Image Sharing and Recovering Based on Chinese Remainder Theorem

Ting-Wei Chuang, Chaur-Chin Chen, Betty Chien [*]
Institute of Information Systems & Applications
National Tsing Hua University, Hsinchu 30013, Taiwan
E-mail: cchen@cs.nthu.edu.tw

Abstract−Due to the rapid growth of information acquisition in the era of the Internet of Things (IoT) and Cloud Computing, the concern about the security of private information raises a lot of interests. This paper investigates image sharing based on the concept of (k,n)-threshold strategy according to the Chinese remainder theorem (CRT). A secret image is distributed into *n* noise-like shadow images preserved by n participants instead of a single carrier. Collecting at least k out of n shadows can reveal the secret image, but fewer than k shadow images could not. We discuss existing CRT-based sharing methods, proposes a simple CRT-based method and illustrates (3,5)-threshold results for RGB color images.

Index Terms−Blakley, Chinese Remainder Theorem (CRT), Image Sharing, Shamir.

I. INTRODUCTION

In the era of the Internet of Things (IoT) and Cloud Computing, the concern about the security of private information raises a lot of interests. On the other hand, the ownership of images such as military images, medical images, art images and etc. have raised people's attention. To avoid the risk that *a secret image* preserved only by a single carrier, the researchers have devoted to the study of image sharing techniques to overcome this risk. Thus motivated, this paper investigates image sharing according to the concept of (k,n)-threshold strategy which distributes a secret image into n noise-like shadow images independently preserved by n participants such that one has to collect at least k out of n shadows to reveal the original secret image. Most of the contemporary image sharing techniques rely on one of the three secret sharing strategies migrated from cryptography, including

(1) Shamir strategy [5, 8] which is based on the concept that a plane polynomial curve of degree k-1 can be uniquely constructed if there are at least k distinct points in the curve are provided. The strategy is processed under modular arithmetic computation.

(2) Blakley strategy [2, 3] is based on the concept that seeking a unique intersecting point of given at least k designated nonparalell planes in a k-dimensional linear space.

(3) The strategy of image sharing based on Chinese remainder theorem (CRT) [1, 6, 7, 10, 11] is to designate a set of simultaneous congruence equations to distribute the information (integers) from each individual pixel into participants such that a secret image can be revealed pixel by pixel by collecting at least k information out of n participants.

Most existing image sharing methods based on Chinese remainder theorem do not provide explicit parameters for the implementations. This paper reviews existing CRT-based sharing metods and proposes a simple (3,5)-threshold method for both gray and color images.

II. IMAGE SHARING BASED ON CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) [7] is issued to solve a set of simultaneous congruence equations which can be stated as follows. Let $m_1, m_2, \cdots, m_k$ be pairwise coprime positive integers, given nonnegative integers $a_1, a_2, \cdots, a_k$, there exists exactly one solution $x \in [0, m_1 m_2 \cdots m_k)$ for the following simultane-

[*]This work is supported by Taiwan MOST Grant 104-2221-E-007-096-MY2

978-1-5090-3071-2/16 $31.00 © 2016 IEEE
DOI 10.1109/IS3C.2016.208

ous congruence equations

$$\begin{aligned} x &\equiv a_1\ (mod\ m_1) \\ x &\equiv a_2\ (mod\ m_2) \\ &\vdots \\ x &\equiv a_k\ (mod\ m_k) \end{aligned} \quad (1)$$

The solution can be obtained by performing the following procedure (CRT).

(1) Denote $M = \prod_{i=1}^{k} m_i$ and let $z_i = M/m_i$ for $1 \leq i \leq k$.

(2) Let $y_i \equiv z_i^{-1}\ (mod\ m_i)$ for $1 \leq i \leq k$.

(3) Let $x \equiv (a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k)\ \ mod\ M$.

(4) $x \equiv a_i\ (mod\ m_i)\ \ \forall\ 1 \leq i \leq k$, so is the unique solution.

For example, $x = 39\ (mod\ 2 \cdot 5 \cdot 7)$ is the solution for the following congruence equations.

$$x \equiv 1\,(mod\,2),\ \ x \equiv 4\,(mod\,5),\ \ x \equiv 4\,(mod\,7) \quad (2)$$

Based on the Chinese remainder theorem (CRT), Mignotte [11], Asmuth and Bloom [1], Shyu [6], Ulutas et al. [10], Tsai and Chen [9] proposed different implementation methods for solving data and image sharing schemes which are reviewed as follows.

A. Mignotte Sharing Scheme [11]

Mignotte's sharing scheme uses special Mignotte sequences of positive integers. Let k, n be positive integers such that $2 \leq k \leq n$, A Mignotte sequence is a sequence of positive integers $2 \leq m_1 < m_2 < \cdots < m_n$ such that $gcd(m_i, m_j) = 1,\ \ for\ 1 \leq i < j \leq n$ where $m_1 m_2 \cdots m_k > m_{n-k+2} m_{n-k+3} \cdots m_n$.

Mignotte threshold secret sharing scheme can be stated as follows.

(1) Let a secret integer $S \in (\alpha, \beta)$, where $\alpha = m_{n-k+2} m_{n-k+3} \cdots \times m_n$ and $\beta = m_1 m_2 \cdots m_k$.

(2) The share a_i is chosen by computing as $a_i \equiv S\ mod\ m_i$ for $1 \leq i \leq n$.

(3) Collecting at least k distinct shares $a_i's$, the secret S could be revealed by using CRT.

One of the disadvantages for this scheme is that the same secret image pixel values will always be encoded as the same value in a shadow image. Asmuth and Bloom [1] has proposed a method to improve this drawback which is adopted by various researches [6, 10, 9] for the implementation of image sharing and recovering which are reviewed as follows.

B. Asmuth and Bloom Based Sharing Scheme [1]

Based on the idea of Asmuth and Bloom for data sharing, Shyu and Chen [6] extended the sharing scheme proposed by Mignotte to devise a threshold image sharing scheme which uses a pseudo random number generator (PRNG) with a seed to ensure that the same pixel values are not necessarily encoded as the same number. However, the implementation becomes somewhat tedious and complicated becasue the corresponding number acquired by PRNG of each pixel should be recorded. Ulutas et al. [10] proposed a method to drop the PRNG recording numbers for pixels. The sharing and revealing procedures by Ulutas et al. [10] can be summarized as follows.

B.1. A Sharing Procdure

(1) Pick up a set of inteters $\{0 < m_0 < m_1 < \cdots < m_n < 257\}$ subject to

  (a) $gcd(m_i, m_j) = 1\ \ for\ 0 \leq i < j \leq n$.

  (b) $m_0 \cdot \prod_{i=1}^{k-1} m_{n+1-i} < M = \prod_{i=1}^{k} m_i$.

(2) Specify an integer $T \in [0, m_0]$ and sequentially take a pixel value p from the secret image and do the following tasks according to a lexicographic order.

  (a) If $p < m_0$, compute

$$y = p + \alpha \cdot m_0 \quad (3)$$

  where α is an integer randomly picked up from $[(T+1), M]$.

  (b) If $p \geq m_0$, compute

$$y = (p - m_0) + \beta \cdot m_0 \quad (4)$$

  where $\beta \in [0, T]$ is randomly picked up.

(3) Compute

$$y_i \equiv y\ \ mod\ m_i \quad for\ \ i = 1, 2, \cdots, n \quad (5)$$

where y_i is the corresponding pixel value in the $i-th$ shadow image for $1 \leq i \leq n$.

(4) Repeat steps (2) and (3) until all pixels of the secret image are processed. The integer m_i associated with the $i-th$ shadow image are preserved by $i-th$ participant.

B.2. The Revealing Procdure

(1) Collect any k shadow images. Sequentially take the first unused pixel a_i from ith shadow image.

(2) Apply the Chinese remainder theorem to solve the following simultaneous equations.

$$\begin{aligned} y &\equiv a_1\ (mod\ m_1) \\ y &\equiv a_2\ (mod\ m_2) \\ &\vdots \\ y &\equiv a_k\ (mod\ m_k) \end{aligned} \tag{6}$$

(3) Compute the random parameter γ, that is, α or β in the sharing procedure by

$$\gamma = \lfloor \frac{y}{m_0} \rfloor \tag{7}$$

The corresponding pixel value of the secret image is $y\ mod\ m_0$ if $\gamma > T$, otherwise, $m_0 + (y\ mod\ m_0)$ if $\gamma \leq T$.

(4) Repeat steps (1∼3) until all of the pixels are revealed.

Note that the random integers α and β are not required in the revealing procedure which improves the work implemented by Shyu and Chen [6]. However, a user-specified threshold integer T must be provided during sharing and revealing procedures.

III. PROPOSED IMAGE SHARING ALGORITHM BASED ON CRT

We extend the sharing scheme proposed by Ulutas in 2009 based upon Chinese Remainder Theorem (CRT) to designate a (k,n)-threshold secret sharing scheme for digital RGB-color images in a TIFF image file format. In the experiments of this paper, we consider each of R,G,B images is shared by using the same sharing method though other sharing strategies could be used. To meet the restrictions of CRT and the pixel range is in [0,255], we store the least significant bits of R,G,B parts in a file without being shared. The most significant 7 bits are right shifted in one position.

A. A Proposed Sharing Algorithm

(1) Select a set of integers $\{m_0, m_1, m_2, \cdots, m_n\}$ which satisfies $m_0 = 128 < m_1 < m_2 < \cdots < m_n \leq 255\}$ and meets the following two requirements.

(a) $gcd(m_i, m_j) = 1$ for $0 \leq i < j \leq n$.

(b) $M = \prod_{i=1}^{k} m_i > m_0 \cdot \prod_{i=1}^{k-1} m_{n+1-i}$.

(2) Each pixel value x_h of r,g,b signals, respectively is computed according to the following equation

$$y_h = (x_h >> 1) + \alpha \cdot m_0, \quad where\ h = r,\ g,\ or\ b$$

As mentioned before, the last bits are stored separately, and α is an integer randomly generated in $(0, \lfloor \frac{M}{m_0} \rfloor)$. The purpose to use α is to avoid the same value is converted into the identical value in a shadow and α is not required for recovering.

(3) We distribute a shadow pixel value for each participant according to the following modular arithmetic from each y_h value obtained above.

$$\begin{aligned} r_i^{(p)} &\equiv y_r\ mod\ m_i \\ g_i^{(p)} &\equiv y_g\ mod\ m_i \quad for\ i = 1, 2, \cdots, n \\ b_i^{(p)} &\equiv y_b\ mod\ m_i \end{aligned} \tag{8}$$

Note that a color pixel p in the $i-th$ shadow image is recorded as $[r_i^{(p)},\ g_i^{(p)},\ b_i^{(p)}]$.

(4) Repeat steps (2) and (3) until all pixels $\{[y_r, y_g, y_b]\}$ of the secret image are processed, then m_i is associated with the $i-th$ shadow image is kept by the $i-th$ participant for $i = 1, 2, \cdots, n$.

B. The Recovering Algorithm

(1) Collect at least k shadow images associated with $m_j's$, say, $m_1, m_2, \cdots, m_k$ without loss of generality.

(2) Sequentially, take the first pixel, say, w, from each of the k shadow images. We use the k values of $\{r_i^{(w)} | i = 1, 2, \cdots, k\}$ and the Chinese Remainder Theorem (CRT) to resolve $y_r^{(w)}$, the similar action is applied to resolve $y_g^{(w)}$ and $y_b^{(w)}$, respectively.

(3) We reverse the sharing process to reveal the pixel values by

$$x_h = ((y_h\ mod\ m_0) << 1) + t_h^{(w)}, \quad h = r,\ g,\ or\ b$$

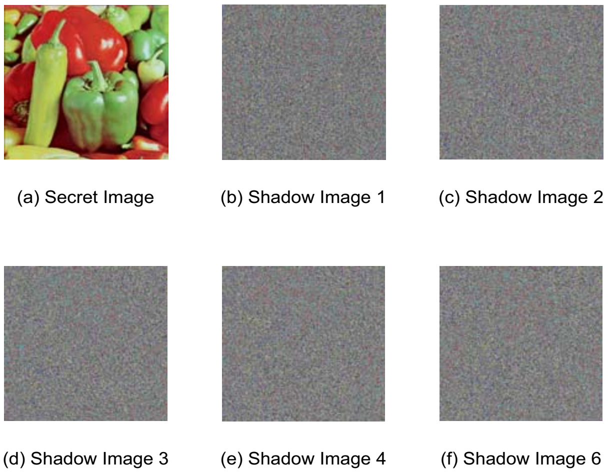
where $t_h^{(w)}$ is the least significant bit value (either 0 or 1) pre-stored before processing image sharing.

(4) Repeat steps (2) and (3) until all pixels of k shadow images are processed.

If an approximate secret image could be accepted, the pre-stored least significant bits could be ignored and can be randomly generated during a recovering process.

IV. EXPERIMENTS

We illustrate our experimental results implemented in a Linux-based system on a $(k, n) = (3, 5)$ threshold method [12]. The parameters $m_0 = 128$ and $(m_1, m_2, m_3, m_4, m_5) = (247, 251, 253, 254, 255)$ are selected so that the pixel values in shadow images randomly lie in the range [0,255) although the first shadow image may only contain pixel values in the range [0,247), all of the five shadow images look like noise without leaking any information of the secret image. A color image ”Peppers” is demonstrated as follows. The shadow images (d), (e), (f) associated with $(m_3, m_4, m_5) = (253, 254, 255)$ can be used to exactly reveal the original image as shown in (a).



(a) Secret Image

(b) Shadow Image 1

(c) Shadow Image 2

(d) Shadow Image 3

(e) Shadow Image 4

(f) Shadow Image 6

Figure 1: An Image and Its Five Shadow Images.

V. DISCUSSION AND CONCLUSION

This paper reviews and discusses commonly used (k, n) threshold methods including Shamir [5, 8], Blakley [2, 3], and CRT-Based methods [1, 10, 11] for image sharing. Generally speaking, a pixel value falls in [0,255] which should be taken into account in the design for image sharing, based on which, we proposed a simple CRT-based method to implement an image sharing and recovering processes. An experiment for $(3, 5)-\mathit{threshold}$ demonstration shows that our method [12] is feasible. Pursuing a sharing algorithm to generate shadow images whose pixel values randomly spread in [0,255] merits further studies.

References

[1] C. Asmuth and J. Bloom, ”A Modular Approach to Key Guarding,” *IEEE Trans. on Information Theory*, vol. 29, no. 2, 208-210, 1983.

[2] G.R. Blakley, ”Safeguarding cryptographic keys,” *Proceedings of the National Computer Conference, American Federation of Information Proceeding Societies*, New York, vol. 48, 313-317, 1979.

[3] C. Chen, W.Y. Fu, and C.C. Chen, ”A Geometry-Based Image Sharing Approach,” *Proceedings of Image and Vision Computing*, Dunedin, Otago, New Zealand, 428-431, 2005.

[4] T.C. Chuang, ”Implementation of Image Sharing Based on Chinese Remainder Theorem,” *M.S. Thesis, National Tsing Hua University*, Hsinchu, Taiwan, April 2015.

[5] A. Shamir, ”How to share a secret?”, *Communications of the ACM*, vol. 22, no. 11, 612-613, 1979.

[6] S.J. Shyu and Y.R. Chen, ”Threshold Secret Image Sharing by Chinese Remainder Theorem,” *IEEE Asia-Pacific Services Computing Conference*, 1332-1337, Yilan, Taiwan, Dec. 9-12, 2008.

[7] D.R. Stinson, ”Cryptography: Theory and Practice,” *Champman & Hall / CRC Press*, 2006.

[8] C.C. Thien and J.C. Lin, ”Secret image sharing,” *Compuers & Graphics*, vol. 26, no. 1, 765-771, 2002.

[9] M.H. Tsai and C.C. Chen, ”A Study on Secret Image Sharing,” *The Sixth International Workshop on Image Media Quality and Its Applications*, 135-139, Tokyo, Japan, September 12-13, 2013.

[10] M. Ulutas, V.V. Nabiyev, and G. Ulutas, ”A New Secret Sharing Technique Based on Asmuth Bloom’s Scheme,” *IEEE International Conference on Application of Information and Communication Technologies*, 1-5, Baku, Oct. 14-16, 2009.

[11] https://en.wikipedia.org/wiki/ Secret_sharing_using_the_Chinese_remainder_theorem, last access on March 24, 2016.

[12] http://www.cs.nthu.edu.tw/.WWW/CRT2016, last access on March 24, 2016.