An Efficient (t, n) Threshold Secret Image Sharing Scheme Based on Thien-Lin Secret Image Sharing

Amitava Nag

Central Institute of Technology, Kokrajhar, BDAT, Assam, India
Email: amitavanag.09@gmail.com
Arup Kumar Chattopadhyay
Institute of Engineering & Management, Kolkata, WB, India
Email: ardent.arup@gmail.com
Paramita Maitra
Institute of Engineering & Management, Kolkata, WB, India
Email: paramitasaha2002@gmail.com

***Abstract*—In a (t, n) threshold secret image sharing scheme (TSIS), a secret image is first encoded into n pieces, normally referred as shares or shadow images. Those share-images can be stored or transferred safely as individually a share-image cannot reveal any detail about the secret image. The receiver or user of the share-images referred as participants. If at least t $(\leq n)$ share-images are submitted by the participants, the secret image can be recomputed. One of the most popular secret image sharing schemes was proposed by Thien-Lin (2002). The authors had proposed two versions of the scheme. The first version of SIS by Thien-Lin is efficient, but lossy as the pixel values more than 250 (< 256) are truncated to 250. The second one is lossless, but it increases the size of the secret image during preprocessing. In this paper, we propose a secret image sharing scheme based on Thien-Lin scheme. We consider a little loss in the reconstructed image which is maximum one per pixel (the loss can be one to five in Thien-Lin scheme) and keep the size of the secret image same. Although buffer pixels may be added for the sake of programming, after reconstruction of the secret image the buffer pixels are easily identifiable and can be safely removed.**

***Index Terms*—secret image sharing, cryptography, lossy reconstruction, lossless reconstruction.**

I. Introduction

The secret sharing schemes are getting popular in secure storage and transfer of data files as they computationally very efficient than traditional cryptographic schemes. Blakley [1] and Shamir [2] (1979) first individually proposed (t, n) threshold secret sharing schemes. The Shamir's scheme was based on Lagrange Polynomial and Blakley's scheme was based on hyperplane geometry. In a (t, n) threshold secret sharing the secret S is encoded into n parts. The n parts are referred as shares or shadows and they must guarantee that they do not reveal any secret as an individual. If t or more $(\leq n)$ shares are available, then only the full secret can be computed back, otherwise nothing. Hence, t is called the threshold in these schemes. Another popular secret sharing scheme base on Chinese Reminder Theorem was proposed by Mignotte [3], which was further improved by Asmuth and Blooms [4].

The study of secret sharing of an image is called Visual Secret Sharing (VSS). Thien and Lin (2002) had proposed their first [5] (t, n) secret image sharing scheme based on the concept of Shamir's secret sharing scheme. Another efficient scheme with scalable shares was proposed by Lin and Wang [6] in 2010.

Secret image sharing schemes based on XOR operations are popular for their computational efficiencies. These schemes include single secret image sharing as well as multi-secret image sharing. The XOR based schemes are discussed in [7], [8], [9]. But most of these are (n, n) secret sharing. A hierarchical threshold secret sharing was proposed by Tassa [10] in 2004. In the hierarchical secret sharing schemes, the secret is shared among a group of participants that is partitioned into levels, set with different priorities in the reconstruction of the secret. Tassa's scheme is based on Birkhoff interpolation. In [11] the authors proposed a key based secret sharing where first the key is used to encrypt the secret. Then the key and encrypted secret both are encoded into n shares and distributed among participants.

In our proposed scheme, we perform some improvement on the Thien-Lin scheme such that the amount of the loss shall be minimized. In section 2, we have briefly reviewed the schemes proposed by Shamir and Thien-Lin. In section 3, we have discussed about different elements of secret image sharing schemes. We have proposed our scheme in section 4. And in section 5, we conclude.

II. Related Literature Review

We briefly review two fundamental schemes in this section: (1) (t, n) threshold secret sharing scheme (SSS) by Shamir and (2) (t, n) threshold secret image sharing scheme (SISS) by Thien-Lin. We consider the following symbols for both the schemes to be reviewed:

- The secrets is S.
- n shares or shadows to be generated are $sh_1, sh_2, \cdots, sh_n$.
- n participants are $\mathcal{P}_1, \mathcal{P}_2, \cdots, \mathcal{P}_n$.
- t is the threshold, which means out of n if t or more $(\leq n)$ shares are available then secret S can be recovered; otherwise not.

A. Review of Shamir (t, n) Secret Sharing Scheme [2]

In the share construction phase, the secret S is encoded into n shares or shadows. Then in recovery phase, if at least t $(t \leq n)$ shares are available the secret S is reconstructed.

1) Construction of the shares :

1) The scheme considers a polynomial of order $(t-1)$ as:

$$f(x) = (a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}) \ mod \ p.$$

where p is a prime, a_0 is the secret S, $a_1, a_2, \cdots, a_{t-1}$ are the coefficients randomly chosen from the range between 0 to $p-1$.

2) The n shares are generated as pairs $sh_i = (x_i, y_i)$ where $y_i = f(x_i)$, $(0 < i \leq n)$ and $(0 < x_i < p)$.
3) Transmit the shares to the participants $\mathcal{P}_i$, $(1 \leq i \leq n)$ such that each participant get exactly one share.

2) Reconstruction of the secret: Consider t shares are available with the combiner. Without loss of generality, we consider the available shares are $sh_1, sh_2, \cdots, sh_t$.

1) Using Lagrange interpolation, polynomial $f(x)$ can be regenerated as:

$$f(x) = \sum_{j=1}^{t} y_j \prod_{m=1, m \neq j}^{t} \frac{x - x_m}{x_j - x_m} \ mod \ p$$

The secret can be determined as $S = f(0)$.

B. Review of Thein-Lin (t, n) Secret Image Sharing Scheme [5]

Thein-Lin extended the Shamir's SS scheme for images. So in Thein-Lin (t, n) secret image sharing scheme, the secret S is essentially an image. In this method all the arithmetic operations are over $GF(251)$. So, the secret image need to preprocessed such that the pixel values more than 250 are truncated. In addition, a *transposition cipher* is applied to the secret image to break the strong correlation between the neighbouring pixels.

1) Construction of share images:

1) The secret image S is sequentially divided into several sections, such that each section is having exactly t pixels.
2) For each section j, we define a polynomial of degree $(t-1)$

$$f_j(x) = (a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}) \ mod \ 251$$

where $a_0, a_1, \cdots, a_{t-1}$ are pixel values belongs to section j.

3) Then, evaluate $f_j(1), f_j(2), \cdots, f_j(n)$ as share-pixels.
4) The n output pixels (the share-pixels of section j) are sequentially added to n share images.
5) The process repeated for all the sections.
6) Finally, it generates the share-images each of which is $\frac{1}{t}$ of the secret image S.

As each t pixels contribute only one pixel to a share-image, the share-image size is $\frac{1}{t}$ of the secret image.

2) Reconstruction of secret image: The following steps will regenerate the secret image from any t share-images. Without loss of generality, we consider the available share-images are: $SI_1, SI_2, \cdots, SI_t$.

1) Initialize the section number $j = 1$.
2) Take the first unprocessed pixel from all t share-images.
3) Use these t pixel values: $f_j(1), f_j(2), \cdots, f_j(t)$ and apply Lagranges interpolation to solve the coefficients $a_0, a_1, a_2, \cdots, a_{t-1}$ of polynomial f_j. The coefficients are the t pixel values of section j of the recovered image.

4) Increment j and repeat the process for section j.
5) Now, apply the inverse permutation cipher to recover the secret image.

III. Entities of (t, n)-threshold Secret Image Sharing Scheme

3) Secret: In Secret Image Sharing Schemes (SISS), the secret SI is the secret image file which must be secured from the adversaries (the unauthorized users or groups).

4) Shares or Shadows: The secret image SI will be encoded into n pieces called shares or shadows. Knowledge of any t or more shares $(\leq n)$ reveals the secret in full. With any less than t shares no part of the secret can be revealed.

5) Dealer: Dealer D is the owner of the secret image SI and responsible to generate the n shares and distributes them among n participants.

6) Participants: The participants $\mathcal{P}_1, \mathcal{P}_2, \cdots, \mathcal{P}_n$ are the users seeking the secret image. If t or more $(\leq n)$ participants submit their shares the secret can be revealed.

7) Combiner: The combiner C is the trusted entity responsible to decode the secret in presence of t or more $(\leq n)$ shares. In our proposed scheme only the combiner can reconstruct the secret.

IV. Proposed Scheme

A. Initial Encryption

Consider the grayscale secret image I_s $(w \times h)$. We compute a random matrix R $(w \times h)$ with the values ranging between 0 and 255. R will be assumed as private share or the secret key, which will be sent privately to the combiner C. We get encrypted image I_c as $I_c = I_s \oplus R$. The encryption is performed to break strong correlation between adjacent pixels of the source image. We implement our (t, n) threshold secret image sharing scheme as follows:

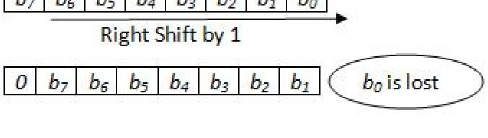
b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
Right Shift by 1
0 b_7 b_6 b_5 b_4 b_3 b_2 b_1
b_0 is lost

Fig. 1. Right shift (by 1) of image pixels causes loss of least significant bit.

B. Share Construction Phase

1) The pixel values are in range, from 0 to 255. But as all the arithmetic operations are performed over $GF(251)$. As a result the values greater than 250 will be truncated to 250. To limit this loss in the pixel values, we perform a one bit right shift for each pixel. That cause one bit (least significant bit) loss for each pixel. At the same time, the most significant bit of all the pixels becomes zero. This ensures every pixel value will be within the range from 0 to 127 as shown in figure 1. Let the per-processed image be I'_c.
2) From the image matrix I'_c, for each row R_i $(i = 1\ to\ h)$ construct m arrays where $m = \lceil \frac{w}{t} \rceil$, where t is the threshold and $t \leq \frac{w}{2}$, padding of zero may be added if required.
   So the arrays are:
$$\{A_{11}, A_{12}, \cdots, A_{1m}\}$$
$$\{A_{21}, A_{22}, \cdots, A_{2m}\}$$
$$\cdots$$
$$\{A_{h1}, A_{h2}, \cdots, A_{hm}\}$$
3) For each array A_{ij} (where $1 \leq i \leq h$ and $1 \leq j \leq m$) consists of exactly t pixels $\{p_0, p_1, ...p_{t-1}\}$. Now to construct the shares, we consider the polynomial as:
$$f_{ij}(x) = (p_0 + p_1 x + p_2 x^2 \cdots + p_{t-1} x^{t-1})\ mod\ 251$$
   Generate the share pixels as:
$$s_1 = f(1), s_2 = f(2), \cdots, s_n = f(n)$$
   For each A_{ij} where $(1 \leq i \leq h)$ and $(1 \leq j \leq m)$ the k^{th} share pixel is represented as S_{ijk}.
4) The share image SI_k where $(1 \leq k \leq n)$ generated as follows:
$$SI_k = \begin{bmatrix} s_{11k} & s_{12k} & \cdots & s_{1mk} \\ s_{21k} & s_{22k} & \cdots & s_{2mk} \\ \cdots & \cdots & \cdots & \cdots \\ s_{h1k} & s_{h2k} & \cdots & s_{hmk} \end{bmatrix}$$
5) Distribute the shares images $SI_1, SI_2, \cdots, SI_n$.

Reconstruction of Secret Image

We assume at least t shareimages are submitted to combiner C. Without loss of generosity we can assume the shares are $SI_1, SI_2, \cdots, SI_t$.

1) The available shares S_k (where $1 \leq k \leq t$) are in following form:

$$SI_k = \begin{bmatrix} s_{11k} & s_{12k} & \cdots & s_{1mk} \\ s_{21k} & s_{22k} & \cdots & s_{2mk} \\ \cdots & \cdots & \cdots & \cdots \\ s_{h1k} & s_{h2k} & \cdots & s_{hmk} \end{bmatrix}$$

2) Now extract one unused pixel from each of t share–images and arrange them (t pixels) as follows:

$$\{s_{111}, s_{112}, \cdots, s_{11t}\}$$
$$\{s_{121}, s_{122}, \cdots, s_{12t}\}$$
$$\cdots$$
$$\{s_{1m1}, s_{1m2}, \cdots, s_{1mt}\}$$
$$\cdots$$
$$\{s_{hm1}, s_{hm2}, \cdots, s_{hmt}\}$$

3) Now we use Lagrange interpolation for given t share pixels (or more $q \leq n$ pixels is q share–images are available) to reveal t real (the secret) pixels as follow:

$$p(x) = \sum_{k=0}^{n} y_k [\prod_{i=0, i \neq k}^{n} \frac{x - x_i}{x_k - x_i}] mod 251$$

4) Compute the arrays A_{ij} where $(1 \leq i \leq h)$ and $(1 \leq j \leq m)$ using the Lagranges interpolation as in following order:

$$\{s_{111}, s_{112}, \cdots, s_{11t}\} \implies A_{11},$$
$$\{s_{121}, s_{122}, \cdots, s_{12t}\} \implies A_{12},$$
$$\cdots$$
$$\{s_{1m1}, s_{1m2}, \cdots, s_{1mt}\} \implies A_{1m},$$
$$\cdots$$
$$\{s_{hm1}, s_{hm2}, \cdots, s_{hmt}\} \implies A_{hm}$$

5) Hence the combiner can rearrange the pixels to reconstruct I'_c. Perform left shift by one (as shown in figure 2) for each pixel of I'_c to recompute the encrypted image I_c.

C. Final Decryption

6) Decrypt it with private share R as $I_s = I_c \oplus R$. It guarantees only combiner can reconstruct the secret. I_s is the reconstructed secret image.

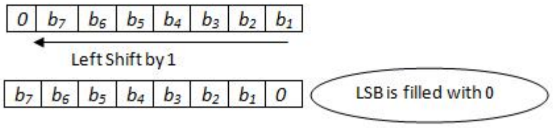

Fig. 2. Left shift (by 1) of image pixels.

V. Conclusion

Our proposed scheme is based on Thein-Lin secret image sharing scheme and we have reduced the loss in pixel values of the reconstructed secret image. In Thein-Lin scheme the maximum loss per pixel is five, whereas in our scheme the maximum loss per pixel is one. The loss of the value from the least significant bit difficult to observe manually and also from the histogram of the image. The secret image needs minimum preprocessing which includes one bit right shift and XOR operation which are computationally very efficient. The random matrix is also treated as a special (private) share-image, which will be secretly transferred to the combiner. This ensures only combiner can recompute the secret image.

References

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Managing Requirements Knowledge, International Workshop on (1979)*, NEW YORK, US, June 1979, pp. 313–317.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22(11), pp. 612–613, November 1979.

[3] M. Mignotte, "How to share a secret," in *Proc. of the 1982 conference on Cryptography*, Burg Feuerstein, Germany, June 1982, pp. 371–375.

[4] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29(2), pp. 208–210, 1983.

[5] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers and Graphics*, vol. 26(5), p. 765770, A 2002.

[6] Y.-Y. Lin and R.-Z. Wang, "Scalable secret image sharing with smaller shadow images," *IEEE Signal Processing Letters*, vol. 17(3), pp. 316–319, March 2010.

[7] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on boolean operations," *Pattern Recognition*, vol. 40(10), pp. 2776–2785, October 2007.

[8] T.-H. Chen and C.-S. Wu, "Efficient multi-secret image sharing based on boolean operations," *Signal Processing*, vol. 19(1), pp. 5–9, January 2011.

[9] C.-C. Chen and W.-J. Wu, "A secure boolean-based multi-secret image sharing scheme," *Journal of Systems and Software*, vol. 92, pp. 107–114, June 2014.

[10] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptography*, vol. 20(2), p. 237264, . 2004.

[11] P. K. Naskar, H. N. Khan, U. Roy, A. Chaudhuri, and A. Chaudhuri, "Shared cryptography with embedded session key for secret audio," *International Journal of Computer Applications*, vol. 26(8), pp. 90–97, July 2011.