




Secret Image Sharing for (k, k) Threshold Based on Chinese Remainder Theorem and Image Characteristics

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

National University of Defense Technology, Hefei 230037, China
publictiger@126.com

Abstract. Secret image sharing (SIS) based on Chinese remainder theorem (CRTSIS) has lower recovery computation complexity than Shamir's polynomial-based SIS. Most of existing CRTSIS schemes generally have the limitations of auxiliary encryption and lossy recovery, which are caused by that their ideas are borrowed from secret data sharing. According to image characteristics and CRT, in this paper we propose a CRTSIS method for (k, k) threshold, based on enlarging the grayscale image pixel values. Our method owns the advantages of no auxiliary encryption and lossless recovery for grayscale image. We perform experiments and analysis to illustrate our effectiveness.

Keywords: Secret image sharing · Chinese remainder theorem
Image characteristics · Lossless recovery

1 Introduction

Secret image sharing (SIS) scheme encodes the secret image into multiple noise-like shadow images i.e., shadows or shares, which are then assigned to multiple participants. The secret can be disclosed by sufficient shadow images while insufficient shadow images rebuild nothing about the secret. SIS may be applied in many scenarios, such as, authentication, watermarking, access control, information hiding, transmitting passwords, distributed storage and computing etc. To share grayscale image, there exist Shamir's polynomial-based method [5], Chinese remainder theorem-based SIS (CRTSIS) [1, 10] and so on [9, 11].

Shamir's polynomial-based SIS [5] encodes the secret image into the constant coefficient of a random $(k - 1)$ -degree polynomial to possess n shadow images, which are then as well assigned to n participants. The secret image can be disclosed with high-resolution making use of Lagrange interpolation by any k or more shadow images. Following Shamir's original scheme and using all the k coefficients of the polynomial to take secrets, Thien and Lin [7] decreased the shadow image size $1/k$ times to the original secret image. Inspired by Thien and

Lin's research, some researchers [4, 12] developed more Shamir's polynomial-based schemes to receive more features. Although Shamir's polynomial-based SIS only needs k shadow images for decoding the distortion-less secret image, it is in general lossy recovery with auxiliary encryption and high computation complexity. On account of the secret is decoded modulo 251 which is less than maximum pixel value 255, the recovery image will be lost when the pixel value of the secret image is larger than 251 so that Shamir's polynomial-based SIS owes a little bit of loss. Image encryption is usually utilized before sharing that results in auxiliary encryption. Because of Lagrange interpolations in the recovery phase, it needs $O(k \log^2 k)$ operations [1], i.e., complicated computations.

CRTSIS overall can achieve the advantages of lossless recovery, no auxiliary encryption and lower recovery computation complexity (the modular only $O(k)$ operations [1]), so that which is discussed by other researchers [2, 3, 6, 8, 10].

Related works of CRTSIS are analyzed as follows. Yan *et al.* firstly [10] discussed CRT in SIS, which may deduce a little information leakage and may be lossy. Shyu and Chen [6] put forward a threshold CRTSIS utilizing Mignotte's scheme based on pseudo random number generator which suffers from auxiliary encryption. Ulutas *et al.* [8] investigated a modified SIS using Asmuth Bloom's secret sharing scheme through dividing the grayscale image pixel values into more possible intervals. It fails to consider pixel value 2 times or more to the parameter, which may lead to lossy recovery. Chunqiang *et al.* [3] designated a CRTSIS employing the chaotic map which results in auxiliary encryption. Chuang *et al.* [2] gave a simple CRTSIS and examined $(3, 5)$ threshold for RGB color images. Their method has the limitation of lossy or least significant bits pre-stored. In addition, their algorithm parameters condition is different from the adopted explicit parameters in the experiment. Finally, most existing CRTSIS schemes fail to provide applicable explicit parameters for the implementations based on the image characteristics. As a result, traditional CRTSIS methods overall suffer from auxiliary encryption, lossy recovery and ignoring the image characteristics, which are caused by that their ideas are borrowed from secret data sharing.

According to image characteristics and CRT, in this paper we propose a CRT-SIS method for (k, k) threshold, through enlarging the grayscale image pixel values. Our method owns the benefits of no auxiliary encryption and lossless recovery for grayscale image. The contributions of this paper are that, according to the image characteristics, our (k, k) threshold CRTSIS for grayscale image is lossless recovery without auxiliary encryption. Furthermore, we provide explicit parameters for the implementations based on image pixel value range. We perform experiments and analysis to illustrate our effectiveness.

The rest of the paper is organized as follows. Section 2 introduces some basic requirements for the proposed method. In Sect. 3, our method is presented in detail. Section 4 is devoted to experimental results. Finally, Sect. 5 concludes this paper.

2 Preliminaries

In this section, we describe some preliminaries for our work. In (k, k) threshold SIS, the original secret image S is encrypted among k shadow images SC_1, SC_2, \dots, SC_k , and the decrypted secret image S' is reconstructed from k shadow images.

2.1 Chinese Remainder Theorem (CRT)

CRT has a long history. It motivates to solve a set of linear congruence equations.

A set of integers $m_i (i = 1, 2, \dots, k)$ are chosen subject to $\gcd(m_i, m_j) = 1, i \neq j$. Then there exists only one solution $y \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_k M_k M_k^{-1}) \pmod{M}$, $y \in [0, M - 1]$ satisfying the following linear congruence equations.

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

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

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

We note that in $[0, M - 1]$ there exists unique solution. If only the first $k - 1$ equations in Eq. (1) are given, we can gain only one solution for 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 $b = 1, 2, \dots, m_k - 1$ are the solutions as well satisfying the first $k - 1$ equations in Eq. (1). Thus, there are another $m_k - 1$ solutions in $[\prod_{i=1}^{k-1} m_i - 1, M - 1]$, other than unique one, which will be applied in the proposed method to get (k, k) threshold.

2.2 The Feature Analysis of Image

Image is different from pure data. The image consists of pixels, and there are some correlations between pixels as well, such as texture, edge, structure and other related information. As a result, SIS should scramble both the pixel values and the correlations between adjacent pixels.

The pixel value range of grayscale image is $[0, 255]$, which should be referred in the SIS design, such as, the secret pixel value is less than 256 and the shadow image pixel value is less than 256 as well. In addition, we know $m_i \leq 256$ in Eq. (1).

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

We present the proposed CRTSIS method for (k, k) threshold based on the secret image S outputting k shadow images SC_1, SC_2, \dots, SC_k and corresponding private modular integers m_1, m_2, \dots, m_k . Our generation Steps are demonstrated in Algorithm 1. And the recovery Steps are given in Algorithm 2.

<p>Algorithm 1. The proposed SIS CRTSIS method for (k, k) threshold</p> <p>Input: The secret image S with size of $H \times W$.</p> <p>Output: k shadow images SC_1, SC_2, \dots, SC_k and corresponding private modular integers m_1, m_2, \dots, m_k.</p> <p>Step 1: Select a set of integers $\{m_1, m_2, \dots, m_k < 256\}$ subject to</p> $\gcd(m_i, m_j) = 1, i \neq j.$ <p>Here we denote $M = \prod_{i=1}^k m_i$ and $N = \prod_{i=1}^{k-1} m_{n-i+1}$.</p> <p>Step 2: For each position $(h, w) \in \{(h, w) 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 3-4 .</p> <p>Step 3: Let $x = S(h, w)$. We have $0 \leq x < 256$. Pick up a random integer A in $[\lceil \frac{N}{256} \rceil, \lfloor \frac{M}{256} - 1 \rfloor]$ and let $y = x + 256A$.</p> <p>Step 4: Compute $a_i \equiv y \pmod{m_i}$ and let $SC_i(h, w) = a_i$ for $i = 1, 2, \dots, k$.</p> <p>Step 5: Output k shadow images SC_1, SC_2, \dots, SC_k and their corresponding private modular integers m_1, m_2, \dots, m_k.</p>

In Algorithm 1 and Algorithm 2, we remark that.

1. In Step 1 of our Algorithm 1, $\{m_1, m_2 \dots, m_k < 256\}$ is due to shadow image pixel value range. We suggest that m_i is as large as possible so that the pixel values of shadow images will randomly lie in large range. $\gcd(m_i, m_j) = 1$ is issued to satisfy CRT conditions. The user may further restrict $\gcd(m_i, 256) = 1$ for $i = 1, 2, \dots, k$ in specific applications.
2. From Step 3 of our Algorithm 1, A is randomly picked up from $[\lceil \frac{N}{256} \rceil, \lfloor \frac{M}{256} - 1 \rfloor]$, thus $N \leq y < M$ in order to obtain (k, k) threshold for y as explained in Sect. 2.1.
3. In Step 3 of Algorithm 1, since $0 \leq x < 256$ and Step 3 of Algorithm 2, we have x can be losslessly reconstructed for arbitrary $x \in [0, 255]$.
4. In Step 3 of Algorithm 1, A is randomly picked up for each x , therefore $y = x + Ap$ can enlarge x value in order to scramble both the pixel value and the correlations between adjacent pixels without auxiliary encryption.
5. In Step 3 of Algorithm 1, $y = x + Ap$ and $x < 256$ can determine only one x due to $x \equiv y \pmod{256}$.

4 Experimental Results and Analyses

In this section, experiments and analyses are realized to show the effectiveness of our method.

<p>Algorithm 2. Secret image recovery of the proposed scheme.</p> <p>Input: k shadow images SC_1, SC_2, \dots, SC_k, their corresponding private modular integers m_1, m_2, \dots, m_k.</p> <p>Output: A $H \times W$ reconstructed secret image S'.</p> <p>Step 1: For each position $(h, w) \in \{(h, w) 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2-3.</p> <p>Step 2: Let $a_i = SC_i(h, w)$ for $i = 1, 2, \dots, k$. To solve the following linear equations by the Chinese remainder theorem.</p> $\begin{aligned} y &\equiv a_1 \pmod{m_1} \\ y &\equiv a_2 \pmod{m_2} \\ &\dots \\ y &\equiv a_{k-1} \pmod{m_{k-1}} \\ y &\equiv a_k \pmod{m_k} \end{aligned} \tag{2}$ <p>Step 3: Compute $x \equiv y \pmod{256}$. Set $S'(h, w) = x$.</p> <p>Step 4: Output the reconstructed secret image S'.</p>

Figure 1 demonstrates the experimental results for (3,3) threshold, where $m_1 = 253, m_2 = 254, m_3 = 255$ and the grayscale secret image is shown in Fig. 1(a). Figure 1(b-d) display the 3 shadow images SC_1, SC_2, SC_3 , which are noise-like. Figure 1(e-h) indicate the reconstructed secret images by any 2 or 3 shadow images based on CRT, from which the recovered secret image from

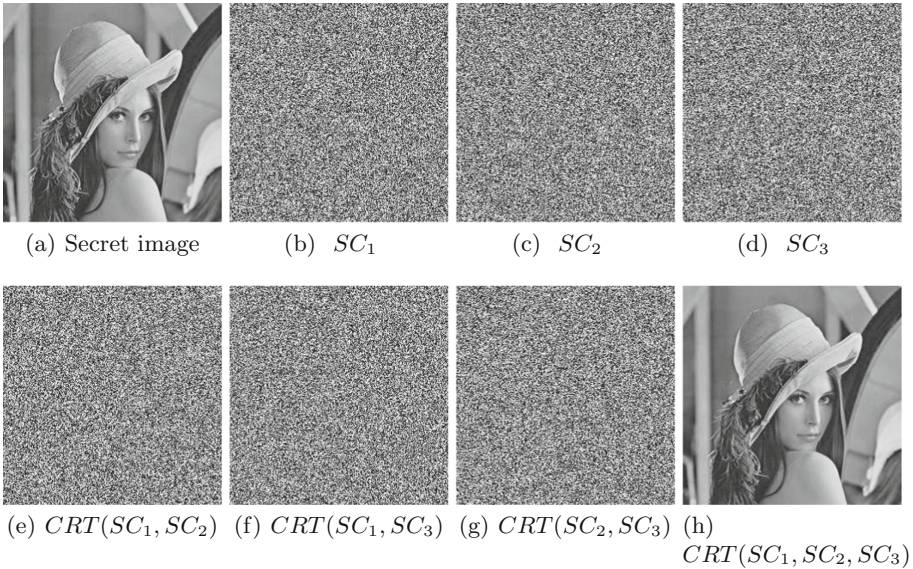


Fig. 1. Experimental example of CRTSIS method for (k, k) threshold, where $k = 3$

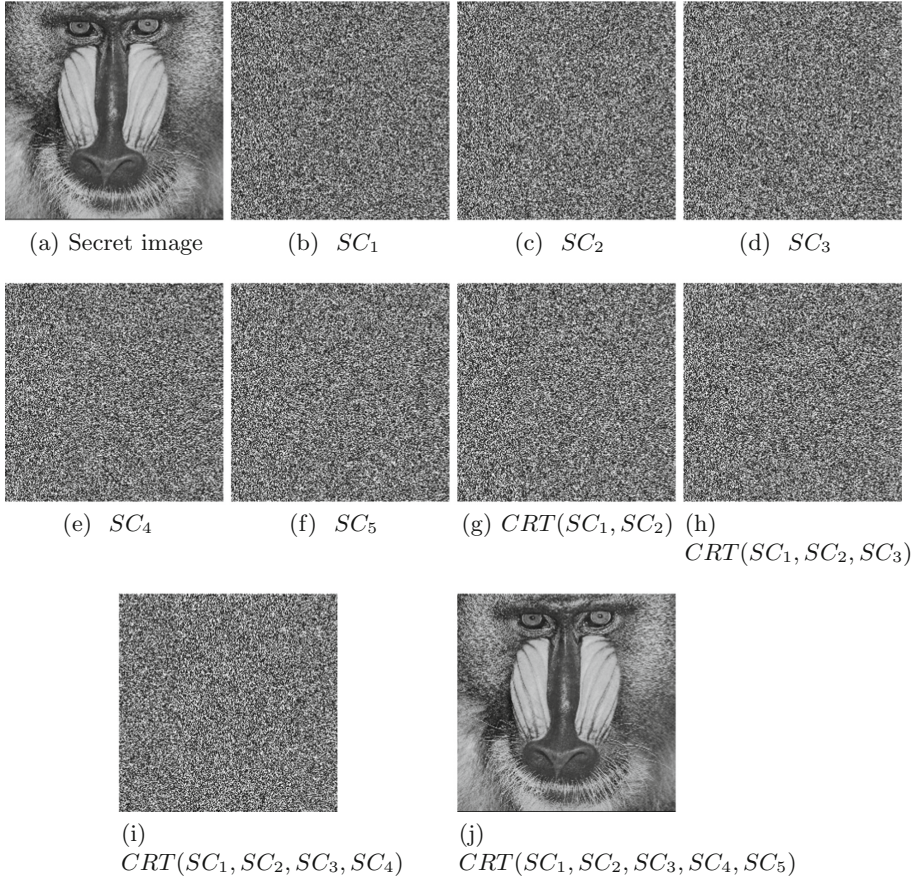


Fig. 2. Experimental example of CRTSIS method for (k, k) threshold, where $k = 5$

$k = 3$ shadow images is lossless by CRT due to $\sum_{h=1}^H \sum_{w=1}^W |S(h, w) - S'(h, w)| = 0$, where $S' = CRT(SC_1, SC_2, SC_3)$ indicates the recovered secret image from SC_1, SC_2, SC_3 by CRT. While any 2 shadow images give no clue about the secret.

The next example, we just give the results by the first t th shadow images for short.

Figure 2 denotes the experimental results for $(5, 5)$ threshold, where $m_1 = 247, m_2 = 251, m_3 = 253, m_4 = 254, m_5 = 255$ and the grayscale secret image is exhibited in Fig. 2(a). Figure 2(b-f) show the 5 shadow images, which are also noise-like. Figure 2(g-j) demonstrate the reconstructed secret image with any t ($2 \leq t \leq 5$) (taking the first t shadow images as an example) based on CRT recovery. When $t < 5$ shadow images are collected, there is no information of the secret image. In contrast, when 5 shadow images are given, the secret image is reconstructed losslessly by CRT.

Based on the above results we can see that:

- Since the shadow images are noise-like, the proposed method has no cross interference of secret image for single shadow image.
- When $t < k$ shadow images are obtained, there is no information of the secret image could be deduced, which shows the security of our scheme.
- When $t = k$ shadow images are given, the secret image will be reconstructed losslessly by CRT.
- CRTSIS method for (k, k) threshold is achieved.

In addition, due to no CRTSIS method for (k, k) threshold designed for image in the literature, we omit the comparisons.

5 Conclusion

In this paper, based on image characteristics and Chinese remainder theorem (CRT), we propose a CRTSIS method for (k, k) threshold, through enlarging the grayscale image pixel values. Our method realizes secure (k, k) threshold and lossless recovery for grayscale image without auxiliary encryption. Experimental results further show the effectiveness of our work, where explicit parameters for the implementations based on image pixel value range are presented. The proposed method may be extended to share color secret image based on color decomposition and color composition. (k, n) threshold extending 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. Chunqiang, H., Xiaofeng, L., Di, X.: Secret image sharing based on chaotic map and Chinese remainder theorem. *Int. J. Wavelets Multiresolut. Inf. Process.* **10**(3), 1250023 (2012). 18 p
4. Li, P., Yang, C.N., Kong, Q.: A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. *J. Real-Time Image Process.* 1–10 (2016)
5. Shamir, A.: How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)
6. Shyu, S.J., Chen, Y.R.: Threshold secret image sharing by Chinese remainder theorem. In: *IEEE Asia-Pacific Services Computing Conference*, pp. 1332–1337 (2008)
7. Thien, C.C., Lin, J.C.: Secret image sharing. *Comput. Graph.* **26**(5), 765–770 (2002)

8. Ulutas, M., Nabiyeu, V.V., Ulutas, G.: A new secret image sharing technique based on Asmuth Bloom's scheme. In: International Conference on Application of Information and Communication Technologies, AICT 2009, pp. 1–5 (2009)
9. Wang, G., Liu, F., Yan, W.Q.: Basic visual cryptography using braille. *Int. J. Digit. Crime Forensics* **8**(3), 85–93 (2016)
10. Yan, W., Ding, W., Dongxu, Q.: Image sharing based on chinese remainder theorem. *J. North China Univ. Tech* **12**(1), 6–9 (2000)
11. Yan, X., Lu, Y.: Progressive visual secret sharing for general access structure with multiple decryptions. *Multimedia Tools Appl.* **77**(2), 2653–2672 (2018)
12. Yang, C.N., Ciou, C.B.: Image secret sharing method with two-decoding-options: lossless recovery and previewing capability. *Image Vis. Comput.* **28**(12), 1600–1610 (2010)