Chinese Remainder Theorem-Based Secret Image Sharing for (k,n) Threshold

Xuehu Yan(✉), Yuliang Lu, Lintao Liu, Song Wan, Wanmeng Ding, and Hanlin Liu

Hefei Electronic Engineering Institute, Hefei 230037, China
publictiger@126.com

Abstract. In comparison with Shamir's original polynomial-based secret image sharing (SIS), Chinese remainder theorem-based SIS (CRTSIS) overall has the advantages of lossless recovery, low recovery computation complexity and no auxiliary encryption. Traditional CRTSIS methods generally suffer from no (k,n) threshold, lossy recovery, ignoring the image characteristics and auxiliary encryption. Based on the analysis of image characteristics and SIS, in this paper we propose a CRTSIS method for (k,n) threshold, through dividing the gray image pixel values into two intervals corresponding to two available mapping intervals. Our method realizes (k,n) threshold and lossless recovery for gray image without auxiliary encryption. Analysis and experiments are provided to indicate the effectiveness of the proposed method.

Keywords: Secret image sharing · Chinese remainder theorem · Lossless recovery · (k,n) threshold

1 Introduction

Secret image sharing (SIS) scheme for (k,n) threshold splits the secret image into n noise-like shadow images i.e., shares or shadows, which are then distributed to n participants. The secret can be reconstructed by k or more shadow images while less than k shadow images gain nothing about the secret. SIS may be applied in many scenarios, such as, access control, information hiding, authentication, watermarking, transmitting passwords, distributed storage and computing etc. [4,11,12]. For sharing gray image, there are Shamir's polynomial-based scheme [7], Chinese remainder theorem-based SIS (CRTSIS) [1,6,13] and so on.

Shamir's original polynomial-based SIS [7] for (k,n) threshold generates the secret image into the constant coefficient of a random $(k-1)$-degree polynomial to get n shadow images, which are then as well distributed to n participants. The secret image can be disclosed with high-resolution by means of Lagrange interpolation by any k or more shadow images. Inspired by Shamir's original scheme, utilizing all the k coefficients of the polynomial and the participant order to embed secret based on modular 251 and secret image encryption, Thien and Lin [9]

X. Sun et al. (Eds.): ICCCS 2017, Part II, LNCS 10603, pp. 433–440, 2017.
https://doi.org/10.1007/978-3-319-68542-7_36

2 Preliminaries

In this section, we straightforward some preliminaries for our work. For (k, n) threshold SIS, the original secret image S is encrypted among n shadow images $SC_1, SC_2, \cdots SC_n$, and the decrypted secret image S' is reconstructed from t $(k \leq t \leq n, t \in \mathrm{Z}^+)$ shadow images.

2.1 Chinese Remainder Theorem (CRT)

CRT has a long history, which can be traced back to the time of Han Xin. It aims to solve a set of linear congruence equations. A set of integers $m_i (i = 1, 2, \cdots, k)$ is chosen subject to $\gcd(m_i, m_j) = 1, i \neq j$.

Then there exists only one solution

$y \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) \pmod{M}$, $y \in [0, M-1])$ for the following linear congruence equations

$$\begin{aligned} y &\equiv a_1 \pmod{m_1} \\ y &\equiv a_2 \pmod{m_2} \\ &\cdots \\ y &\equiv a_{k-1} \pmod{m_{k-1}} \\ y &\equiv a_k \pmod{m_k} \end{aligned} \tag{1}$$

where $M = \prod_{i=1}^{k} m_i$, $M_i = {}^{M}\!/_{m_i}$ and $M_i M_i^{-1} \equiv 1 \pmod{m_i}$.

$\gcd(m_i, m_j) = 1, i \neq j$ results in that every equation in Eq. (1) will not be eliminated by other equations.

We remark that in $[0, M-1]$ there exists exactly one solution. If only the first $k-1$ equations in Eq. (1) are collected, we can obtain only one solution satisfying the first $k-1$ equations in $[0, \prod_{i=1}^{k-1} m_i - 1]$, denoted as y_0. While in $[0, M-1]$, $y_0 + b \prod_{i=1}^{k-1} m_i$ for $b = 1, 2, \cdots, m_i - 1$ are also the solutions for the first $k-1$ equations in Eq. (1). Thus, there are another $m_i - 1$ solutions in $[\prod_{i=1}^{k-1} m_i - 1, M-1]$, other than only one, which will be utilized in the proposed scheme to possess (k, n) threshold.

2.2 The Feature Analysis of Image

Digital image differs from pure electronic data. The image is composed of pixels, and there exists some correlations between pixels, such as structure, texture, edge and other related information. Thus, SIS should scramble not only the pixel values but also the correlations between adjacent pixels.

The pixel value of the gray image is in $[0, 255]$, which should be considered in the SIS design, such as, the secret pixel value should be in the range as well as $m_i \leq 256$.

3 The Proposed CRTSIS Method for (k, n) Threshold

We present the proposed CRTSIS method for (k, n) threshold based on the original secret image S resulting in n output shadow images $SC_1, SC_2, \cdots SC_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$. Our generation Steps are described in Algorithm 1. And the recovery Steps are presented in Algorithm 2.

```
Algorithm 1. The proposed SIS CRTSIS method for $(k, n)$ threshold
Input: The original secret image $S$ with size of $H \times W$
Output: $n$ shadow images $SC_1, SC_2, \cdots SC_n$ and corresponding privacy modular integers $m_1, m_2, \cdots m_n$
Step 1: Choose a set of integers $\{128 \leq p < m_1 < m_2 \cdots < m_n \leq 255\}$ subject to
    1. $\gcd(m_i, m_j) = 1, i \neq j$.
    2. $\gcd(m_i, p) = 1$ for $i = 1, 2, \cdots, n$.
    3. $M > pN$
    where $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$ and $p$ is public among all the participants
Step 2: Compute $T = \left[ \frac{\left\lfloor \frac{M}{p} - 1 \right\rfloor - \left\lceil \frac{N}{p} \right\rceil}{2} + \left\lceil \frac{N}{p} \right\rceil \right]$ and $T$ is public among all the participants as well. For each position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 3–4
Step 3: Let $x = S(h, w)$
    If $0 \leq x < p$, pick up a random integer $A$ in $\left[T + 1, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ and let $y = x + Ap$
    Else pick up a random integer $A$ in $\left[\left\lceil \frac{N}{p} \right\rceil, T\right)$ and let $y = x - p + Ap$.
Step 4: Compute $a_i \equiv y \pmod{m_i}$ and let $SC_i(h, w) = a_i$
Step 5: Output $n$ shadow images $SC_1, SC_2, \cdots SC_n$ and their corresponding privacy modular integers $m_1, m_2, \cdots m_n$
```

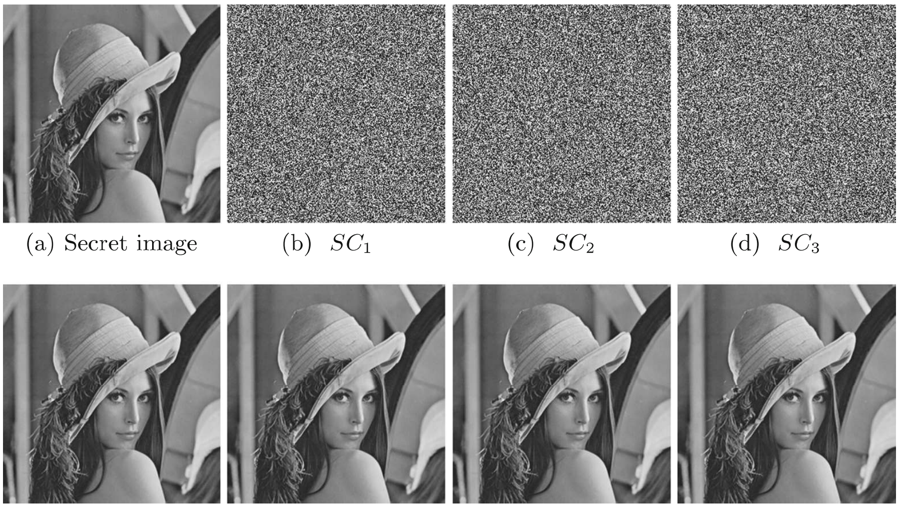
For Algorithms 1 and 2, we remark that.

1. In Step 1 of our Algorithm 1, $\{128 \leq p < m_1 < m_2 \cdots < m_n \leq 255\}$ is given by image pixel value range and $pN < M$. We suggest that p is as small as possible for security as well as m_i is as large as possible so that the pixel values in shadow images can randomly lie in large range. $\gcd(m_i, m_j) = 1$ and $\gcd(m_i, p) = 1$ aim to satisfy CRT conditions.
2. In Step 3 of our Algorithm 1, we know A is randomly picked up from $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$, thus $0 \leq y < M$ in order to obtain (k, n) threshold for y as explained in Sect. 2.1.
3. In Step 3 of Algorithm 1, T divides interval $\left[\left\lceil \frac{N}{p} \right\rceil, \left\lfloor \frac{M}{p} - 1 \right\rfloor\right]$ into two parts with a view to classify $0 \leq x < p$ or $p \leq x \leq 255$ according to Step 3 of Algorithm 2. As a result, x can be losslessly recovered for arbitrary $x \in [0, 255]$.
4. In Step 3 of Algorithm 1, A is randomly picked up for every x, therefore $y = x + Ap$ can enlarge x value so as to scramble not only the pixel value but also the correlations between adjacent pixels without auxiliary encryption.
5. In Step 3 of Algorithm 1, $y = x + Ap$ and $x < p$ can determine only one x based on $x \equiv y \pmod{p}$.

```
Algorithm 2. Secret image recovery of the proposed scheme.
Input: $k$ shadow images $SC_{i_1}, SC_{i_2}, \cdots SC_{i_k}$, their corresponding privacy modular integers $m_1, m_2, \cdots m_n$, $p$ and T.
Output: A $H \times W$ recovered secret image $S'$.
Step 1: For each position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2-3.
Step 2: Let $a_{i_j} = SC_{i_j}(h, w)$ for $j = 1, 2, \cdots, k$. To solve the following linear equations by the Chinese remainder theorem.
    $$\begin{aligned} y &\equiv a_1 \,(\text{mod } m_1) \\ y &\equiv a_2 \,(\text{mod } m_2) \\ &\cdots \\ y &\equiv a_{k-1} \,(\text{mod } m_{k-1}) \\ y &\equiv a_k \,(\text{mod } m_k) \end{aligned} \tag{2}$$
Step 3: Compute $T^* = \left\lfloor \frac{y}{p} \right\rfloor$. If $T^* \geq T$, let $x \equiv y \,(\text{mod } p)$. Else let $x \equiv y \,(\text{mod } p) + p$. Set $S'(h, w) = x$.
Step 4: Output the recovered binary secret image $S'$
```

4 Experimental Results and Analyses

In this section, experiments and analyses are performed to evaluate the effectiveness of our method.


(a) Secret image (b) SC_1 (c) SC_2 (d) SC_3

(e) $CRT(SC_1, SC_2)$ (f) $CRT(SC_1, SC_3)$ (g) $CRT(SC_2, SC_3)$ (h) $CRT(SC_1, SC_2, SC_3)$

Fig. 1. Experimental example of CRTSIS method for (k, n) threshold, where $k=2, n=3$

CRT recovery. When $t < k$ shadow images are collected, there is no clue about the secret image. While when k or more shadow images are collected, the secret image are reconstructed losslessly by CRT.

Based on the above results we can conclude that:

- The shadow images are noise-like, therefore the proposed scheme has no cross interference of secret image in single shadow image.
- When $t < k$ shadow images are collected, there is no information of the secret image could be gained, which shows the security of the proposed scheme.
- When $t(k \leq t \leq n)$ shadow images are recovered by CRT, the secret image could be reconstructed losslessly by CRT.
- CRTSIS method for (k, n) threshold is achieved.

5 Conclusion

In this paper, based on the study of image feature and Chinese remainder theorem (CRT), we propose a CRTSIS method for (k, n) threshold, through dividing the gray image pixel values into two intervals corresponding to two available mapping intervals. Our method realizes (k, n) threshold and lossless recovery for gray image without auxiliary encryption. Experimental results of typical SIS schemes further show the effectiveness of our work. Parameters evaluating and analyzing will be our future work.

Acknowledgments. The authors would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491).

References

1. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theory **29**(2), 208–210 (1983)
2. Chuang, T.W., Chen, C.C., Chien, B.: Image sharing and recovering based on Chinese remainder theorem. In: International Symposium on Computer, Consumer and Control, pp. 817–820 (2016)
3. Hu, C., Liao, X., Xiao, D.: Secret image sharing based on chaotic map and Chinese remainder theorem. Int. J. Wavelets Multiresolut. Inf. Process. **10**(3), 1250023 (2012). [18 pages]
4. Fu, Z., Ren, K., Shu, J., Sun, X., Huang, F.: Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans. Parallel Distrib. Syst. **27**(9), 2546–2559 (2016)
5. Li, P., Ma, P.J., Su, X.H., Yang, C.N.: Improvements of a two-in-one image secret sharing scheme based on gray mixing model. J. Vis. Commun. Image Represent. **23**(3), 441–453 (2012)
6. Mignotte, M.: How to share a secret. In: Beth, T. (ed.) EUROCRYPT 1982. LNCS, vol. 149, pp. 371–375. Springer, Heidelberg (1983). doi:10.1007/3-540-39466-4_27
7. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)