in [Thien, C.C., Lin, J.C., 2002. Secret image sharing. Comput. Graphics 26 (1), 765–770], which improves its efficiency in storage, transmission, and data hiding.
© 2005 Elsevier B.V. All rights reserved.

Keywords: Secret sharing; Image sharing; Shadow image; Data hiding

1. Introduction

The continuing improvements in computer technologies and the rapid increase in Internet usage are responsible for the increasing popularity of network-based data transmission. In many applications, such as the communication of commercial affairs or military documents, important images must be kept secret. Many image-protection techniques, such as data encryption (Cheng and Xiaobo, 2000; Bourbakis and Dollas, 2003) and steganography (Marvel et al., 1999; Petitcolas et al., 1999), have been proposed to increase the security of secret images. However, one common defect of these techniques is their policy of centralized storage, in that an entire protected image is usually maintained in a single information carrier. If a cracker detects an abnormality in the information carrier in which the protected image resides, he or she may intercept it, attempt to decipher the secret inside, or simply ruin the entire information carrier (and once the information carrier is destroyed, the secret image is also lost forever). Secret image sharing is an image protection mechanism that does not suffer from these problems. It works by splitting the secret image into n incurious shadow images that are transmitted and stored separately. One can reconstruct the original image if at least a preset number r ($1 \leqslant r \leqslant n$) of these n shadow images are obtained; knowledge of less than r shadow images is insufficient for revealing the secret image.

The concept of secret sharing was introduced independently by Shamir (1979) and Blakley (1979). They proposed the so-called (r,n)-threshold scheme. The method involves dividing important data D into n pieces of shadow data. The important data D can be reconstructed if r of the n pieces of shadow data are obtained, but even complete knowledge of $r-1$ pieces of shadow data reveals no information about D. Many studies (Karnin et al., 1983; Stinson, 1994; Verheul and van Tiborg, 1997; Blundo and Santis, 1997) have investigated implementations of the (r,n)-threshold scheme, mainly concentrating on the communication of keys in cipher systems. Benaloh and Leichter (1989) proposed a more generalized sharing method by specifying several subgroups that had to be resolved to reveal the hidden secrets. Noar and Shamir (1995)

[*] Corresponding author. Tel.: +886 3 3507001x3406; fax: +886 3 4340700.
E-mail address: rzwang@mcu.edu.tw (R.-Z. Wang).

0167-8655/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.patrec.2005.09.021

proposed a new cryptographic technique called visual cryptography for sharing image-based secrets that was based on the human visual system. In visual cryptography, the secret message is distributed in many transparency shadows that consist of many noisy black dots. Superimposing the shadows that contain the secret message makes the message recognizable by human eyes. Recently, Thien and Lin (2002) proposed a secret image sharing method based on the (r, n)-threshold scheme that involved performing modular arithmetic operations in the prime Galois Field GF(P). Each generated shadow image is $1/r$ the size of the secret image in their lossy scheme, and is approximately $1/r$ in the lossless version.

This paper proposes a secret image sharing method that utilizes smaller shadow images. In the proposed method, n shadow images are derived from the secret image, and any r shadow images among the n shadow images can reveal the secret image, but less than r shadow images will not. As indicated by Thien and Lin (2002), the small size of each shadow image is advantageous in their subsequent use. The proposed method is introduced in Section 2, Section 3 presents the experimental results, and conclusions are drawn in Section 4.

2. Proposed method

Secret image sharing works by deriving n shadow images from the secret image using a sharing function, where each shadow image can be transmitted and stored separately. This method splits the secret image in several shadow images, which decreases the risks of data corruption and loss. However, the total size of the n shadow images is considerable, and hence the size of the generated shadow image should be carefully considered when designing an image sharing system.

The remainder of this section is divided as follows: the sharing method used to derive the n shadow images from the secret image is introduced in Section 2.1, the reveal method used to reconstruct the secret image from any r shadow images is presented in Section 2.2, and a modified sharing version that decreases the error propagation problem is stated in Section 2.3. Finally, the security properties of the proposed method are discussed in Section 2.4.

2.1. Sharing phase

Consider a t-bit secret image $\mathrm{SE} = \{\mathrm{se}_{ij}\}$, where $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. We want to derive n shadow images SH1, SH2, ..., SHn from SE, whereby the secret image can be reconstructed from any r of the n shadow images. First, a difference image $\mathrm{DIFF} = \{\mathrm{diff}_{ij}\}$ of SE is computed using

$$\mathrm{diff}_{ij} = \begin{cases} \mathrm{se}_{ij} & \text{if } i = 0 \text{ and } j = 0, \\ \mathrm{se}_{ij} - \mathrm{se}_{(i-1)j} & \text{if } i \neq 0 \text{ and } j = 0, \\ \mathrm{se}_{ij} - \mathrm{se}_{i(j-1)} & \text{otherwise.} \end{cases} \tag{1}$$

Note that diff_{ij} has values from $-2^t + 1$ to $2^t - 1$. To reduce the amount of data fed to the subsequently sharing process, the difference image is encoded using a Huffman coding scheme (Storer, 1988). Every t bits arriving from the Huffman coding output stream are grouped sequentially into a sharing coefficient, and every r generated sharing coefficients form a sharing section. Without loss of generality, for the jth sharing section, the polynomial sharing function of degree $r - 1$ is defined as

$$q_j(x) = (a_0 + a_1 x + \cdots + a_{r-1} x^{r-1}) \bmod 2^t, \tag{2}$$

where $a_0, a_1, \ldots, a_{r-1}$ are the r sharing coefficients in the sharing section. We take the shadow numbers $x = 1, 2, \ldots, n$ into the sharing function and evaluate the n output pixels $w_1, w_2, \ldots, w_n$, respectively:

$$w_1 = q_j(1), \ldots, w_i = q_j(i), \ldots, w_n = q_j(n). \tag{3}$$

Note that in the proposed method, all arithmetic operations in the sharing functions are evaluated in GF(2^t). The n output pixels $(w_1, w_2, \ldots, w_n)$ of this sharing section are then assigned to the jth pixel individually to n shadow images (SH1, SH2, ..., SHn). We summarize the proposed secret image sharing method in the following steps:

1. Apply the differencing function in Eq. (1) to the secret image SI and obtain the difference image DIFF.
2. Apply a Huffman coding scheme to encode the difference image, and obtain the output Huffman codes.
3. Sharing section generation:
   - 3.1. Sequentially take t bits from the output Huffman codes generated in Step 2 to form a sharing coefficient.
   - 3.2. Repeat Step 3.1 until r sharing coefficients are generated, which form a sharing section.
4. Use the r sharing coefficients of the sharing section generated in Step 3 to serve as the coefficients of Eq. (2). We generate the sharing function $q(x)$. For each shadow image with shadow numbers $i = 1, 2, \ldots, n$, evaluate $q(i)$ in GF(2^t) to generate n pixels for the n shadow images.
5. Repeat Steps 3 and 4 until all bits in the Huffman codes stream are processed.
6. Record the shadow number, the Huffman code table, and all of the generated pixels in the shadow image SHi.

Note that Thien and Lin (2002) use a key to permute the pixels before performing any sharing process, the main purpose of which is to hide the correlation between neighboring pixels. In their scheme, if the method uses the sharing process directly, the shadow images will adumbrate the shapes of the original image. Fig. 1 shows this phenomenon when applying the Thien and Lin scheme to share the secret image "Jet" with no permutation. In the method proposed in the present study, the original secret image is processed using the image differencing procedure and encoded using Huffman codes before sharing. This procedure hides the