Applied Mechanics and Materials Vols. 284-287 (2013) pp 3025-3029

doi:10.4028/www.scientific.net/AMM.284-287.3025

An Efficient Secret Image Sharing Scheme

Kuang-Shyr Wu[1,a], Tsung-Ming Lo[2,b]

[1]Department Computer Science and Information Engineering, Chien Hsin University of Science and Technology, Jhongli 320, Taiwan, ROC.

[2]Department of Computer and Communication, China University of Techlology, Hukou 303, Taiwan, ROC.

[a]keithwu@uch.edu.tw, [b]c36ltm@cute.edu.tw

Keywords: Secret Sharing, Image Sharing.

Abstract. This paper refers to a novel (*r*, *n*)-threshold secret image sharing scheme with low information overhead. The secret image is encoded into *n* noise-like shadow images in such a way that any *r* of the *n* shares can be used to reveal the secret, and no information about the secret can be revealed from any *r*–1 or fewer shares. The size of the shadow images is relatively small. Compared with the commonly used in the field of secret image sharing "Thien-Lin algorithm (2002)," the proposed scheme provides an alternative solution for light images. For the security analysis in the case of a 256×256 gray level secret image, if a hacker acquires any $r - 1$ shadow images, the hacker can construct only $r - 1$ equations, then the possibility of guessing the right solution is only 1/256. Hence, there are (256×256)/*r* polynomials, the possibility of obtaining the right image is only (1/256) (256 ×256)/*r*. The experimental results and theoretically analysis demonstrate that the proposed scheme performs well.

Introduction

The effective and secure protections of important message are primary concerns in commercial or military application [1]. Many techniques such as image hiding and watermarking were developed to increase the security of the secret.

To address the reliability issue, the approach of secret image sharing [1] is a glamorous approach for protecting sensitive information. The basic idea of secrete sharing is to transform an image into *n* shadow images that are transmitted and stored separately. The original image can be reconstructed only if the shadow images participated in the revealing process form a qualified set. To avoid the single-point-failure, the (*r*, *n*)-threshold image sharing schemes were therefore developed. In these schemes, the original image can be revealed if *r* or more of these *n* shadow images are obtained, but anyone who with complete knowledge of *r*–1 shares gets nothing about the original image.

In 1979, George Blakley [2] and Adi Shamir [3] proposed the original idea of secret sharing independently. The proposed (*r*, *n*)-threshold scheme encodes the input datat into *n* shares, which are then distributed amongst *n* recipients. As mentioned above, the input data can be reconstructed by anyone who obtains a predefined number *r*, where $2 \le r \le n$, of the shares.

Thien and Lin [1] proposed an outstanding secret image sharing (SIS) scheme based on the (*r*, *n*)-threshold. In their scheme, the size of generated shadow images is only 1/*r* of that of the original image, which is advantageous in later storage and transmission. Following the work of Thein and Lin, some image sharing schemes [4-6] have been proposed to reduce the size of the shadow images. Lin and Tsai [4] transformed the secret image to frequency domain, and shared the first ten coefficients of each block. Wang and Su [5] designed an SIS method applying the image difference and the algorithm of Huffman coding in the sharing process. Chang *et al.* [6] proposed a method for color images sharing with smaller shadow images.

To achieve higher flexibility in various applications, many improved image sharing schemes have been explored. Lin and Tsai [7] incorporated digital watermarking technique with the image sharing technique to have additional capabilities of steganography and authentication. Thien and Lin [8]

developed a method to make the shadow images look like portraits. Chen and Lin [9] applied the sharing concept to build a fault-tolerant progressive image transmission approach. Bai [10] classified the sharing schemes into two categories, the one called Perfect Secret Sharing (PSS) remains the same requirement as the original idea [1,3], and the other called Ramp Secrete Sharing (RSS) has the property that the exposed information is proportional to the size of the unqualified group. Bai [10] also proposed an image secret sharing scheme by using Matrix projection and Shamir's method. For the RSS, recently, Wang *et al*. [11] designed an incrementing Visual Cryptography (VC) scheme using random grids.

Among the secret sharing schemes, Thein-Lin scheme [1] remains the first choice due to its simplicity. Especially for the embedded systems and hand-held devices, many operations proposed by other researchers such as Galois Field GF(2^m) and inverse Matrices operations might not be visible or need extra computation power. Those complicated operations would increase the power consumption or chip area.

The rest of the paper is organized as follows. Section 2 reviews Shamir's and Thien-Lin's schemes. The proposed image sharing method is introduced in Section 3, and experimental results are shown in Section 4. Finally, conclusions are summarized in Section 5.

Review

The Shamir (*r*, *n*) Secret Image Sharing Scheme. Shamir [3] developed an (*r*, *n*)-threshold based secret sharing scheme for $2 \le r \le n$, n is the number of shadow images. The secret can be reconstructed by obtaining the predefined number r of n shares. The scheme is to construct a polynomial function as

$$f(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1}) \bmod p, \tag{1}$$

where p is a prime number, a_0 is the secret data and the remaining coefficients $a_1, a_2, \ldots, a_{r-1}$ are randomly chosen (known values) from the integer range $[0 \,..\, p-1]$.
For each secret data, a secret share is a pair of (x_i, y_i) where

$$y_i = f(x_i),\ 1 \le i \le n, \text{ and } 0 < x_1 < x_2 < \ldots < x_n < p. \tag{2}$$

According to Eq. 1 and Eq. 2, if we acquire any r or more pairs of the n shares, then at least r equations $y_i = f(x_i)$ can be set up, the secret data a_0 is therefore resolved.
On the other hand, the secret data a_0 can also be easily obtained by using Lagrange's interpolation [3].

The Thien-Lin (*r*, *n*) Secret Image Sharing Scheme. In 2002, Thien and Lin [1] extended Shamir's idea and proposed an SIS scheme based on the (*r*, *n*)-threshold scheme in which each generated shadow image is $1/r$ the size of the secret image. In their method, the arithmetic operations are evaluated in the prime Galois Field GF(251). As a result, a preprocessing to truncate the pixel values larger than 250 is needed. They also applied a permutation step on the original image before performing sharing process to hide the correlation among neighboring pixels.
Consider a secret image O, comprising m pixels, to encode O to n shadow images $S_1, S_2, S_3, \ldots, S_n$, the sharing steps of the Thein-Lin (*r*, *n*) secret image sharing scheme, where $2 \le r \le n$, are summarized below.
Step 1. Truncate the pixel values in O greater than 250 (251 to 255) to 250, O' denotes the image after truncation.
Step 2. Generate a permutation sequence with a secret key to permute the pixels of O', the permutated image is expressed as Q.
Step 3. Set the current processing section number j to 1.
Step 4. Sequentially take r non-processed pixels, say $a_0, a_1, a_2, \ldots, a_{r-1}$, of Q to form a section j, and create a polynomial of degree $r-1$ as following:

$$f_j(x)=(a_0+ a_1x+ a_2x^2+...+ a_{r-1}x^{r-1}) \bmod 251. \quad (3)$$

Step 5. Generate the n pixels

$$f_j(1), f_j(2), f_j(3),\ldots, f_j(n), \quad (4)$$

and sequentially assign to the n shadow images $S_1, S_2, S_3,\ldots, S_n$.
Step 6. Increase j by 1.
Step 7. Repeat Steps 4 to 6 until all pixels of Q are processed.

Note that, this method utilizes all the coefficients of Eq. 3 to share the secret pixels so that the size of the shadow images can be $1/r$. Also note that, the process mentioned above is a lossy image sharing scheme, there is no prediction to completely get the original image O back although the visual quality is excellent.
For the sharing phase of Thien-Lin (r, n) SIS scheme, without loss of generality, we assume the r shares are $S_1, S_2, S_3,\ldots, S_r$, the following steps can be used to reveal the secret image O' using any r ($2 \le r \le n$) of the shadow images.
Step 1. Set the current processing section number j to 1.
Step 2. Take one non-processed pixel from each of the r shadow images.
Step 3. Use these r pixels, *i.e.* $f_j(1), f_j(2),\ldots, f_j(r)$, and Lagrange's interpolation to solve the coefficients $a_0, a_1, a_2,\ldots, a_{r-1}$ in Eq. 3. They are the corresponding r pixel values of the *j-th* section in Q.
Step 4. Increase j by 1.
Step 5. Repeat Steps 2 to 4 until all pixels of the shadow images $S_1, S_2, S_3, \ldots, S_r$ are processed.
Step 6. Apply the inverse-permutation operation to Q to recover the secret image to O'.

Thien and Lin also provided an elegant lossless version for SIS [1], this part is omitted due to the paper length limitation.

The Proposed Method

In this study, the proposed method is introduced by changing the prime number 251 of Thein-Lin's method to 257. It seems impossible to store a number great than 255 into a gray level image, but indeed, it works correctly when the values of $f_j(x)$ in Eq. 3 are in the range [0..255], the only condition we need to deal with is the case of "256."
The proposed method has three benefits. Firstly, by using the prime number 257, the preprocessing of the truncation is no longer necessary, the computation time is saved. Indeed, the problem we are facing is the overflow, not the truncation any more. Secondly, a simply and fast encryption using table lookup technique is applied to replace the permutation process, this technique can accelerate the preprocessing time more.
Thirdly, the only drawback of the Thien-Lin's method is that the light images might not be applicable because of the truncation process. Our proposed method can overcome this drawback.
Technically speaking, the major difference between the proposed method and Thein-Lins' is that we use prime number 257 instead of 251, but many details are crucial.
To encode an image O to n shadow images, $S_1, S_2, S_3,\ldots, S_n$, the sharing steps of the proposed method are summarized below.
Step 1. Take the XOR operation to a pre-defined random table R and O. R is generated by a pseudo random number generator in advance. Q denotes the randomized image.
Step 2. Set the current processing section number j to 1.
Step 3. Sequentially take r non-processed pixels, say $a_0, a_1, a_2,\ldots, a_{r-1}$, of Q to form a sharing section j. Without loss of generality, let the current processing section be the *j-th* section of the image, and create a polynomial of degree r–1 as following:

$$f_j(x)=(a_0+ a_1x+ a_2x^2+...+ a_{r-1}x^{r-1}) \bmod 257. \quad (5)$$

Step 4. Generate the n shadow pixels as Eq. 4.
Step 5. If $f_j(x) = 256$, let the first non-zero pixel of $\{a_0, a_1, a_2 ,\ldots, a_{n-1}\}$ be decreased by 1, say $a_0 = a_0 - 1$, and goto Step 4.
Step 6. Sequentially assign pixels generated in Step 4 to the *j-th* pixel of the n shadow images.
Step 7. Increase j by 1.
Step 8. Repeat Steps 3 to 7 until all pixels of Q are processed.

In Step 5, it is needed to prove that there is no all-zero condition for $\{a_0, a_1, a_2 ,\ldots, a_{n-1}\}$ in the case of $f_j(x) = 256$, Otherwise, we might not find "the first non-zero pixel."
Assume under the case of $f_j(x) = 256$, we have $a_0 = a_1 = a_2 = a_{r-1} = 0$ which is the all-zero condition, then the polynomial Eq. 5 becomes $f_j(x) = 0 + 0x + 0x^2 + \ldots + 0x^{r-1}$ which makes $f_j(x) = 0$. As a result, $f_j(x) \neq 256$ is a contradiction to the assumption. Hence, the proof is done.
Similar to Thien-Lin's Scheme, the following steps can be used to reveal the secret image O.
Step 1. Set the current processing section j to 1.
Step 2. Take a non-processed pixel of position j from each of the r shadow images.
Step 3. Use these r pixels $f_j(1)$, $f_j(2)$, $f_j(3)$,…, $f_j(r)$ and Lagrange's interpolation to solve the coefficients a_0, a_1, a_2 ,…, a_{r-1} in Eq. 5. They are exactly the r pixel values of the *j-th* section in Q.
Step 4. Increase j by 1.
Step 5. Repeat Steps 2 to 4 until all pixels of the shadow images are processed.
Step 6. Apply the XOR operation to the predefined random image R and Q to get the secret image O'.

Experimental Results

The experimental results of the proposed method are prepared in this section. Fig. 1 shows the (2, 4)-threshold image sharing scheme. The 256×256 gray level secret image "Lena" is shown is Fig. 1, the randomized image is shown in Fig. 2, and the four shadow images are shown in Fig. 3. Note that, the size of each shadow image is only 1/2 of that of the secret image. Fig. 4 is the reconstructed image obtaining any two out of Fig. 3 in which the size of the reconstructed image is the same as the secret image.
For the security issue, the theoretical analysis is given as follows. In the experiment, we used a 256×256 gray level secret image. For this image, due to each section is formed of r pixels, there are $(256 \times 256)/r$ sections, *i.e.* $(256\times256)/r$ polynomials. To solve the r pixels (coefficients) of the polynomial, r equations should be acquired. If a hacker acquires any $r - 1$ shadow images, the hacker can construct only $r - 1$ equations, then the possibility of guessing the right solution is only 1/256. Hence, there are $(256\times256)/r$ polynomials, the possibility of obtaining the right image is only $(1/256)^{(256\times256)/r}$. This value is $(1/251)^{(256\times256)/r}$ in Thein-Lin's method [1].

Fig. 1. The secret image.

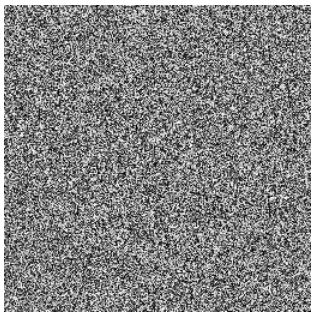

Fig. 2. The randomized image after XOR operation.

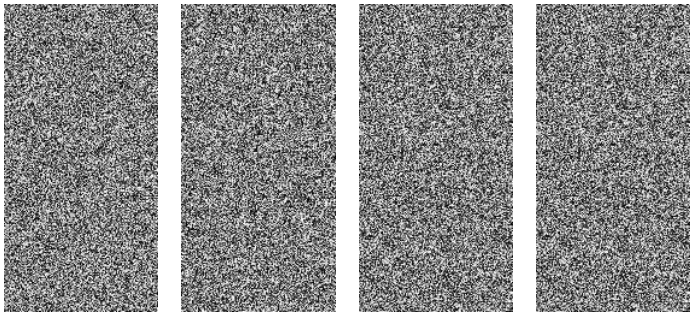

Fig. 3. The four noise-like shadow images of the secret image.

Fig. 4. The reconstructed image.

Conclusions

This work proposes a secret image sharing method. The concept is to use prime number 257 to replace 251 in Thein-Lin's method [1]. The proposed method has the properties: (i) a secret image can be reconstructed from any *r* shadow images nearly perfect or without any loss, (ii) the method reduces the size of shadow images for further storage or transmission, (iii) the proposed method can protect the secret image if any (*r*-1) or fewer shadow images are stolen, the possibility of guessing right is quite low, and (iv) this method can be applied to light images. The experimental results and theoretically analysis show that the proposed scheme performs well.

References

[1] C.C. Thien and J.C. Lin, "Secret image sharing," Computers and Graphics, Vol. 26, No. 5, pp. 765-770, (2002).

[2] G.R. Blakley, "Safeguarding cryptographic keys," AFIPS Conference Proceedings, Vol. 48, pp. 313-317, (1979).

[3] A. Shamir, "How to share a secret," Communications of the ACM, Vol. 22, No. 11, pp. 612-613, (1979).

[4] C.C. Lin and W.H. Tsai, "Secret image sharing with capability of share data reduction," Optical Engineering, Vol. 42, pp. 2340-2345, (2005).

[5] R.Z. Wang and C.H. Su, "Secret image sharing with smaller shadow images," Pattern Recognition Letters, Vol. 27, No. 6, pp. 551-555, (2006).

[6] C.C. Chang, C.C. Lin and Y.H. Chen, "A novel secret image sharing scheme in color images using small shadow images," Information Sciences, Vol. 178, pp. 2433-2447, (2008).

[7] C.C. Lin and W.H. Tsai, "Secret image sharing with steganography and authentication," Journal of Systems and Software, Vol. 73, No. 3, pp. 405-414, (2004).

[8] C.C. Thein and J.C. Lin, "An image sharing method with user-friendly shadow images," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 12 pp. 1161-1169, (2003).

[9] S.K. Chen and J.C. Lin, "Fault-Tolerant and Progressive Transmission of images," Pattern Recognition, Vol. 38, No. 12, pp. 2466-2471, (2005).

[10] L. Bai, "A Reliable (k,n) Image Secret Sharing Scheme with Low Information Overhead," International Journal of Computers and Applications, Vol. 32, No. 1, pp. 9-14, (2010).

[11] R.Z. Wang, Y.C. Lan, Y.K. Lee, S.Y. Huang, S.J. Shyu, T.L. Chia, "Incrementing visual cryptography using random grids," Optics Communications, Vol. 283, pp. 4242-4249, (2010).