EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

A secret image sharing scheme for light images

Kuang-Shyr Wu

Abstract

In this study, a new (*r*, *n*)-threshold secret image sharing scheme with low information overhead for images is provided, which has a low distortion rate, and is more applicable for light images. A secret image is encoded into *n* noise-like shadow images to satisfy the condition that any *r* of the *n* shares can be used to reveal the secret image, and no information on the secret can be revealed from any *r* – 1 or fewer shares. The size of the shadow images is relatively small. The experimental results show the effectiveness of the proposed scheme.

Keywords: Secret sharing, Image sharing

1. Introduction

Recently, digital-image sharing has played an important role because of the increasing requirements for image transmission. Effective and secure protection for important messages is a primary concern in commercial and military applications [1]. Numerous techniques, such as image hiding and watermarking, were developed to increase the security of the secret.

For the reliability issue, particularly for large-sized images, such as satellite or medical images, the secret image sharing (SIS) approaches are useful for protecting sensitive information [1]. 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 that participated in the revealing process form a qualified set. To avoid the single-point failure, for example, the encoded content is corrupted during transmission, the (*r*, *n*)-threshold image sharing schemes were therefore developed. In these developed schemes, the original image can be revealed if *r* or more of these *n* shadow images are obtained; however, users who with complete knowledge of *r* – 1 shares cannot obtain the original image.

Currently, numerous approaches have been developed for image sharing. Blakley [2] and Shamir [3] independently proposed original concepts of secret sharing in 1979. The proposed (*r*, *n*)-threshold scheme encodes the input data *D* into *n* shares, which are then distributed among *n* recipients. As previously mentioned, *D* can be reconstructed by anyone who obtains a predefined number *r*, where $2 \le r \le n$, of the images.

In 2002, Thien and Lin [1] proposed an elegant SIS scheme based on the (*r*, *n*)-threshold. In the scheme, the size of generated shadow images is only $1/r$ of that of the original image, which is advantageous in subsequent storage and transmission. Following the work of Thien and Lin, certain 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.

For the concern of flexibility in various applications, many improved image sharing schemes were 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. Lukac and Plataniotis [10] utilized the concept of bit-level decomposition to share color images. Bai [11] classified the sharing schemes into two categories, the first called perfect secret sharing remains the same requirement as the original idea [1], and the other called ramp secrete sharing (RSS) has the property that the exposed information is proportional to the size of

Correspondence: keithwu@uch.edu.tw
Department of Computer Science and Information Engineering, Chien Hsin University of Science and Technology, No. 229, Jianxing Rd, Zhongli City, Taoyuan County 32097, Taiwan

the unqualified group. Bai [11] also proposed an SIS scheme by using a combination of matrix projection and Shamir's method. For the RSS, recently, Wang et al. [12] designed an incrementing visual cryptography scheme using random grids; Chen and Tsao [13] investigated a threshold RG-based visual secret sharing scheme aiming at providing the wide-use version.

Although numerous secret sharing schemes have been developed, the Thien–Lin scheme [1] remains the first choice among various applications because of its simplicity and efficiency. In particular, for embedded systems and hand-held devices, numerous operations of SIS schemes proposed by other researchers, such as Galois Field GF(2^m) and inverse matrices, might not be visible or require extra computation power. These complicated operations would increase the power consumption or chip area for the chip design process.

In the Thien–Lin scheme, the input pixel values must be truncated into 0 to 251. The light pixel values greater than 251 of the secret image are lost. This drawback might not be suitable for light images. Therefore, the proposed method mainly focuses on the improvement of the Thien–Lin scheme.

The remainder of the article is organized as follows. Section 2 reviews the Shamir and Thien–Lin's schemes. The proposed SIS method is introduced in Section 3, and experimental results and theoretical analysis are shown in Section 4. Finally, conclusions are summarized in Section 5.

2. Review

Image sharing is a critical means in the field of digital image security and digital image hiding. The basic idea in image sharing is to divide secret data into pieces for distribution to different persons, and certain subsets of these people can recover the entire secret. In general, image sharing can be described as dividing a secret image into n sub images, which have a certain degree of viability, but do not contain each other's information. Through the application of an indeterminate equation, the gray values of images are divided in order to achieve image sharing and encryption. The secret image can be reconstructed through the complete knowledge of r sub images, where $r \le n$.

A simple and effective algorithm for image sharing based on above description is addressed in Section 2.1.

2.1. The Shamir (*r*, *n*) SIS 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

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

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 $[0 \ldots p-1]$.

For each secret data, a secret share is a pair of (x_i, y_i) where

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

According to Equations (1) and (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 held in hand, the secret data a_0 is therefore resolved.

On the other hand, the secret data a_0 can also easily be obtained by using Lagrange's interpolation [3].

2.2. The Thien–Lin (*r*, *n*) SIS scheme

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 2002. In their method, the arithmetic operations are evaluated in the prime Galois Field GF(251). Consequently, a preprocessing to truncate pixel values larger than 250 is necessary. They also applied a permutation step on the original image before performing a sharing process to hide the correlations 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 Thien–Lin (r, n) SIS 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, $a_0, a_1, a_2, \ldots, a_{r-1}$, of Q to form a section j, and create a polynomial of degree $r-1$ as follows:

$$f_j(x) = \left(a_0 + a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1}\right) \bmod 251. \tag{3}$$

Step 5. Generate n pixels:

$$f_j(1), f_j(2), f_j(3), \ldots, f_j(n), \tag{4}$$

and sequentially assign them 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 through 6 until all pixels of Q are processed.

This method uses all the coefficients of Equation (3) to share the secret pixels so that the size of the shadow images can be $1/r$. This process is a lossy SIS scheme, no prediction exists to completely recover the original image O although the visual quality is good.

For the sharing phase of the Thien–Lin (r, n)-SIS scheme, without loss of generality, we assume the r shares are $S_1, S_2, S_3,\ldots, S_r$, and 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, $f_j(1), f_j(2), f_j(3),\ldots, f_j(r)$, and Lagrange's interpolation to solve the coefficients $a_0, a_1, a_2,\ldots, a_{r-1}$ in Equation (3). They are the corresponding r pixel values of the jth section in Q.
Step 4. Increase j by 1.
Step 5. Repeat Steps 2 through 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 the permuted image Q to recover the secret image to O'.

3. The proposed method

For the SIS of light images, the Thien–Lin method might not be sufficient to conduct the light areas because of the truncation. In this study, the first step of the proposed method is to change the prime number 251 of Thien–Lin's method to 257, in which the remainders are in the range of [0. . .256].

Figure 1 The secret image (original image for sharing) Lena

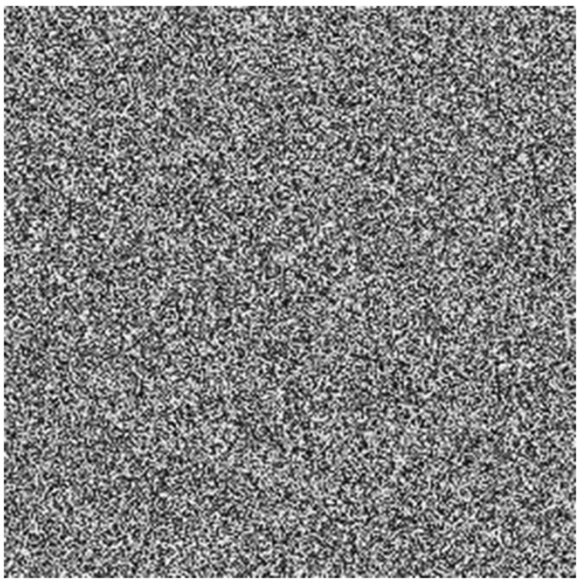

Figure 2 The secret image after permutation

The purpose of extension of the prime number is to protect the light image pixels from truncation errors, but it appears impossible to store a number greater than 255 into an 8-bit pixel. However, it works correctly when the pixel values of $f_j(x)$ in Equation (3) are in the range of [0. . .255], the only exception we are required to satisfy is "256."

The major difference between the proposed method and the Thien–Lin method is that we use prime number 257 instead of 251, this change makes the truncation error disappeared, but numerous details still remain crucial.

To encode an image O into n shadow images, $S_1, S_2, S_3,\ldots, S_n$, the sharing steps of the proposed method are summarized below.

Step 1. Generate a permutation sequence with a secret key to permute the pixels of O, Q depicts the permutated image.
Step 2. Set the current processing section number j to 1.
Step 3. Sequentially, take r not-processed yet pixels, $a_0, a_1, a_2,\ldots, a_{r-1}$, of Q to form a sharing section j. Without loss of generality, let the current processing section be the jth section of the image, and create a polynomial of degree $r - 1$ as follows:

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

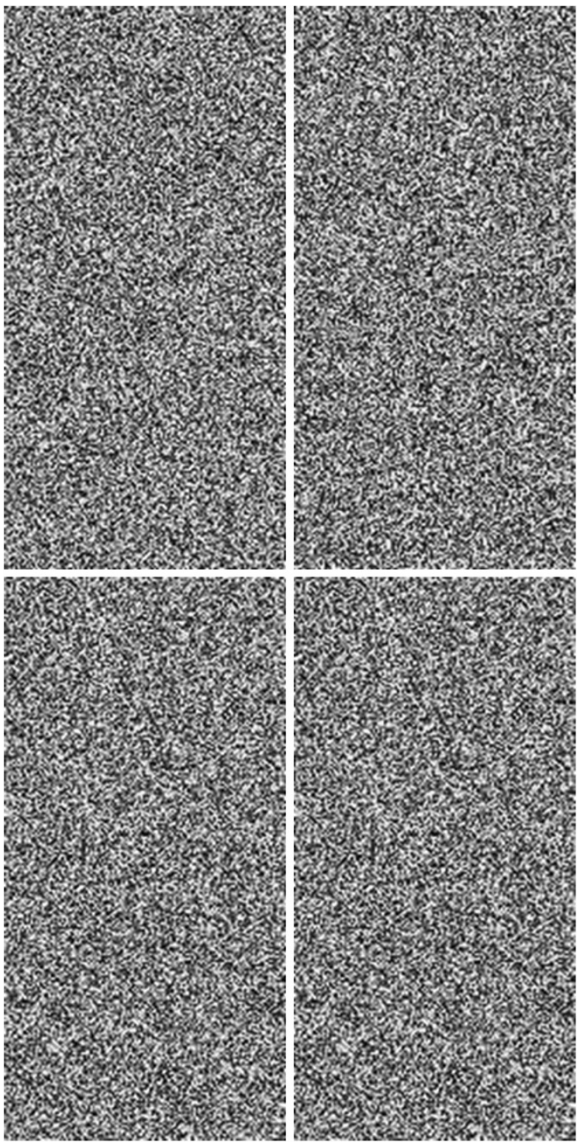

Figure 3 The four noise-like shadow images of the secret image

Step 4. Generate the n shadow pixels:

$$f_j(1), f_j(2), f_j(3), \ldots, f_j(n), \quad (6)$$

set $f_j(x)$ to zero if $f_j(x)$ is equal to 256.

Step 5. Assign $f_j(1), f_j(2), f_j(3), \ldots, f_j(n)$ in Equation (6) to the jth pixel of the n shadow images accordingly.

Step 6. Increase j by 1.

Step 7. Repeat Steps 3 through 6 until all pixels of Q are processed.

We set $f_j(x)$ to zero for the specific case of "256" in Step 4 to solve the overflow problem, but the normal pixel values of zero are also affected. If this case occurs, the sharing step is not lossless, and the decoding result will trend to be unacceptable. Therefore, we need to develop a decoding scheme to solve this problem.

The proposed decoding scheme uses a similarity calculation process of the surrounding pixels to avoid the distortion problem.

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 not-processed yet pixel of position j from each of the r shadow images.

Step 3. If any of the r pixels is equal to zero, record position j into a file, otherwise run Step 3.1.

Step 3.1 Use these r pixels $f_j(1), f_j(2), f_j(3), \ldots, f_j(r)$ and Lagrange's interpolation to solve the coefficients $a_0, a_1, a_2, \ldots, a_{r-1}$ in Equation (5). They are exactly the r pixel values of the jth section in Q.

Step 4. Increase j by 1.

Step 5. Repeat Steps 2 through 4 until all pixels of the shadow images are processed.

Step 6. Apply the inverse-permutation operation to the permuted image Q to get the secret image to Q'.

Step 7. For each j (recorded in Step 3), run Step 3.1 by different combinations of zero and 256 for the zero pixels of the shadow image (the other pixels remain the same values), then we have several candidate solution sets (the number of combinations) in hand. Calculate each pixel's squared Euclidean distances with its known neighboring pixels (at most eight) and sum them up for every solution set, the solution set with minimal distance is the solution we need for Section j.

Figure 4 The reconstructed image by using the proposed method

Store each pixel value of Section j in Q'. The new image O' is the reconstructed secret image.

The proposed method has three benefits. First, by using the prime number 257, the preprocessing of the truncation is no longer necessary, and computation time is saved. Second, the problem we are facing in our scheme is no longer the truncation but the overflow. Therefore, the distortion can be minimized by the use of correlation calculation of adjacent pixels.

Third, the only drawback of the Thien–Lin method is that the light images might not be good enough. Because the proposed method has no truncation process needed so that the light images are applicable to the proposed method.

4. Experiments

The experimental results of the proposed method are prepared in this section to show the (2, 4)-threshold SIS scheme. The 256 × 256 gray-level secret image "Lena" is shown in Figure 1. The permuted image is shown in Figure 2, and the four shadow images are shown in Figure 3. The size of each shadow image is only 1/2 of that of the secret image. Figure 4 is the reconstructed image obtaining any two out of four in Figure 3, in which the size of the reconstructed image is identical to the secret image.

For security, the following is a theoretical analysis. In this experiment, we used a 256 × 256 gray-level secret image. For this image, because each section is formed of r pixels, there are $(256 \times 256)/r$ sections, that is $(256 \times 256)/r$ polynomials. To solve the r pixels (coefficients) of the polynomial, r equations should be acquired. If a hacker acquires $r - 1$ shadow images, he can construct only $r - 1$ equations. The possibility of guessing the right solution is then only 1/256. Hence, if there are $(256 \times 256)/r$ polynomials, the possibility of obtaining the correct image is only $(1/256)^{(256\times256)/r}$. In the Thien–Lin method, the possibility is $(1/251)^{(256\times256)/r}$ [1].

5. Conclusions

This proposed method gives us an insight into SIS. The concept is to use prime number 257 to replace 251 in Thien–Lin's method [1]. The proposed method has the following properties: (i) a secret image can be reconstructed from any r shadow image nearly perfectly or without any loss; (ii) the method reduces the size of the 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, and the possibility of guessing right is low; and (iv) this method can be used on light images. The experimental results and theoretically analysis show that the proposed scheme performs well.

Competing interests
The author declares that he has no competing interests.

Received: 14 November 2012 Accepted: 21 February 2013
Published: 15 March 2013

References

1. CC Thien, JC Lin, Secret image sharing. Compt. Graph. **26**(5), 765–770 (2002)
2. GR Blakley, Safeguarding cryptographic keys, in Proceedings of AFIPS 1979 National Computer Conference, New Jersey. USA **48**, 313–317 (1979)
3. A Shamir, How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
4. CC Lin, WH Tsai, Secret image sharing with capability of share data reduction. Opt. Eng **42**, 2340–2345 (2005)
5. RZ Wang, CH Su, Secret image sharing with smaller shadow images. Pattern Recognit. Lett. **27**(6), 551–555 (2006)
6. CC Chang, CC Lin, YH Chen, A novel secret image sharing scheme in color images using small shadow images. Inf. Sci **178**, 2433–2447 (2008)
7. CC Lin, WH Tsai, Secret image sharing with steganography and authentication. J. Syst. Softw. **73**(3), 405–414 (2004)
8. CC Thien, JC Lin, An image sharing method with user-friendly shadow images. IEEE. Trans. Circuits Syst. Video Technol. **13**(12), 1161–1169 (2003)
9. SK Chen, JC Lin, Fault-tolerant and progressive transmission of images. Pattern Recognit. **38**(12), 2466–2471 (2005)
10. R Lukac, KN Plataniotis, Bit-level based secret sharing for image encryption. Pattern Recognit. **38**(5), 767–772 (2005)
11. L Bai, A reliable (k, n) image secret sharing scheme with low information overhead. Int. J. Compt. Appl. **32**(1), 9–14 (2010)
12. RZ Wang, YC Lan, YK Lee, SY Huang, SJ Shyu, TL Chia, Incrementing visual cryptography using random grids. Opt. Commun **283**, 4242–4249 (2010)
13. TH Chen, KH Tsao, Threshold visual secret sharing by random grids. J. Syst. Softw **84**, 1197–1208 (2011)

doi:10.1186/1687-6180-2013-49
Cite this article as: Wu: A secret image sharing scheme for light images. *EURASIP Journal on Advances in Signal Processing* 2013 **2013**:49.