Secret Image Sharing Safety

Wen-Pinn Fang
Department of Computer Science and Information Engineering, Yuanpei University
wpfang@mail.ypu.edu.tw

***Abstract*—Secret image sharing is an elegant method with the advantages of small share size and fault tolerance. In (n, r) sharing, one cannot obtain the secret image without collecting a sufficient number of shares. Conversely, the secret image can be recovered by collecting enough number of shares. Secret image sharing scheme has been shown to be a perfect sharing scheme, in which all pixel values are independent. The property of natural images can be exploited to reveal parts of secret is possible. This study demonstrates a simple example to show that, and proposed some suggestions to solve question.**
[1]

*Keywords:*secret image sharing; fault tolerance; security; nature image

I. INTRODUCTION

Secret image sharing (SIS) was originally presented by Thein and Lin [1] in 2002. The shares have small size, fault tolerance and security. The original idea, proposed by Shamir [2], is the extension of secret sharing scheme to image. It is presented below as mentioned in Ref [3]. Secret sharing is a reliable method for cryptographic key protection, and has many valuable properties. It is a perfect threshold scheme, in which the size of each share does not exceed the size of the secret, and the security does not rely on unproven mathematical assumptions. To maintain these advantages, Thien and Lin changed the values of polynomial coefficients a_j into a corresponding pixel value of a secret image. According to their design, the size of the shares is very small. They also proved that secure. The recovery image in [1] is lossy if the pixel value of the secret image exceeds 251. The recovery image's pixel will be 251 rather than the original values. To overcome the information loss problem, without extra overhead needed, Yang *et al.* [4] in 2007 presented a method that modifies the field to Galois Field in mod 2^8 to obtain lossless recovery of a secret image. There are a lot of relative reports as shown in [5-10]. For instance, Thein and Lin developed a friendly secret image sharing scheme [5] to let the shares meaningful. Fang and Lin[6] designed a special share that can be used to recover a group of secrets. Thein *et al.* [7] designed a sharing method that combines data hiding techniques. Chen and Lin[8] and Fang[9] presented progressive recovery approaches in the spatial and frequency domains. Wang and Su [10] improved secret image sharing efficiency in storage, transmission and data hiding.

This paper is supported by National Science Council under grant 96-2218-E-264-001.

This study discusses a frequently occurring situation regarding of non-random pixel values. There are some clues to recover the original secret image with shares in which the number is less than threshold. Based on this assumption, key protection is also needed in secret image sharing.

The rest of this paper is organized as follows. Section 2 discusses recovery for secret image sharing without enough shares. A discussion is given in Sec. 3.

The Shamir (t-w)-threshold scheme in $\boldsymbol{Z_p}$

Initialization Phase

1. D chooses w distinct, non-zero elements of Z_p, denoted $x_i, 1 \le i \le w$ which requires $p \ge w+1$. For $1 \le i \le w$, D gives the value x_i to P_i. The x_i values are public.

Share Distribution

2. Suppose that D wants to share a key $K \in Z_p$. D secretly chooses (independently at random) $t-1$ elements of Z_p, $a_1,\ldots,a_{t-1}$.
3. For $1 \le i \le w$, D calculates $y_i=a(x_i)$, where

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \mod p.$$

4. For $1 \le i \le w$, D gives the share y_i to P_i

II. RECOVERY FOR SECRET IMAGE SHARING WITHOUT A SUFFICIENT NUMBER OF SHARES

This section demonstrates the recovery of a secret image without a sufficient number of shares.

A. Secret Image Sharing

As shown in Ref[1], SIS generates n shares. No secrets can be obtained without collecting a sufficient number (less than threshold r) of shares. After obtaining a sufficient number of shares, one can recover the original secret image. Before describing the method, the notation is defined as

P: secret image, $W \times H$

n: number of shares

r: threshold

share size: $(W/r)\times H$

S_k : kth share, k=[1,n]

(i,j) : pixel value in the location(i,j)

Sharing phase:

As shown in Fig. 1(a)

Step 1. Define the value of threshold r

Step 2. Divide secret image into non-overlapping sections, with size of any section being r pixels

Step 3. Every section of shares can be generated by plugging in pixel value into a_i.

$$f(x)=(a_0+a_1x+\ldots+a_{r-1}x^{r-1}) \bmod 251 \quad (1)$$

Recovery phase:

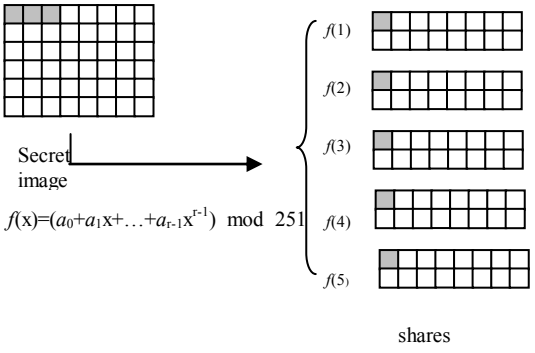
Step 1. Gather r shares

Step 2. Plug in the pixel value of shares in the equation (2)

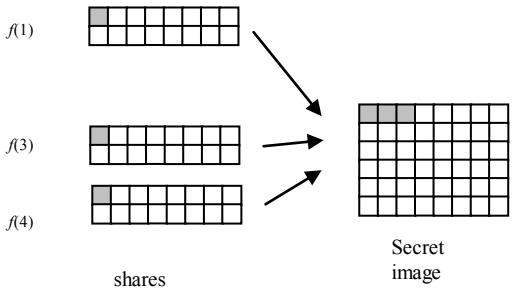
Step 3. Solve Eqs. (2) or (3), with the answers being the pixel value of secret image.

$$f(\mathrm{k})= S_{\mathrm{k}}(\mathrm{m}) \quad (2)$$

$$\begin{cases} (a_0+a_1+\ldots+a_{r-1})=f(1) \\ (a_0+2a_1+\ldots+2^{r-1}a_{r-1})=f(2) \\ \vdots \\ (a_0+(r-1)a_1+\ldots+(r-1)^{r-1}a_{r-1}) =f(r-1) \end{cases} \quad (3)$$



(a)



(b)

Fig.1 the flow of secret image sharing,(a) is the flow of sharing phase (b) is the flow of recovery phase.

B. Recovery without enough shares

Traditional secret image sharing involves collecting enough shares to recover the secret image. Equation 2 has infinite solutions if just with less than r equations, assuming that no relationship exists between neighboring pixels. , the secret image can be recovered if some equation can be created, or some relationship between the neighboring pixels can be identified.

C. Example for recovery without enough shares

If the threshold is 3, and two shares are available, and many neighboring pixels have the same color as pixels, it can be written down as $a_1=a_2$.Therefore, Eq. (4) is obtained.

$$\begin{cases} f(1)=a_0+a_1+a_2 \\ f(2)= a_0+2a_1+4a_2 \\ a_1=a_2 \end{cases} \quad (4)$$

After solving Eq. (4), the answer is given as Eq. (5).

$$\begin{cases} a_0=(3f(1)-f(2))/2 \\ a_1=(f(2)-f(1))/4 \\ a_2=a_1 \end{cases} \quad (5)$$

When the three coefficients are 22, 22, 18 shown in Fig.2, the pixel value of the first pixel in each share is

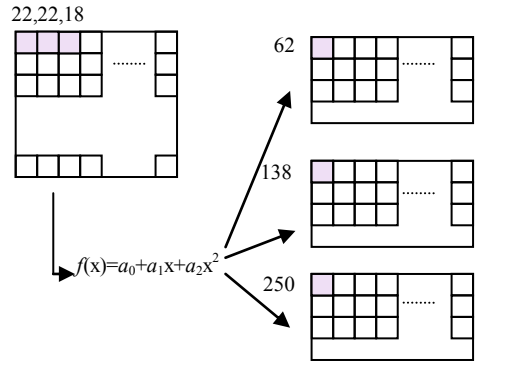
$$22+22\times1+18\times1^2=62$$
$$22+22\times2+18\times2^2=138$$
$$22+22\times3+18\times3^2=250$$

if only two of three shares are available, such as 62 and 250 as below.

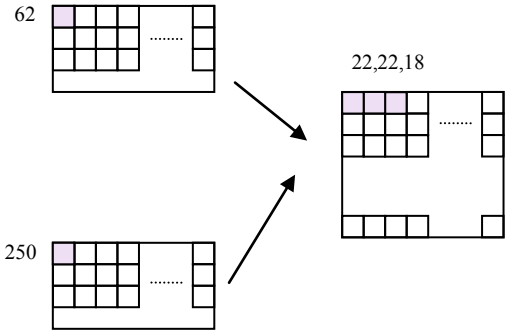
$$\begin{cases} 62=a_0+a_1+a_2 \\ 250=a_0+a_13+a_23^2 \\ a_2=a_1 \end{cases} \quad (6)$$

Solve equation (6), the answers will be a_0=22, a_1=22, a_2=18, and the secret is recovered.

Part of the secret image can be recovered, as indicated in Fig.3.

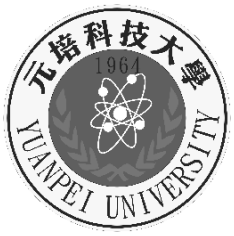


(a)

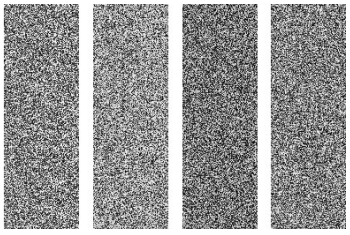


(b)

Fig. 2 An example of sharing and recovery



(a)



(b)

(c)

Fig.3 An example of recovery for secret image sharing without enough shares. In this example, n=4, r=3 (a) is the secret image; (b) shows the shares, and (c) is the recovered image with 2 shares

III. Discussion and Remarks

This study demonstrated the recovery of a secret image without enough shares. Compared with Fig.3(a) and (c), the most parts can be recognized. The PSNR between secret image and recovery image can be estimated after a little analysis. For example, if the size of secret image is 512×512. There are 70% pixels same color pairs. The average different between two not-same-value pixels are 128(that is the different are random). As shown in equation (7) and (8), the PSNR will be 38.162dB.

Although Eq. (4) is not suitable for the images with a lot of texture, such as Monkey, other equations can be designed, assuming that the image has many pixels with a linear relationship, such as $a_1=(a_0+a_2)/2$.

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j)-K(i,j)\right\|^2 \qquad (7)$$

$$PSNR=20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (8)$$

Section 2 reveals an important issue in secret image sharing. Key protection is required during transmission. Part of the secret can be recovered when the number of collected shares is below the threshold. Thein and Lin [1] stated that process permutation before generate the shares. Permutation before the sharing phase simply makes the shares noisy-like. If the permutation method is public, then it is not safe. Restated, the sharing engine could be modified to prevent the secret from being leaked when the number of collected shares is less than the threshold. Adding random numbers is a possible solution. It is similar to the report [2] about the secret sharing scheme. For instance, (3, 4) sharing, requires an order-2 polynomial equation in the traditional secret image sharing [2]. Equations 9 and 10 generate a order-3 equation, the equations are show in Equation 9 is the conventional secret image sharing engine, and equation 8 is a suggestion.

$$f(x)=(a_0+a_1x+a_2x^2) \bmod 251 \qquad (9)$$

$$f(x)=(a_0+a_1x+a_2x^2+Rx^3) \bmod 251 \quad (10)$$

$$f(x)=(a_0+a_1x+\ldots+a_{r-1}x^{r-1}+Rx^r) \bmod 251 \quad (11)$$

To generalize, transform Eq. 9 to Eq. 11

Here, R denotes a random number. The coefficient R, impedes guessing of the relationships among coefficients. Of course, the random number R creates a payload. If the safety in secret image sharing is assured, when transmitting the shares, the public key should be combined to solve the problem.

REFERENCES

[1]C.C. Thien and J.C. Lin, "Secret image sharing", *Computers and Graphics*, 26(1), 2002, pp. 765-770.

[2] A. Shamir, "How to share a secret", Communications of the Association for Computing Machinery, 1979, pp. 612-613.

[3] D.R. Stinson, Cryptography Theory and Pratice, p.327, CRC,U.S.A. ,1995.

[4] C.N. Yang, T.S. Chen, K. H. Yu and C.C. Wang, "Improvements of image sharing with steganography and authentication", *The Journal of System and Software*, 80,2007, pp.1070-1076.

[5] C.C. Thien and J.C. Lin, " An image-sharing method with user-friendly shadow images", *IEEE Transactions on Circuits and Systems for Video Technology*, 3(12), 2003, pp.1161-1169.

[6] W.P. Fang, J.C. Lin, "Universal Share for the Sharing of Multiple Images," *Journal of the Chinese Institute of Engineers* , Vol. 30, No. 4, 2007, 6, pp. 753-757.

[7] C.C. Thein, W.P. Fang and J.C. Lin, "Sharing Secret Images by Using Base-transform and Small-size Host images" *International Journal of Computer Science and Network Security*, 6, 2006, 7, pp. 219-225.

[8] S.K. Chen and J.C. Lin, "Fault-tolerant and progressive transmission of images", *Pattern Recognition*, 38(12), 2005, pp.2466-2471.

[9] W.P. Fang, "Multi-layer Progressive Secret Image Sharing," *7th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision*, Vouliagmeni Beach, Athen, Greece, 2007, 8.

[10] R.Z. Wang and C.H. Su , "Secret image sharing with smaller shadow images", *Pattern Recognition Letters* ,Vol. 27,(6), 2006, pp. 551-555.