Sharing an Image with Variable-size Shadows

Shyong Jian Shyu[1,*], Chun-Chieh Chuang[2] and Ying-Ru Chen[1]
[1]*Department of Computer Science and Information Engineering*
Ming Chuan University, No. 5 De Ming Road, Gui Shan, Taoyuan 333, Taiwan
[2]*Department of Computer Science, Taipei Municipal University of Education*
No. 1 Ai-Guo West Road, Taipei 100, Taiwan
[*]sjshyu@mail.mcu.edu.tw

Abstract- *Most secret image sharing schemes produce shadows with an equal size including the well know Shamir's and Thien-Lin's approaches that are based upon polynomial interpolation. In this paper we utilize Chinese remainder theorem to design a novel threshold secret image scheme which produces shadows with different sizes. To share an image secretly among n participants, our scheme determines n relative prime moduli based upon which the image is encoded into n shadows which are distributed to the n participants such that every group of r participants could recover the image by using their shadows and moduli, while any group of less than r participants cannot. Since a shadow is a collection of the remainders of its corresponding modulus in our scheme, the size of the shadow is dependent on that of the modulus. Our scheme is more flexible then those in the literature due to the reason that by choosing a proper set of relative prime moduli the dealer is able to distribute shadows with different sizes to participants with different degrees of importance.*

Keywords: Secret sharing, Threshold structure, Secret image sharing, Chinese remainder theorem.

1. Introduction

Secret sharing aims at protecting a secret by a group of participants where each participant owns a part of the secret called *shadow* which reveals nothing about the secret. To recover the secret, *threshold secret sharing* addresses that only when a certain number (called *threshold*) of participants can reconstruct the secret be using their shadows altogether, while any group of less than the threshold number of participants cannot. Consider a secret s and a set of participants $P = \{1, 2, \dots, n\}$ sharing s. Any approach that achieves the requirements of secret sharing for s with a threshold r among the n participants in P is called an *r out of n* (or (r, n)) *threshold secret sharing scheme*.

Shamir [1] and Blakley [2] independently proposed threshold secret sharing schemes in 1979. Shamir's approach is based upon the *polynomial interpolation* in a two-dimensional space, while Blakley's scheme originates from the intersections of some high-dimensional planes in a high-dimensional space. Shamir's scheme is simple and easy to implement so that it has attracted many researchers' attention [3-7]. We give a brief introduction to Shamir's scheme in the following.

Consider an r–1 degree polynomial:

$$f(x) = a_0 + a_1x^1 + a_2x^2 + \dots + a_{r-1}x^{r-1}$$

where all computations are perform in $GF(p)$ in which p is a prime (or a power of 2 or a prime), $1 \le a_{r-1} < p$, $0 \le a_w < p$ for $0 \le w \le r-2$, and $1 \le x < p$. Shamir's (r, n) scheme apply this polynomial to share a secret s. The dealer sets s to be a_0 and randomly chooses $a_1, a_2, \dots, a_{r-1}$ to form $f(x)$. Then, he/she chooses $x_1, x_2, \dots, x_n$ as *keys* based upon which $f(x_1), f(x_2), \dots, f(x_n)$ are computed as *shadows*. The n pairs of $(f(x_i), x_i)$'s, $1 \le i \le n$, are distributed to the n participants one by one. Since any group of r (or more) $(f(x_i), x_i)$'s is able to obtain $(a_0, a_1, \dots, a_{r-1})$ by solving the r equations using polynomial interpolation, s (= a_0) is thus recovered. None of any group of less than r participants can solve the r equations completely. We say that s is shared by n participants in an (r, n) threshold structure.

Thien and Lin [8] in 2002 extended Shamir's scheme so that the polynomial-based idea can be applied to share a secret image. Consider an image P with N pixels in total which is shared in an (r, n) threshold structure. Thien-Lin's scheme first diffuses all N pixels in P and organizes them into N/r segments with r pixels each. Let the r pixels in segment t be denoted as $(a_0, a_1, \dots, a_{r-1})_t$ for $1 \le t \le N/r$. The values of these r pixels of segment t are assigned to be the r coefficients of the polynomial to form $f_t(x)$. Then, the dealer determines n keys $x_1, x_2, \dots, x_n$, and computes $f_t(x_1), f_t(x_2), \dots, f_t(x_n)$ for

$1 \leq t \leq N/r$. After that, $f_1(x_i)$, $f_2(x_i)$, … , $f_{N/r}(x_i)$ are merged into a *shadow image* D_i for $1 \leq i \leq n$. The dealer distributes (D_i, x_i) to participant i for $1 \leq i \leq n$. It is not hard to see that r (or more) participants can recover $(a_0, a_1, \ldots, a_{r-1})_t$ by their r pairs of keys and shadows with polynomial interpolation for all equations $f_t(x)$'s, $1 \leq t \leq N/r$. $(a_0, a_1, \ldots, a_{r-1})_1$, $(a_0, a_1, \ldots, a_{r-1})_2$, … , $(a_0, a_1, \ldots, a_{r-1})_{N/r}$ are indeed the N pixels in P which have been diffused ever. After re-ordering all of the pixels, we reconstruct P. The shadow size of Thien-Lin's approach is N/r, that is, each D_i contains N/r pixels for $1 \leq i \leq n$. If the original Shamir's approach is directly applied to share the image, the size of each shadow is N. Therefore, Thien-Lin's scheme reduces the size of the shadows as compared to Shamir's.

However, the sizes of all shadow images are the same in either Thien-Lin's or Shamir's approach. In real-world applications, this might not always be an advantage. For instance, a particular participant (the boss, some secret agent, etc.) would like to carry a shadow with a smaller size (than others) for reducing the cost, burden or other concerns. Our interest in this paper is thus to design a secret image sharing scheme with various shadow sizes. Since the dealer could define the degrees of importance of the participants and distribute the different-sized shadows to the participants in terms of their degrees. Essentially, the proposed scheme is based upon the *Chinese remainder theorem*.

The rest of the paper is organized as follows. We introduce Chinese remainder theorem and how to apply CRT to accomplish secret sharing in Section 2. Our threshold scheme for sharing images is proposed in Section 3. Some experiments results and related discussions are reported in Section 4. Section 5 gives some concluding remarks.

2. Previous Studies

2.1 Chinese reminder theorem

Consider a secret value x and $m \geq 2$ positive relatively prime moduli, namely $q_1, q_2, \ldots, q_m$. Let $Q = q_1 \times q_2 \times \ldots \times q_m$ and s_i be the remainder of x modulo q_i for $1 \leq i \leq m$. The Chinese remainder theorem (CRT) asserts that the following system has a unique solution x in Z_Q [9, 10]:

$$x \equiv s_1 \pmod{q_1}$$
$$x \equiv s_2 \pmod{q_2}$$
$$\ldots$$
$$x \equiv s_m \pmod{q_m}$$

Give a number x and m positive relatively prime moduli $q_1, q_2, \ldots, q_m$ where $x \in Z_Q$, the above system is described as:

$$(s_1, s_2, \ldots, s_m) = CRT\_remainders(x, m, q_1, q_2, \ldots, q_m).$$

The solution $x \in Z_Q$ can be obtained by many ways. One of the popular approaches is to compute M_i and its *multiple inverse* c_i (under modulus q_i) for all moduli q_i, $1 \leq i \leq m$ [10] first as follows:

$$M_i = Q / q_i;$$
$$c_i M_i = 1 \bmod q_i.$$

Then x can be obtained by

$$x = \left(\sum_{i=1}^{m} s_i c_i M_i\right) \bmod Q.$$

To ease the following applications of finding a solution based upon CRT, we organize these operations as a procedure:

$$x = CRT\_solution(m, q_1, q_2, \ldots, q_m, s_1, s_2, \ldots, s_m)$$

where $x \equiv s_i \pmod{q_i}$ for $1 \leq i \leq m$.

2.2 Threshold secret sharing by CRT

Let x be a secret value and $q_1, q_2, \ldots, q_m$ be m positive relatively prime moduli where $Q = q_1 \times q_2 \times \ldots \times q_m$ and $x \in Z_Q$. Since $(s_1, s_2, \ldots, s_m) = CRT\_remainder(x, m, q_1, q_2, \ldots, q_m)$, a naïve idea for applying CRT for sharing x among the m participants may be using s_i as the shadow for participant i, $1 \leq i \leq m$. (This was adopted by Meher and Patra in their secret image sharing scheme in 2006 [11].) For instance, assume that $m = 3$ and $(q_1, q_2, q_3) = (3, 5, 7)$. Consider a secret $x = 97$ sharing by the 3 (=m) participants. Since $(s_1, s_2\ s_3) = (1, 2, 6)$ (= $CRT\_remainder(97, 3, 3, 5, 7)$), i.e.

$$97 \equiv 1 \bmod 3$$
$$97 \equiv 2 \bmod 5$$
$$97 \equiv 6 \bmod 7$$

(s_i, q_i) might be distributed to participant i for $i = 1, 2, 3$. Then, only when all three participants contribute their information can they compute $x = 97$; while any group of less than two participants cannot.

Yet, we give an example to illustrate that such naïve application is incorrect in some cases. Consider the same scenario except for $x = 18$. We have $(s_1, s_2\ s_3) = (0, 3, 4)$ (= $CRT\_remainder(18, 3, 3, 5, 7)$):

$$18 \equiv 0 \bmod 3$$
$$18 \equiv 3 \bmod 5$$
$$18 \equiv 4 \bmod 7$$

Indeed, all three participants can obtain 18 (18 = $CRT\_solution(3, 3, 5, 7, 0, 3, 4)$. However, participants 1 and 3 (or 2 and 3) can do so by using their (0, 3) and (4, 7) (or (3, 5) and (4, 7)) (18 = $CRT\_solution(2, 3, 7, 0, 4)$ = $CRT\_solution(2, 5, 7,$

3, 4)) too. Thus, it is not a (3, 3) scheme, let alone a threshold scheme. This naïve application of CRT cannot establish a threshold secret sharing scheme.

To share a secret by using CRT is not a new topic, Mignotte [12] and Asmuth-Bloom [13] proposed (r, n) threshold secret sharing schemes in 1983 individually. Some following studies can be found in [14-17]. Our scheme is based upon Mignotte's idea that is introduced as follows.

Consider n relatively positive prime moduli $q_1 < q_2 < \ldots < q_n$. Let $\alpha = q_{n-r+2} \times q_{n-r+3} \times \ldots \times q_n$ (the product of maximal $r-1$ moduli) and $\beta = q_1 \times q_2 \times \ldots \times q_r$ (the product of the minimal r moduli). Let secret x satisfy $\alpha < x < \beta$. The dealer distributes (s_i, q_i) to participant i for $1 \le i \le n$ where $(s_1, s_2, \ldots, s_n) = CRT\_remainder(x, n, q_1, q_2, \ldots, q_n)$ so as to accomplish sharing x among the n participants in an (r, n) structure. Assume that any group of $r-1$ participants, say $\{i_1, i_2, \ldots, i_{r-1}\}$, compute as follows with their shadows and moduli:

$$y = CRT\_solution(r-1, q_{i_1}, q_{i_2}, \ldots, q_{i_{r-1}}, s_{i_1}, s_{i_2}, \ldots, s_{i_{r-1}}).$$

They can only retain a solution y in $Z_{Q'}$ where $Q' = q_{i_1} \times q_{i_2} \times \ldots \times q_{i_{r-1}} \le \alpha$ $(= q_{n-r+2} \times q_{n-r+3} \times \ldots \times q_n)$ according to CRT. Since $y \le \alpha < x$, $y \ne x$. On the other hand, when r participants, say $i_1, i_2, \ldots, i_r$, compute as follows with all their shadows and moduli, they can recover x:

$$x = CRT\_solution(r, q_{i_1}, q_{i_2}, \ldots, q_{i_r}, s_{i_1}, s_{i_2}, \ldots, s_{i_r}).$$

Therefor the (r, n) threshold property holds.

3. The Proposed Scheme

Consider an $h \times w$ secret image I with M bits in total and a set of n participants sharing I. Our encoding process first chooses n relatively prime moduli $q_1 < q_2 < \ldots < q_n$, and compute $\alpha = q_{n-r+2} \times q_{n-r+3} \times \ldots \times q_n$ and $\beta = q_1 \times q_2 \times \ldots \times q_r$. We regard secret image I as a series of l blocks with d-bit each (i.e. $l = \lceil M/d \rceil$) and take each block, say I_k, as an encoding unit for $1 \le k \le l$. Let x_k denote the decimal value of the d-bit of block I_k, $0 \le x_k \le 2^d-1$.

To cope with the cases like natural images which comprise blocks of similar or even same colors, we simply introduce a series of random numbers, namely *random*()'s, in range $[0, 2^d-1]$ with an initial seed e and perform $x_k \oplus random()$ for all blocks in order to diffuse the values of all blocks where $\oplus$ is the "xor" operation. (Note that it would be shown later that the seed e is also shared among the n participants in the (r, n) structure.)

To maintain the (r, n) threshold property, we adjust the diffused value x_k to be x_k' to assure that the constraint $\alpha < x_k' < \beta$ is met. This is done by adding a pre-determined offset p to the diffused value x_k where $\alpha < p < \beta - 2^d$.

Formally, we set e as the seed of the random sequence, i.e.

$$random\_seed(e),$$

and set the range of the random numbers generated as

$$random\_range(0{:}2^d-1);$$

then perform

$$x_k' = (x_k \oplus random()) + p$$

for all I_k's, $1 \le k \le l$ where *random*() returns a random number which is a member of a random sequence seeded by e. Note that we deliberately set p as the seed e, i.e. $e = p$ in our implementation. Then, x_k' is shared among the n participants in an (r, n) structure by using CRT for all I_k's:

$$(s_{k,1}, s_{k,2}, \ldots, s_{k,n}) = CRT\_remainder(x_k', n, q_1, q_2, \ldots, q_n)$$

where $0 \le s_{k,i} < q_i$. We take $z_i = \lceil \log_2 q_i \rceil$ bits to store $s_{k,i}$ for $1 \le k \le l$ and $1 \le i \le n$. All z_i-bit remainders are merged z_i-bit by z_i-bit to form shadow S_i, i.e.

$$S_i = s_{1,i} \,\|\, s_{2,i} \,\|\, \ldots \,\|\, s_{l,i}$$

where $\|$ denotes the concatenation operation. Thus, the bit-length (size) of S_i is $z_i \times l$ $(= \lceil \log_2 q_i \rceil \times \lceil M/d \rceil)$.

Further, p is shared among the n participants in the (r, n) structure by using CRT, too; that is,

$$(a_1, a_2, \ldots, a_n) = CRT\_remainder(p, n, q_1, q_2, \ldots, q_n).$$

The dealer thus distributes (S_i, a_i, q_i) to participant i for $1 \le i \le n$. Since $q_1 < q_2 < \ldots < q_n$, we have $|z_1| \le |z_2| \le \ldots \le |z_n|$, and consequently, $|S_1| \le |S_2| \le \ldots \le |S_n|$. That means the sizes of the shadows are different (which depend on those of the moduli). Or, each participant receives a part of information whose size is related to his/her degree of importance.

The encoding algorithm is formally illustrated as follows.

<u>Encoding algorithm</u>

Input: a secret image I with M bits in total, a set of participants $P = \{1, 2, \ldots, n\}$ with various degrees of importance, threshold r $(2 \le r \le n)$, and parameter d

Output: shadows S_i and a_i, and modulus q_i for $1 \le i \le n$

1. Choose $\{q_1, q_2, \dots, q_n \mid (q_i, q_j) = 1, 2 \le q_1 < q_2 < \dots < q_n < 2^d\}$ according to the degrees of importance in P
2. $\alpha = q_{n-r+2} \times q_{n-r+3} \times \dots \times q_n$; $\beta = q_1 \times q_2 \times \dots \times q_r$
3. Choose seed p randomly with $\alpha < p < \beta - 2^d$
4. *random_seed*(p); *random_range*($0{:}2^d-1$)
   // set p as the seed of the random sequence ranging from 0 to 2^d
5. Partition I into l ($=\lceil M/d \rceil$) segments: $I_1, I_2, \dots, I_l$ // I_k is with d bits, $1 \le k \le l$
6. for (each I_k, $1 \le k \le l$) do

6.1 { x_k = the decimal representation of I_k

6.2 $x_k' = (x_k \oplus \text{random}()) + p$

6.3 for (each i, $1 \le i \le n$) do $s_{k,i} = x_k' \bmod q_i$ // $|s_{k,i}| = \lceil \log_2 q_i \rceil$

}

7. for (each i, $1 \le i \le n$) do

7.1 { $S_i = \varnothing$

7.2 for (each k, $1 \le k \le l$) do $S_i = S_i \cup \{s_{k,i}\}$ // Append $s_{k,i}$ ($|s_{k,i}| = \lceil \log_2 q_i \rceil$) after S_i ($S_i = S_i \,\|\, s_{k,i}$)

}

8. for (each i, $1 \le i \le n$) do $a_i = p \bmod q_i$
9. Output($S_1, S_2, \dots, S_n, a_1, a_2, \dots, a_n, q_1, q_2, \dots, q_n$)
   // the dealer distributes (S_i, a_i, q_i) to participant i

---

Participant i gets (S_i, a_i, q_i) from the dealer for $1 \le i \le n$. It is noticed that the size of shadow S_i is $\lceil \log_2 q_i \rceil \times \lceil M/d \rceil$ for $1 \le i \le n$. Thus the sizes of S_1, $S_2, \dots, S_n$ are determined by those of $q_1, q_2, \dots, q_n$ which are defined according to the degrees of importance of the participants. This offers a flexible decision about which participant is more/less important at the dealer's convenience.

The decoding algorithm is shown in the following.

Decoding algorithm

Input: r participants $i_1, i_2, \dots, i_r \in P$ and the corresponding moduli $q_{i_1} < q_{i_2} < \dots < q_{i_r}$, shadows $S_{i_1}, S_{i_2}, \dots, S_{i_r}$ and $a_{i_1}, a_{i_2}, \dots, a_{i_r}$, and parameter d

Output: the secret image I

1. $p = \mathit{CRT\_solution}(r, a_{i_1}, a_{i_2}, \dots, a_{i_r}, q_{i_1}, q_{i_2}, \dots, q_{i_r})$
2. for ($1 \le j \le r$) $z_j = \lceil \log_2 q_{i_j} \rceil$
3. *random_seed*(p); *random_range*($0{:}2^d-1$)
4. $I = \varnothing$
5. $l = |S_1| / z_1$ // l is the number of blocks; each shadow has the same l
6. for (each k, $1 \le k \le l$) do

6.1 { for (each S_{i_j}, $1 \le j \le r$) do

{ $s_{k,j}$ = the first z_j bits of S_{i_j}

$S_{i_j} = S_{i_j} - \{s_{k,j}\}$ // delete the first z_j bits from S_{i_j}

}

6.2 $y_k = \mathit{CRT\_solution}(r, s_{k,1}, s_{k,2}, \dots, s_{k,r}, q_{i_1}, q_{i_2}, \dots, q_{i_r})$

6.3 $x_k = (y_k - p) \oplus \mathit{random}()$

6.4 make x_k to be d-bit long

6.5 $I = I \cup \{x_k\}$ // Append x_k after I by d-bit concatenation ($I = I \,\|\, x_k$)

}

7. Output(I)

---

4. Experimental Results

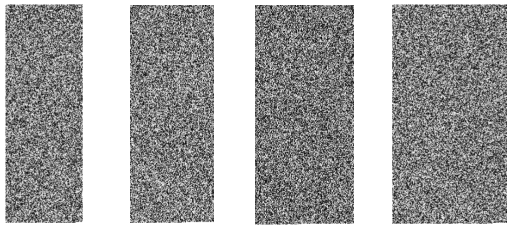
We report the implementation results of our scheme for testing a simple (3, 4) case in this section. Our program was coded in Microsoft C# and run in a PC with Windows. A 256×256 gray-level Lena image was regarded as the secret image I as shown in Figure 1 which is shared by four participants 1, 2, 3 and 4 with the degrees of importance 4 < 3 < 2 < 1. We assume that the dealer would like to produce four shadows S_1, S_2, S_3 and S_4 for participants 1, 2, 3 and 4 respectively with $|S_1| \leq |S_2| \leq |S_3| \leq |S_4|$ so that the most important participant 1 gets the smallest shadow. (Of course, this is the dealer's decision about who gets the smallest shadow.)

In our implementation, we set d as 29 and (q_1, q_2, q_3, q_4) = (1009, 2026, 5095, 31651); thus, α = 5095 × 31651 = 161261845 and β = 1009 × 2026 × 5095 = 10415372230. The secret image is treated as a one dimensional array with M = 256×256×8 = 524288 bit (since one gray pixel takes 8 bits specifying the gray scales in a Windows environment). The number of blocks in our experiment is $l = \lceil M/d \rceil$ = 18079. Note that we simply append white pixels in the last block to make the number of pixels within it to be 29.

Figure 2 shows the four shares S_1, S_2, S_3 and S_4 produced by our encoding algorithm with pixels 89×256, 98×256, 115×256 and 133×256 respectively which meet the requirement of $|S_1| \leq |S_2| \leq |S_3| \leq |S_4|$. Let us explain why the pixels of S_1 is 89×256. Each remainder of a 29-bit block under modulus q_1 (= 1009) is less than 1009 and is stored by using $\lceil \log_2 q_1 \rceil = \lceil \log_2 1009 \rceil$ = 10 bits. Thus, after encoding all l blocks, there are 18079×10 = 180790 encoded bits which constitute S_1. The bit-lengths of the other shadows are determined in the same way. For the display and comparison purposes, we took these consecutive bits as a series of 8-bit gray pixels which constitute a gray-level image with a height of 256. Since $\lceil (180790/8)/256 \rceil$ = 89, thus the width and height of S_1 become 89 and 256 respectively.

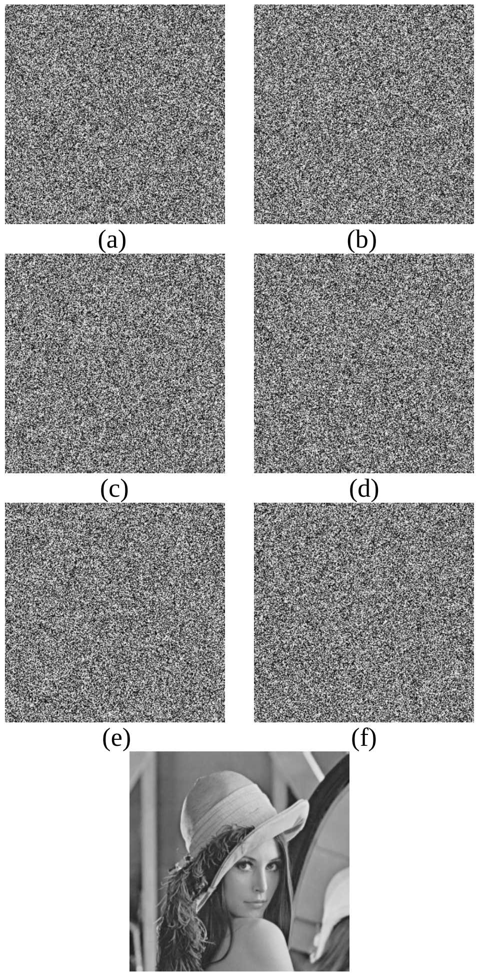
Figure 3 illustrates the reconstructed images from our decoding algorithm by various groups of participants where (a)-(g) are reconstructed results by {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}, {1, 2, 3} respectively. Note that the results obtained by {1, 2, 4}, {1, 3, 4}. {2, 3, 4} and {1, 2, 3, 4} are exactly the same as Figure 3 (g), which is the same as the original Lena image; therefore, we just omit them here. Besides, the pixels (width×height) of these resultant images are all 256×256. This is due to our assumption that the groups of more than one participant knew d (the block size), l (the number of blocks) and the decoding algorithm so that they applied CRT to recover the 29-bit secret blocks by using their information and displayed their result as a 8-bit based gray-level image.

Figure 1. Secret image to be shared.



(a) (b) (c) (d)

Figure 2. Shadows produced by the encoding algorithm: (a) S_1, (b) S_2, (c) S_3, (d) S_4.



(a) (b) (c) (d) (e) (f) (g)

Figure 3. Reconstructed results from the decoding algorithm by various groups of participants: (a) {1, 2}, (b) {1, 3}, (c) {1, 4}, (d) {2, 3}, (e) {2, 4}, (f)

{3, 4}, (g) {1, 2, 3}.

It is easily seen from Figure 3 that any group of less than three participants cannot recover *I*, while all groups of three or more participants can. The attractive feature is that $|S_1| \le |S_2| \le |S_3| \le |S_4|$ whose sizes are determined by the values of the chosen moduli which define the degrees of importance of the participants. These results demonstrated the feasibility and applicability of our scheme.

5. Concluding Remarks

We propose and implement a novel threshold secret image sharing scheme that produce shadows with different sizes by using CRT in this paper. The shadow sizes produced by our scheme are correlated with the degrees of importance of the participants. As compared to the conventional Shamir's and the recent Thien-Lin's approaches which produce shadows with the same size, our scheme is more flexible so that it can be applied to some practical situations that the parts of information given to different participants are with different sizes in terms of their degrees of importance.

It is lucid that our scheme can be easily applied to secretly share a color image in a threshold structure. In the near future, we shall analyze the secrecy of our scheme. In the decoding and encoding algorithms, *d* is designed to be an input parameter and the seed *e* is the same as *p*. To increase the level of secrecy, *d* and *e* might be shared among the *n* participants in an (*r*, *n*) structure.

References

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

[2] G. R. Blakley, "Safeguarding cryptographic keys," *in AFIPS Conf. Proc.*, vol. 48, pp. 313-317, 1979.

[3] E. F. Brickell, "Some ideal secret sharing schemes," *Journal of Combinatorial Mathematics and Combinatorial Computing* , vol. 6, pp. 105-113, 1989.

[4] C.-C. Chang, and R.-J. Hwang, "Sharing secret images using shadow codebooks," *Information Sciences - Informatics and Computer Science: An International Journal*, vol. 111, no. 1-4, pp. 335-345, 1998.

[5] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Proceedings of IEEE. Globecom '87*, pp. 99-102, 1987.

[6] C.-C. Lin, and W.-H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.

[7] K. J. Tan, and H. W. Zhu, "General secret sharing scheme," *Computer Communications*, vol. 22, pp. 755-757, 1999.

[8] C.-C. Thien, and J.-C. Lin, "Secret image sharing," *Computers and Graphics*, vol. 26, pp. 765-770, 2002.

[9] Darel W. Hardy, and Carol L. Walker, *Applied Algebra: codes, ciphers, and discrete algorithms*, Prentice Hall, 2003.

[10] W. Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hill, 2005.

[11] P. K. Meher, and J. C. Patra, "A new approach to secure distributed storage, sharing and dissemination of digital image," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 373-376, 2006.

[12] M. Mignotte, "How to share a secret," *In T. Beth, editor, Lecture Notes in Computer Science*, vol. 149, pp. 371-375, 1983.

[13] C. Asmuth, and J. Bloom, "A Modular Approach to Key Safeguarding," *IEEE Transactions on information theory*, vol. IT-29, no. 2, pp. 208-210, 1983.

[14] T. Galibus, and G. Matveev, "Generalized mignotte's sequences over polynomial rings," *Electr. Notes Theor. Comput. Sci.*, vol. 186, pp. 43-48, 2007.

[15] S. Iftene, "Compartmented secret sharing based on the Chinese remainder theorem," *Cryptology ePrint Archive*, 2005.

[16] S. Iftene, "General secret sharing based on the Chinese remainder theorem," *Cryptology ePrint Archive*, Report 2006/166, 2006.

[17] H.-X. Li, L.-J. Pang, and W.-D Cai, "An efficient threshold multi-group-secret sharing scheme," *Advances in Soft Computing*, vol. 40, pp. 911-918, 2007.