J. Algebra Comb. Discrete Appl.
6(3) • 147–161

Received: 10 February 2019
Accepted: 19 August 2019

Journal of Algebra Combinatorics Discrete Structures and Applications

A generalization of the Mignotte's scheme over Euclidean domains and applications to secret image sharing*

Research Article

Ibrahim Ozbek, Fatih Temiz, Irfan Siap

Abstract: Secret sharing scheme is an efficient method to hide secret key or secret image by partitioning it into parts such that some predetermined subsets of partitions can recover the secret but remaining subsets cannot. In 1979, the pioneer construction on this area was given by Shamir and Blakley independently. After these initial studies, Asmuth-Bloom and Mignotte have proposed a different (k, n) threshold modular secret sharing scheme by using the Chinese remainder theorem. In this study, we explore the generalization of Mignotte's scheme to Euclidean domains for which we obtain some promising results. Next, we propose new algorithms to construct threshold secret image sharing schemes by using Mignotte's scheme over polynomial rings. Finally, we compare our proposed scheme to the existing ones and we show that this new method is more efficient and it has higher security.

2010 MSC: 11K31, 94A08, 94A62, 13F07

Keywords: Mignotte sequences, Secret image sharing, Secret sharing scheme, Euclidean domain

1. Introduction

The rapid improvement of technology and the increase of the usage of the internet day by day introduces some new challenges. One of the most important challenge is the security of data (message/image). There are several techniques in literature for keeping the data secure. One of them is applying a secret sharing scheme (a.k.a. key safeguarding scheme). Secret sharing schemes play an important role in cryptography especially where the secret key is supposed to be distributed in parts to shareholders so that

* *This research was partially supported by The Scientific and Technological Research Council of Turkey, Project No: 114F388.*
Ibrahim Ozbek; Yildiz Technical University, Graduate School of Science and Engineering, Department of Mathematics, Istanbul, Turkey (email: ibrhmozbek@gmail.com).
Fatih Temiz (Corresponding Author); Istanbul Gelisim University, Department of Management Information Systems, Istanbul, Turkey (email: ftemiz@gelisim.edu.tr).
Irfan Siap; Jacodesmath Institute, Department of Mathematics, Istanbul, Turkey (email: irfan.siap@gmail.com).

some of predetermined shares can recover the key. In order to construct such schemes many methods have been developed over the last 30 years [14]. The first secret sharing scheme is introduced by Blakley and Shamir independently [2, 12]. They propose a (k, n) threshold secret sharing scheme, i.e. any k out of n participants can reconstruct the secret key but any $k-1$ or fewer participants cannot reconstruct it.

In [1, 9], Asmuth-Bloom and Mignotte propose a different (k, n) threshold modular secret sharing scheme by using Chinese remainder theorem. These two methods depend on a particular choice of the ordering and the selection of positive integers that are used as module. Mignotte's method is over integers, on the other hand Asmuth-Bloom's modular approach is applicable to not only integers but also to Euclidean domains in general. In [5], Mignotte's construction is further generalized to not necessarily relatively coprime integers which are called generalized Mignotte sequences and an application to e-voting is presented.

Also, another generalization of Mignotte's construction over polynomial rings is given in [16].

In [10], Naor and Shamir propose an interesting method for encrypting visual data which is called visual cryptography. In this method, there is no cryptographic computation to recover secret image, that is, decoding process of the method is based solely on human visual system. After this pioneer construction, to overcome memory space problem, Thien and Lin propose threshold secret image sharing scheme by using Shamir's scheme [17]. In this scheme, they consider each k pixels of a secret image S as coefficients of polynomials and compute the values of these polynomials to generate the n shadow images. Since the scheme's reconstruction is based on Lagrange interpolation, any k out of n shadow images can reconstruct the secret image S but any $k-1$ or fewer shadow images cannot reconstruct the secret image. By taking advantage of Huffman encoding, Wang and Su come up with a new secret image sharing scheme that uses smaller shadow images [19]. In [8], Meher and Patra design a new scheme which is not a threshold by taking advantage of Chinese remainder theorem. Unlike the previous work, the shadow images of this scheme may have distinct sizes. In [13], Shyu and Chen give another threshold scheme which is based on Mignotte's secret sharing scheme.

In this study, we give a generalization of Mignotte's scheme over Euclidean domains. We also construct threshold secret image sharing schemes based on generalization of Mignotte's scheme over polynomial rings. We organize this paper as follows: In Section 2, we give basics of secret sharing schemes and recall the construction of Mignotte's scheme. The generalization of Mignotte's scheme over Euclidean domains is given in Section 3. In Section 4, we propose new algorithms to construct threshold secret image sharing schemes and an experimental result is presented in Section 5. In section 6, the security analysis of algorithms is also analyzed. In Section 7, our proposed secret image sharing scheme is compared with the state of the art methods. Finally, conclusions and comparisons to the existing methods are summarized in Section 8.

2. Preliminaries

A secret sharing scheme is a method of sharing a secret S among n participants $P = \{P_1, P_2, \ldots, P_n\}$ by using a distribution rule $F = \{f \,|\, f : V \to P\}$ such that some predetermined subsets of 2^P can reconstruct the secret S, where V is the set of shares (shadows). The subsets that can construct the secret S are called access structures and the set of such subsets is denoted by Γ, and any subset of participants that is not in Γ cannot reconstruct the secret S. If every k out of n participants can determine the secret S and any out of $k-1$ or fewer participants cannot determine the secret S, then this scheme is called a (k, n) threshold scheme and the access structure of this scheme is $\Gamma = \{A \,|\, |A| \geq k, A \subseteq 2^P\}$ [12]. Also, if $k-1$ or fewer participants cannot obtain any helpful information about the secret S, i.e. do not have any advantage in order to reconstruct the key, then this is called a perfect secret sharing scheme [14].

There are various kinds of generalizations of Chinese remainder theorem (CRT) in literature, we give some of them which are necessary for our constructions in the following sections. The following is called Chinese remainder theorem for commutative rings [4].

Theorem 2.1. *Let $I_1, I_2, \ldots, I_n$ be ideals of a commutative ring R with identity such that $I_i + I_j = R$*

for all $i \neq j$. Then, there exists a ring isomorphism

$$\varphi : R/I_1I_2\cdots I_n \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

$$x \mapsto x \bmod I_1, x \bmod I_2, \ldots, x \bmod I_n.$$

Conversely, given the module values of x, then x is uniquely determined up to congruence modulo the ideal

$$I = I_1I_2\cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n.$$

The version of this theorem can be given in a similar way for integers and polynomial rings (also Euclidean domains) [3, 6]. Next, we give a more general version of CRT developed by Ore such that $q_1, q_2, \ldots, q_n$ do not have to be pairwise relatively prime [11].

Theorem 2.2. *[11] Let $q_1, q_2, \ldots, q_n \geq 2$ be a collection of positive integers. For any set of elements a_i the system of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \bmod q_1 \\ x &\equiv a_2 \bmod q_2 \\ &\vdots \\ x &\equiv a_n \bmod q_n \end{aligned}$$

has a solution if and only if $a_i \equiv a_j \bmod (q_i, q_j)$ for all $i \neq j$, $1 \leq i, j \leq n$, where (q_i, q_j) is the greatest common divisor of q_i and q_j. Moreover, the system has a unique solution in modulo $q = lcm(q_1, q_2, \ldots, q_n)$, where q is the least common multiple of $q_1, q_2, \ldots, q_n$ and it can be computed as follows

$$x \equiv a_1\frac{q}{q_1}b_1 + a_2\frac{q}{q_2}b_2 + \cdots + a_n\frac{q}{q_n}b_n$$

where b_i are integers such that $b_1\frac{q}{q_1} + b_2\frac{q}{q_2} + \cdots + b_n\frac{q}{q_n} = 1$.

If $q_1, q_2, \ldots, q_n$ are relatively prime, then we obtain the standard version of CRT. Furthermore, a general version of CRT can be applied to polynomial rings [16].

The Chinese remainder theorem has many applications in literature [3]. One of them is on secret sharing. There are two different pioneer constructions to recover the secret S with CRT given by Asmuth-Bloom and Mignotte [1, 9]. Next, we recall the construction of Mignotte's scheme.

Mignotte's Construction

Mignotte introduced a (k, n) threshold secret sharing scheme using a special subset of coprime numbers which are called Mignotte's sequences [9]. The trick of this construction is the choice of the secret S in a particular range. Now, let us recall the construction given by Mignotte based on CRT.

The system is composed by a dealer and n participants. The dealer constructs the system and gives the shares to the participants as follows:

1. Dealer chooses positive integers $q_1 < q_2 < \cdots < q_n$ such that $(q_i, q_j) = 1$ for all $1 \leq i < j \leq n$ and

$$\prod_{i=n-k+2}^{n} q_i < \prod_{i=1}^{k} q_i.$$

2. The secret S is a randomly chosen integer in the following interval

$$\prod_{i=n-k+2}^{n} q_i < S < \prod_{i=1}^{k} q_i.$$

3. The shadows v_i are computed as:

$$\begin{aligned} v_1 &\equiv S \bmod q_1 \\ &\vdots \\ v_n &\equiv S \bmod q_n \end{aligned}$$

and distributed to the participants $P_i = (v_i, q_i)$ for all $1 \leq i \leq n$.

4. Given k out of n distinct participants $\{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\}$, the secret S is recovered uniquely in modulo $q = q_{i_1} q_{i_2} \cdots q_{i_k}$ using the standart CRT as follows:

$$S \equiv v_{i_1} r_{i_1} \frac{q}{q_{i_1}} + \cdots + v_{i_k} r_{i_k} \frac{q}{q_{i_k}} \bmod q$$

where $r_{i_j} \frac{q}{q_{i_j}} \equiv 1 \bmod q_{i_j}$ for all $1 \leq j \leq k$.

Example 2.3. *Let us consider a* $(2, 4)$ *threshold scheme and choose pairwise coprime numbers* $q_1 = 11, q_2 = 15, q_3 = 17$, *and* $q_4 = 26$. *The secret can be chosen inside the interval* $26 < S < 165$. *Let* $S = 124$ *and the corresponding shadows be* $v_1 = 3$, $v_2 = 4$, $v_3 = 5$, $v_4 = 20$. *Each participant in a system has a pair of information* (v_i, q_i). *Suppose that* P_1 *and* P_2 *want to find the secret* S *by using their shadows* $\{(3, 11), (4, 15)\}$. *First,* $r_1 = 3, r_2 = 11$ *is found and the secret can be computed uniquely modulo* 165 *as follows:*

$$S \equiv (3 \cdot 3 \cdot 15 + 4 \cdot 11 \cdot 11) \bmod 165 \equiv 124.$$

In this example, we see that any two out of four participants can recover the secret by putting their partial information together.

3. Generalization of Mignotte's scheme over Euclidean domains

In this section, we generalize the threshold secret sharing scheme given by Mignotte [9] to Euclidean domains. Let us first recall the definition of Euclidean domains.

Definition 3.1. *Let* D *be an integral domain and* $R = Z^+ \cup \{0\}$ *be the set of nonnegative integers.* D *is called Euclidean domain if there is a norm function* $N : D \backslash \{0\} \to R$ *with the following two properties:*

1. *For any* $a, b \in D \backslash \{0\}$, $N(a) \leq N(ab)$,
2. *For all* $a, b \in D$ *with* $b \neq 0$ *we can write* $a = qb + r$ *for some* $q, r \in D$ *such that* $r = 0$ *or* $N(r) < N(b)$.

Now, we construct a (k, n)-threshold scheme over a Euclidean domain. Let D be a Euclidean domain. Choose the elements $q_1, \ldots, q_n \in D$ such that $(q_i, q_j) = 1$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$ and $N(q_i) < N(q_j)$ for all $i < j$, where N is a suitable degree function defined on Euclidean domain. Dealer chooses a secret $S \in D/\langle q_1 \cdots q_n \rangle$ satisfying the following conditions:

1. $N(\alpha) = N(q_{n-k+2}) N(q_{n-k+3}) \cdots N(q_n) < N(S)$ and
2. $N(S) < N(\beta) = N(q_1) N(q_2) \cdots N(q_k)$.

The Dealer now determines the shares $v_1, \ldots, v_n$ to be distributed to the n participants in the following way:

$$\begin{aligned} v_1 &\equiv S \bmod q_1 \\ v_2 &\equiv S \bmod q_2 \\ &\vdots \\ v_n &\equiv S \bmod q_n. \end{aligned}$$

Since $D/\langle q_{j_1} q_{j_2} \ldots q_{j_k} \rangle \cong D/\langle q_{j_1} \rangle \times D/\langle q_{j_2} \rangle \times \cdots \times D/\langle q_{j_k} \rangle$ where $q_{j_1}, q_{j_2}, \ldots, q_{j_k} \in \{q_1, q_2, \ldots, q_n\}$, any k out of n participants can reconstruct the secret S by using CRT over Euclidean domains [6]. For instance, first k participants can reconstruct the secret S in the following way:

1. For $1 \leq j \leq k$, define $\mu_j = \prod_{\substack{i=1 \\ i \neq j}}^{k} q_i$ and $\eta_j = \mu_j^{-1} \pmod{q_j}$ where $\eta_j < q_j$.
2. Then, the secret can be computed by

$$S \equiv v_1 \mu_1 \eta_1 + v_2 \mu_2 \eta_2 + \cdots + v_k \mu_k \eta_k \pmod{q_1 q_2 \cdots q_k}. \tag{1}$$

Theorem 3.2. *For the given construction above, any $k-1$ or fewer participants cannot reconstruct the secret S.*

Proof. Assume that any $k-1$ out of n participants come together to reconstruct the secret S. Let these participants $P_{j_1}, P_{j_2}, \ldots, P_{j_{k-1}}$ reconstruct r as a secret with their own shares. It is easily seen that $N(r) < N(S)$ and $S = r + \delta q_{j_1} q_{j_2} \ldots q_{j_{k-1}}$ for some $\delta \in D$. This means that any $k-1$ or fewer participants cannot reconstruct the secret S. □

It is easily seen that the best probability of finding the secret S is

$$\frac{N(q_{j_1} q_{j_2} \cdots q_{j_{k-1}})}{N(\beta) - N(\alpha)}.$$

If the range of norm is large enough, it will be an infeasible problem to determine the secret S.

Example 3.3. *Let us construct a $(2,3)$ threshold secret sharing scheme based on a specific Euclidean domain, i.e. Gaussian integers $Z[i]$. We choose three coprime Gaussian numbers, $11+8i$, $-3-13i$, $7+4i$ and compute their norms $185, 178, 65$ ($N(a+bi) = a^2+b^2$) respectively. Dealer chooses the norm of the secret inside the following interval $185 < S < 11570$. Suppose that dealer chooses the norm of the secret as 424 and a Gaussian integer $18-10i$. After choosing the secret, dealer computes the shares of participants as follows:*

$$\begin{aligned} 18-10i &\equiv -1-7i \pmod{11+8i} \Rightarrow v_1 = -1-7i, \\ 18-10i &\equiv 5-7i \pmod{-3-13i} \Rightarrow v_2 = 5-7i, \\ 18-10i &\equiv 3 \pmod{7+4i} \Rightarrow v_3 = 3. \end{aligned}$$

Hence a $(2,3)$ threshold secret sharing scheme is designed such that any 2 out of 3 participants can reconstruct the secret. We pick P_1 and P_3 and compute the secret in the following way:

$$Z[i]/(11+8i) \times Z[i]/(7+4i) \to Z[i]/(45+100i)$$

$$(-1-7i)(7+4i)[(7+4i)^{-1} \pmod{11+8i}] + 3(11+8i)[(11+8i)^{-1} \pmod{7+4i}]$$

After computing the inverse of Gaussian integers, $(7+4i)^{-1} \pmod{11+8i} \equiv -12+2i$ and $(11+8i)^{-1} \pmod{7+4i} \equiv 7-2i$, we substitute the values and the secret is computed as follows

$$S = (-1-7i)(7+4i)(-12+2i) + (3)(11+8i)(7-2i) \pmod{45+100i} \equiv 18-10i.$$

In the next section, we build our methods over two specific Euclidean domains. Gaussian ring of integers and polynomial rings over fields.

4. A new algorithm for secret image sharing

In this section, we present a new (k, n) threshold secret image sharing scheme such that any k out of n shadow images can reconstruct the secret image S but any $k-1$ or fewer shadow images cannot reconstruct S. The idea behind this construction is a generalization of Mignotte's scheme [16] over polynomial rings. A recent study on Secret Sharing Scheme over polynomial rings is presented in [16]. The difference between our scheme and the method introduced in [16] is that the irreducible polynomials in [16] are chosen of the same degrees (Remark 3.1, [16]). Here in our method we do not impose such a restriction hence this gives us flexibility on construction which leads to a faster applicability and better security.

Since the gray value of a pixel is between 0 and 255 this fact forces us to consider algorithms for distinct prime numbers $p = 251$ and $p = 257$, which are the closest prime numbers smaller and larger than $p = 255$, or the finite field extension $GF(2^8)$. For the first algorithm, we must reduce all the gray values between $251 - 255$ to 250. In the second algorithm, we can encounter invalid gray value, i.e. 256. To overcome this problem, we must increase the size of shadow images (see Algorithm 2, Step 3 and Step 5). In the third algorithm, since the gray values range from 0 to 255, each gray value has a 2-adic representation $a_0 + a_1 2 + \cdots + a_7 2^7$ for some $a_i \in Z_2$, hence there is a map $Z_{256} \to {}^{Z_2[x]}/_{\langle f(x)\rangle}$, $a \to (a_0, \ldots, a_7)$ where $f(x)$ is an irreducible polynomial of degree 8 over Z_2. Since $GF\left(2^8\right) \cong {}^{Z_2[x]}/_{\langle f(x)\rangle}$ and $GF\left(2^8\right)^{\times} = \langle\alpha\rangle$, we have a one-to-one and onto map

$$\phi : Z_{256} \to GF\left(2^8\right)$$
$$a \to \begin{cases} 0, & if\, a = 0 \\ \alpha^{i_a}, & if\, a \neq 0 \end{cases}$$

where $\alpha^{i_a} = a_0 + a_1\alpha + \cdots + a_7\alpha^7$. Because of the above map ϕ, unlike the other two algorithms, there is no truncation and invalid gray value in the last algorithm.

Suppose that we intend to construct a (k, n) threshold secret image sharing for an $m \times r$ secret image S. We first choose n polynomials $q_1, q_2, \ldots, q_n$ such that $(q_i, q_j) = 1$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$ and $\alpha = \deg(q_{n-k+2} \times q_{n-k+3} \times \cdots \times q_n) < \beta = \deg(q_1 \times q_2 \times \cdots \times q_k)$. We suppose that the secret image is divided into $1 \times s$ row vectors such that s divides r. The crucial part of the algorithm is choosing $s-1$ degree polynomials $s_i(x) = g_{i,0} + g_{i,1}x + \cdots + g_{i,s-1}x^{s-1}$, called secret polynomials corresponding the i^{th} partition of S, such that $\alpha < \deg(s(x)) < \beta$, where $g_{i,0}, g_{i,1}, \ldots, g_{i,s-1}$ are the s ordered pixels of i^{th} partition. For the i^{th} partition of S, the i^{th} partition of n shadow images $S_1, S_2, \ldots, S_n$ are obtained in the following way:

$$\begin{aligned} v_{i,1} &\equiv s_i(x) \bmod q_1 \\ v_{i,2} &\equiv s_i(x) \bmod q_2 \\ &\vdots \\ v_{i,n} &\equiv s_i(x) \bmod q_n \end{aligned} \tag{2}$$

where the polynomials $v_{i,j}$ are called shadow polynomials. The steps of algorithms for this secret image sharing schemes are illustrated as follows.

4.1. Algorithm 1 for $p = 251$

The Share Construction

1. If there exists gray values larger than 250, they are set to 250. Thus the gray values are now between the range $0 - 250$. Here there will be some loose of pixel colors that are not distinguishable by naked eye.

2. Choose n polynomials $q_1, q_2, \ldots, q_n$ such that $(q_i, q_j) = 1$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$ and $\alpha = \deg(q_{n-k+2} \times q_{n-k+3} \times \cdots \times q_n) < \beta = \deg(q_1 \times q_2 \times \cdots \times q_k)$.

3. The secret polynomials $s_i(x)$ corresponding to i^{th} partition of the secret image are obtained by letting the s coefficients be the gray values of s pixels of i^{th} partition such that $\alpha < \deg(s_i(x)) = s - 1 < \beta$.

4. Using the secret polynomial $s_i(x)$ for i^{th} partition, generate n shadow polynomials $v_{i,j}$ for all $1 \leq j \leq n$ by using Equation 2 and set $l_i = \deg(q_i)$ for $1 \leq i \leq n$.

5. For all partitions of the secret image, apply Steps 3 and 4.

Remark: The degrees of n polynomials $q_1, q_2, \ldots, q_n$ can be chosen arbitrarily as long as the condition $\deg(q_{n-k+2} \times q_{n-k+3} \times \cdots \times q_n) < \deg(q_1 \times q_2 \times \cdots \times q_k)$ is satisfied. If at least one of the polynomials $q_1, q_2, \ldots, q_n$ have different degree than the others, then the size of one of $S_1, S_2, \ldots, S_n$ may be different from each other. In order to correctly reconstruct the image, we must give the information of number of pixels in partitions for each shadow images to the participants. This means that the shares of participants are (S_i, q_i, l_i) for all $1 \leq i \leq n$, where l_i is the number of pixels in each partition.

The Reconstruction Phase

1. For all $1 \leq i \leq n$, generate k shadow polynomials using first l_i pixels of k shadow images.

2. Using k shadow polynomials $v_{1,i_1}, v_{1,i_2}, \ldots, v_{1,i_k}$ and Equation 1, one can obtain the secret polynomial $s_1(x)$, i.e. we first get s pixels of the secret image.

3. For all other pixels of k shadow images, apply Step 1 and 2.

4.2. Algorithm 2 for $p = 257$

The Share Construction

1. Choose n polynomials $q_1, q_2, \ldots, q_n$ such that $(q_i, q_j) = 1$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$ and $\alpha = \deg(q_{n-k+2} \times q_{n-k+3} \times \cdots \times q_n) < \beta = \deg(q_1 \times q_2 \times \cdots \times q_k)$.

2. Find the secret polynomial $s_i(x)$ for the i^{th} partition of the secret image such that $\alpha < \deg(s_i(x)) = s - 1 < \beta$.

3. By using Equation 2, find the shadow polynomials $v_{i,j}$ for all $1 \leq j \leq n$ and apply the following steps.

   (a) If the coefficients of $v_{i,j}$'s are not equal to 255 or 256, the i^{th} partition of S_j is generated by using the coefficients of $v_{i,j}$.

   (b) If a coefficient v_{i,j_k} of $v_{i,j}$ is equal to 255, then consider 255 as a couple 255 and 0 and write $255x^{k-1} + 0x^k$ as the polynomial $v_{i,j}$.

   (c) If a coefficient v_{i,j_k} of $v_{i,j}$ is equal to 256, then consider 256 as a couple 255 and 1 and write $255x^{k-1} + 1x^k$ as the polynomial $v_{i,j}$.

4. For all other pixels of the secret image, apply Steps 2 and 3.

5. Extend the shadow images to a rectangular array by padding with redundant pixels such that if the gray value of the last pixel of non-extended shadow image is m then all the redundant pixels are of gray value $m + 1$.

The Reconstruction Phase

1. For given k shadow images, find the last pixel value which is different than the consecutive one and reduce them by deleting the redundancy.
2. Take the first l_i pixels of any k shadow images and apply the following steps:
   (a) If any gray value of the first partition of S_j is not 255, the shadow polynomial $v_{i,j}$ is obtained by using first l_i pixels of S_j.
   (b) If the gray value $a_{1,l}$ of the first partition of S_j is equal to 255, then the pixels $a_{1,l}$ and $a_{1,l+1}$ are converted to $(a_{1,l} + a_{1,l+1})\, x^{l-1}$ in the polynomial $v_{1,j}$.
3. Using the k shadow polynomials $v_{1,i_1}, v_{1,i_2}, \ldots, v_{1,i_k}$ and Equation 1, we obtain secret polynomial $s_1(x)$, i.e. we get first s pixels of the secret image.
4. To all pixels of k shadow images, apply Step 1 and 2.

4.3. Algorithm 3 for $GF(2^8)$

The Share Construction

1. Find the field elements corresponding to the gray values in the secret image with using the map ϕ.
2. Choose n polynomials $q_1, q_2, \ldots, q_n$ in $GF(2^8)[x]$ such that $(q_i, q_j) = 1$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$ and $\alpha = \deg(q_{n-k+2} \times q_{n-k+3} \times \cdots \times q_n) < \beta = \deg(q_1 \times q_2 \times \cdots \times q_k)$.
3. The secret polynomials $s_i(x)$ corresponding to i^{th} partition of the secret image are obtained by letting the s coefficients be as the ϕ-image of the gray values of s pixels of i^{th} partition such that $\alpha < \deg(s_i(x)) = s - 1 < \beta$.
4. Using the secret polynomial $s_i(x)$ for i^{th} partition, generate n shadow polynomials $v_{i,j}$ for all $1 \leq j \leq n$ by using Equation 2 and set $l_i = \deg(q_i)$ for $1 \leq i \leq n$.
5. For $1 \leq j \leq n$, calculating ϕ^{-1}-image of the coefficients of the shadow polynomials $v_{i,j}$, construct i^{th} partition of shadow images.
6. For all partitions of the secret image, apply Steps 3, 4 and 5.

Remark: For this construction, all operations are performed over the finite field extension $GF(2^8)$.

Reconstruction Phase

1. For all $1 \leq i \leq n$, generate k shadow polynomials using first l_i pixels of k shadow images.
2. Calculate ϕ-image of the coefficients of the shadow polynomials $v_{1,i_1}, v_{1,i_2}, \ldots, v_{1,i_k}$. For these k polynomials over $GF(2^8)$, applying an Equation 1, determine the secret polynomial $s_1(x)$ over $GF(2^8)$.
3. Calculating ϕ^{-1}-image of the coefficients of the secret polynomials $s_1(x)$, construct first s pixels of secret images.
4. For all other pixels of k shadow images, apply Step 1, 2 and 3.

5. An experimental result

To illustrate Algorithm 1, we design a $(2, 4)$ threshold secret image sharing scheme. The secret image S is chosen as a 256×256 pixels Pepper image shown in Figure 1 (a). To construct the shadow images, we choose relatively prime four polynomials $q_1 = x^4 + 85x^2 + 4x + 23$, $q_2 = x^4 + 54x^3 + 99x^2 + 27x + 105$, $q_3 = 23x^4 + 81x^3 + 201x^2 + 153x + 83$, $q_4 = x^4 + x^3 + 81x^2 + 103$ where the condition $\alpha = 4 < \beta = 8$ is satisfied. We take $s = 8$ so that the size of the shadow images are $1/2$ of the size of the secret image since division of each $s_i(x)$ corresponding to 8 pixels, by $q_j(x)$ gives us a remainder polynomial of degree 3, corresponding to 4 pixels. The shadow images S_1, S_2, S_3, S_4 with respect to the secret image S are illustrated in Figure 1 (b).

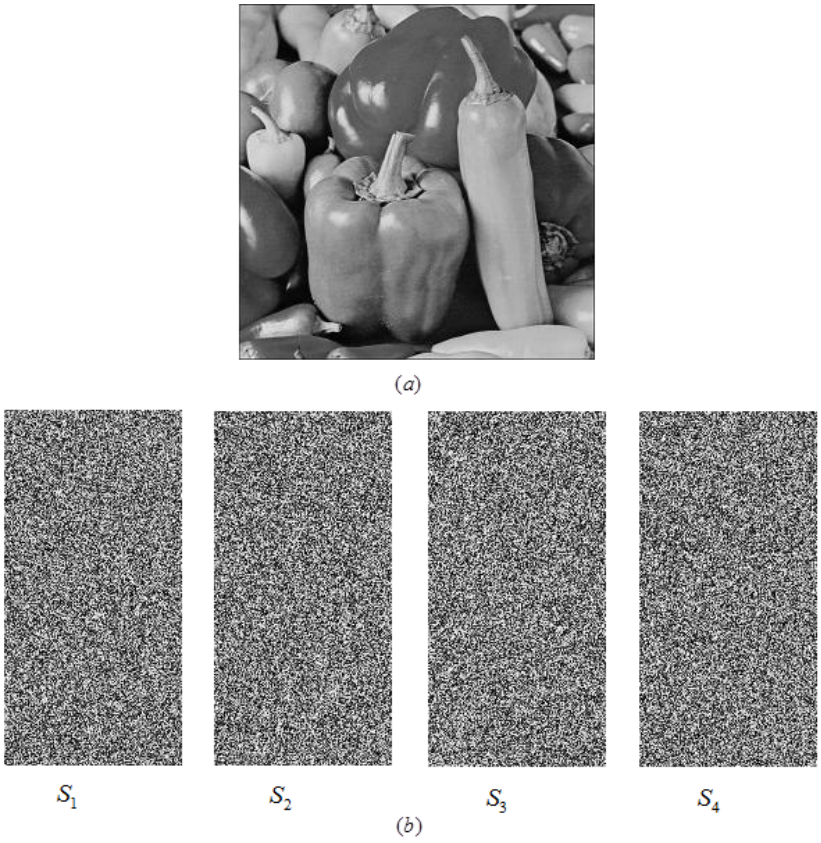


Figure 1: (a) 256×256 Secret Image S; (b) 128×256 Shadow Images S_1, S_2, S_3, S_4

To recover the secret image, a combination of any 2 participants having shadow images is sufficient. This reconstruction is illustrated in Figure 2.

Note that, for (k, n) threshold secret image sharing, if we take the degrees of each polynomial q_i as m and degree of secret polynomial $km - 1$, the size of each shadow image is one-kth of the size of secret image as the construction of Thien and Lin [17]. Further, recently an image sharing method that avoids permutation is introduced in [18]. Our method also differs and presents a more applicable nature compared to [18]. In [18], the shares distributed to the holders are each of sizes 256×256. In our method, the sizes are 128×256 which gives a storage advantage.

We present another illustrative example to show how we can control the size of shares using the same $(2, 4)$ threshold secret image sharing scheme. We can take the irreducible polynomials of degree 5 or 6. By choosing four irreducible polynomials $q_1 = x^5 + 12x^4 + 53x^3 + 177x^2 + 46x + 91, q_2 = x^5 + 132x^4 + 131x^3 +$

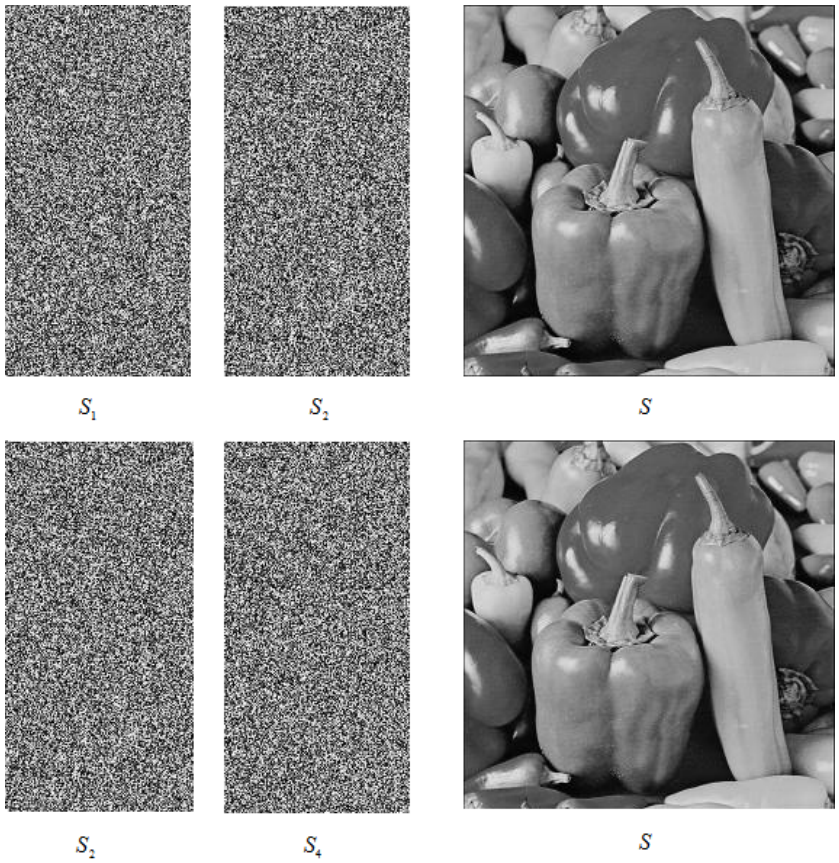


Figure 2: Some Examples of Reconstruction

$117x^2+114x+11, q_3 = x^5+151x^4+175x^3+21x^2+173x+39, q_4 = x^5+151x^4+48x^3+13x^2+164x+145$, we obtain the shadow images of size 160×256 (Figure 3). Also, the size of the shadow images would be 196×256 if the irreducible polynomials were chosen of degree 6.

6. Security analysis

In this section, we show that any $k-1$ or fewer shadow images cannot reconstruct $m \times r$ secret image S. Without loss of generality, suppose that last $k-1$ participants come together to reconstruct the secret image S and that assuming they know how to read the pixels of shadow images. Assume that they want to reconstruct the first partition of the secret image, without loss of generality, they first generate the shadow polynomials $v_{1,n-k+2}, v_{1,n-k+3}, \ldots, v_{1,n}$ by using the first partitions of the shadow images and the secret polynomial $r_1(x)$ corresponding to these shadow polynomials is computed by using CRT such that $\deg(r_1(x)) < \alpha$ where $\alpha = \deg(q_{n-k+2}q_{n-k+3}\ldots q_n)$. Assume that $r_1(x)$ has the maximum degree, i.e., $\deg(r_1(x)) = \alpha - 1$ and secret polynomial of the first partition of secret image $s_1(x)$ has minimum degree, i.e., $\deg(s_1(x)) = \alpha + 1$. It is easily seen that $s_1(x) = r_1(x) + \gamma_1(x)(q_{n-k+2}q_{n-k+3}\cdots q_n) \pmod p$ for some $\gamma_1(x) \in GF(p)$, where p is either 251, 256 or 257. This means that the probability of finding the right polynomial is $1/p^2$ at the best. Since, the secret image S has $m \times r/s$ partitions, the probability of reconstruction the right image is $\left(1/p^2\right)^{m\times r/s}$ at the best. For the given example, the probability of obtaining the right image is $\left(\frac{1}{251^4}\right)^{256\times 32} \approx \left(\frac{1}{2}\right)^{261212}$. Furthermore, we assume that the

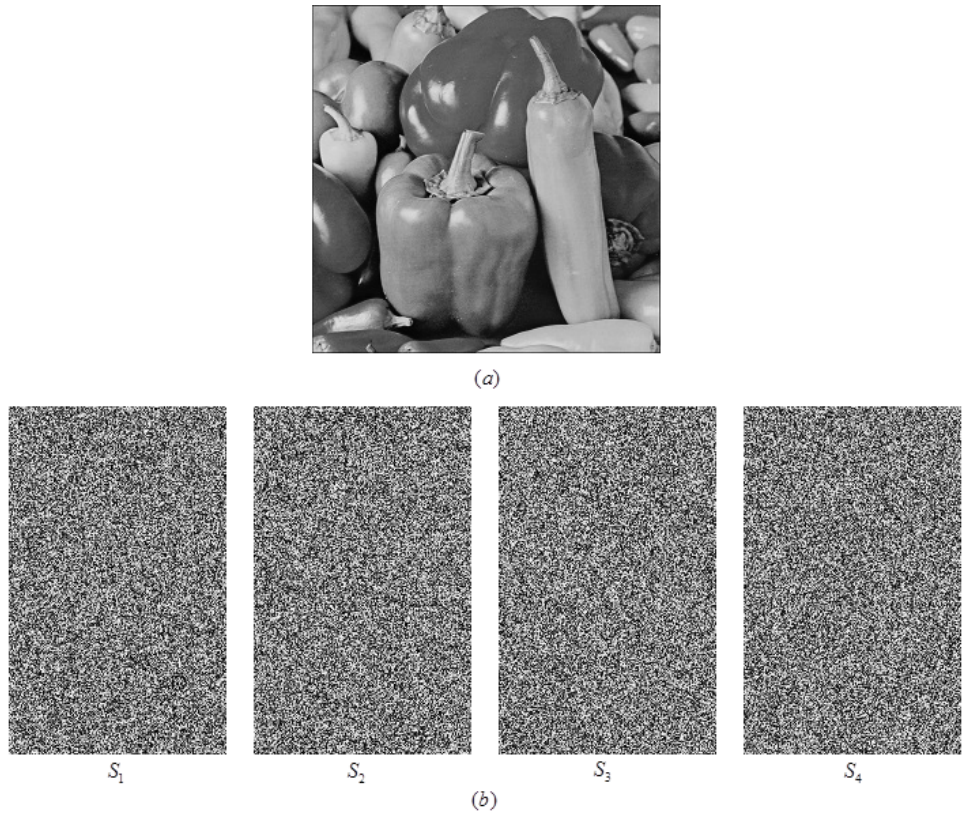


Figure 3: (a) 256×256 Secret Image S; (b) 160×256 Shadow Images S_1, S_2, S_3, S_4

person who wants to reconstruct the secret image knows the size of partition of shadow images and secret image. If an unauthorized person does not hold into this information, then the problem becomes more infeasible to solve.

It is clear that, as a special case of our construction, if we choose the degrees of polynomials q_i as m and the secret polynomial $km - 1$, then our construction and [17] have the same security level.

We present some results of another example where the secret image S is chosen as a 512×512 pixels Pepper image. The histograms of the original picture and the shares are provided in Figure 4. It is observed that the shares have a very uniform histograms. We would like to point out that getting uniformly distributed encrypted images is a problem by itself and some other techniques besides are used in order to be successful ([7, 15]). Here, we do not employ additional tools in order to get this achievement.

Also we have computed the entropy of the original image and the shares S_1, S_2, S_3 and S_4 as 7.5937, 7.9700, 7.9700, 7.9701, 7.9702 respectively. The last four evaluations that correspond to the shares are close to 8 which point to a good entropy level. Further, the Structural Similarity Index Measure (SSIM)[20] is applied between the shares that solve the problem (we recall that two of them solve the original image) and the original image and these results are given in Table 1. The results in Table 1 show that SSIM is close to zero which also gives a promising result.

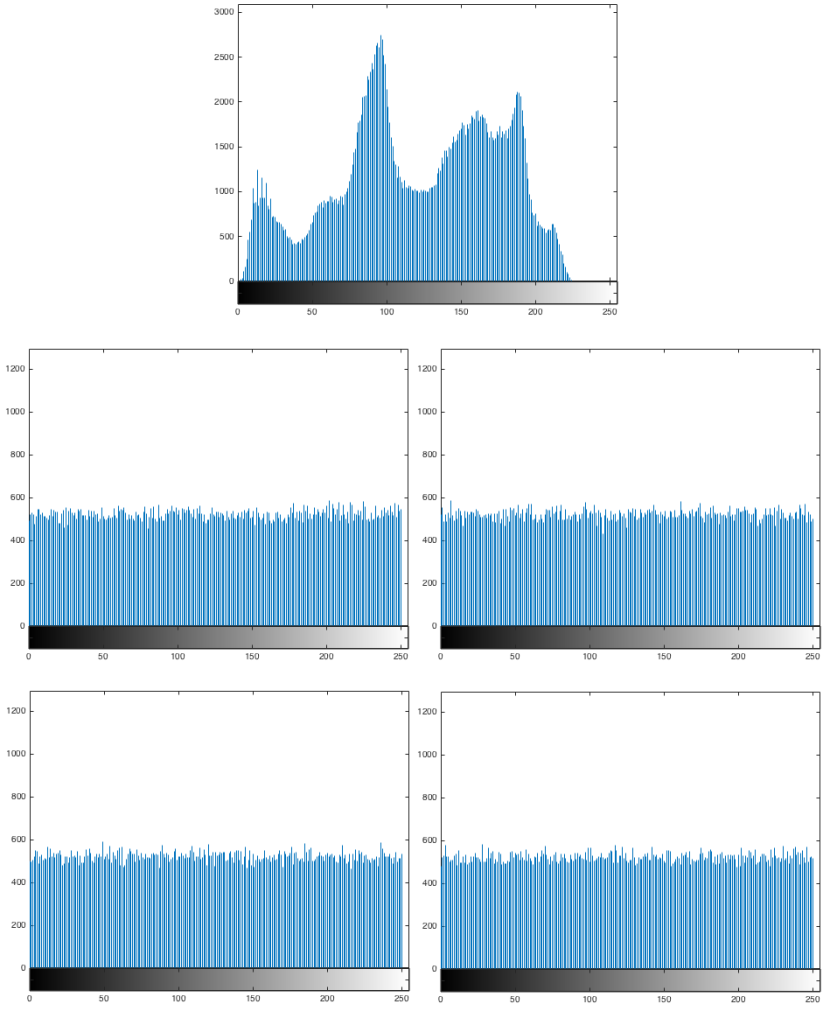


Figure 4: Histogram of 512×512 Original Image (OI); Histograms of 256×512 Shadow Images S_1, S_2, S_3, S_4 respectively

Share Images	SSIM
S_1 and S_2	-2.6959×10^{-04}
S_1 and S_3	-3.2801×10^{-04}
S_1 and S_4	-7.0751×10^{-05}
S_2 and S_3	2.7211×10^{-04}
S_2 and S_4	5.2297×10^{-04}
S_3 and S_4	5.2318×10^{-04}

Table 1: SSIM of shares and the original image.

We present the performance comparison between these three algorithms over the above example graphically (Figure 2). The graph shows the elapsed time of the secret sharing process over the various finite fields. (A 2.5 GHz processor and 8.00 GB RAM standard computer over MATLAB R2015b is used.) As seen, the performance over $GF(256)$ is slower than the other fields. This is due to the algebraic manipulations over the extension field. On the other hand, there is no meaningful difference between the

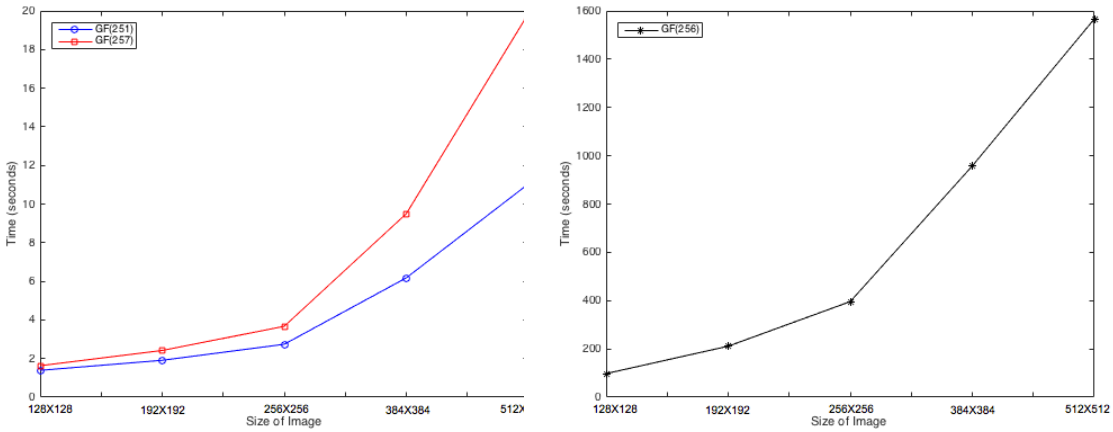


Figure 5: Elapsed time of secret sharing process over the various fields

Table 2: Comparison of Secret Image Sharing Methods

SIS	Entropy				Size	Needing
	S_1	S_2	S_3	S_4		
SC	7.8942	7.8942	7.8942	7.8942	256×512	PRN Padding
TL	7.9080	7.9655	7.9624	7.9696	256×512	Permutation
OTS	7.9700	7.9700	7.9701	7.970	256×512	No Need

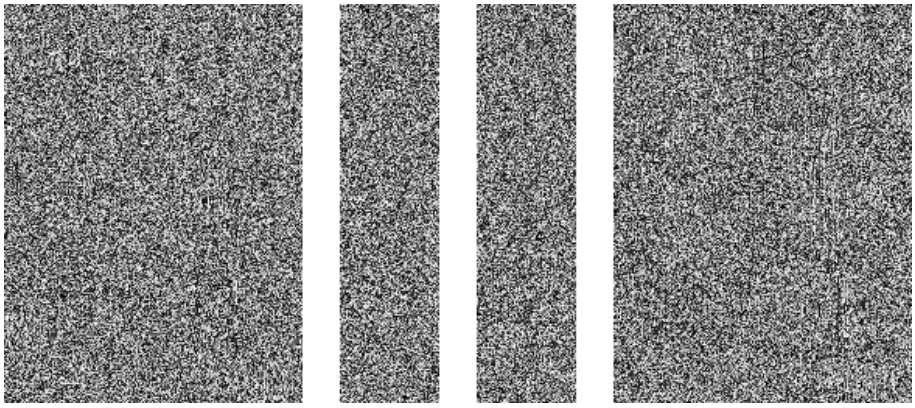
other two prime fields and algorithms are faster compared to the extension field $GF(256)$.

7. A comparison with other schemes

We show the efficiency of our scheme (OTS) by comparing it with the threshold secret image sharing (SIS) schemes introduced in [13] (SC) and [17] (TL). The entropies and sizes of shadow images are given in Table 2. The entropies of shadow images constructed by our scheme are closer to 8 which indicates the reliable security of the system, despite our scheme does not need any permutation or random numbers padding. Without applying a permutation, the original image is still perceptible by naked eye after (2,4) secret image sharing using the scheme of [17]. We also derive the same security level with [17] without using a permutation which is also required to be shared as a secret. The sizes of the shadow images are all half of the size of the original image for given applications. However, as distinct from others, the sizes of the shadow images can differ in our scheme. Further, by waiving the scheme to be threshold, we can improve the flexibility of the system and discriminate the participants for authorization as shown in the next illustrative example. By choosing four irreducible polynomials $q_1 = x^6+10x^5+75x^4+23x^3+64x+3$, $q_2 = 5x^2+3$, $q_3 = 215x^2+157$ and $q_4 = x^6+101x^5+250x^4+123x^3+99x+231$, we obtain the shadow images of sizes 196×256, 64×256, 64×256 and 196×256 respectively (Figure 6). Also, a shadow image would be of size 160×256 for an irreducible polynomial of degree 5 or 96×256 for an irreducible polynomial of degree 3. The shadow images S_2 and S_3 cannot reconstruct the secret image S, for instance.

On the other hand, the scheme given in [13] is not as flexible as our scheme. For instance, 512×512 pixels gray color image forces us to choose d as a power of 2 and hence q_is which are smaller than 255 as given in the example forces us to choose $d = 8$, in order to design a (2,4) threshold scheme. Therefore, the sizes of shadow images will be the same as the original image. Besides, the choice of q_is are not

(a)



(b)

Figure 6: Secret Image S (a) and Shadow Images S_1 of size 196×256, S_2 of size 64×256, S_3 of size 64×256 and S_4 of size 196×256 respectively (b)

so independent for a secret image sharing since the pixel values of an image are determined in a fixed spectrum. Further, the histograms of shadow images may give an information about q_is.

8. Conclusion

In this study, we generalize Mignotte's scheme over Euclidean domains and present a new threshold secret image sharing. We show that Mignotte's generalized construction over Gaussian integers has higher security level than Mignotte's construction over integers. We also give threshold secret image sharing algorithms for primes $p = 251$, $p = 257$ and over Galois field $GF(256)$. One of the advantages of these algorithms is that there is no need to apply a permutation which needs to be known by all participants permutation as in [17] or add a random value as in [13]. Unlike [17], in our scheme, one can choose arbitrarily the number of pixels s which is the length of each partition that the secret image divided into, providing that s divides r for an $m \times r$ secret image to construct (k, n) scheme and so the choice of k which is the minimum number of participants who can reconstruct the secret is flexible. Unlike [13] and [17], the sizes of the shadow images can differ and so this increases the applicability and the security. We also show that finding the secret image for unauthorized person is an infeasible problem. Furthermore, in [16] there is a restriction on the degree of the irreducible polynomials which narrows the selection choice

of such polynomials to be applied. Here, we do not impose such a restriction which makes the scheme more practical and secure. We finally realize our proposed method over an example which illustrates the new algorithm.

References

[1] C. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inform. Theory 29(2) (1983) 208–210.
[2] G. R. Blakley, Safeguarding cryptographic keys, Proc. Am. Federation of Information Processing Soc. (AFIPS'79) National Computer Conf. 48 (1979) 313–317.
[3] P. Dingyi, S. Arto, D. Cunsheng, Chinese Remainder Theorem: Applications in Computing, Coding,Cryptography, World Scientific, 1996.
[4] T. Hungerford, Abstract Algebra: An Introduction, Cengage Learning, Boston, 2012.
[5] S. Iftene, General secret sharing based on the Chinese Remainder Theorem with applications in E–Voting, Electronic Notes in Theoretical Computer Science 186 (2007) 67–84.
[6] E. V. Krishnamurthy, Error–Free Polynomial Matrix Computations, Springer Science and Business Media, New York, 2012.
[7] J. B. Lima, R. M. Campello de Souza, Histogram uniformization for digital image encryption, 25th SIBGRAPI Conference on Graphics, Patterns and Images (2012) 55–62.
[8] P. K. Meher, J. C. Patra, A new approach to secure distributed storage, sharing and dissemination of digital image, IEEE International Symposium on Circuits and Systems (2006) 373-376.
[9] M. Mignotte, How to share a secret,In: Cryptography, EUROCRYPT 1982, Lecture Notes in Computer Science 149 (1983) 371–375.
[10] M. Naor, A. Shamir, Visual cryptography, In: Advances in Cryptology–EUROCRYPT 1994, Lecture Notes in Computer Science 950 (1994) 1–12.
[11] O. Ore, The general Chinese remainder theorem, The American Mathematical Monthly 59(6) (1952) 365–370.
[12] A. Shamir, How to share a secret, Comm. ACM 22(11) (1979) 612–613.
[13] S. J. Shyu, Y. R. Chen, Threshold secret image sharing by Chinese remainder theorem,IEEE Asia–Pacific Services Computing Conference (2008) 1332–1337.
[14] D. R. Stinson, An explication of secret sharing schemes, Des. Codes Cryptogr. 2(4) (1992) 357–390.
[15] S. Somaraj, M. A. Hussain, Performance and Security Analysis for Image Encryption using Key Image, Indian Journal of Science and Technology 8(35) (2015).
[16] G. Tatyana, M. Genadii, Generalized Mignotte's sequences over polynomial rings, Electronic Notes in Theoretical Computer Science 186 (2007) 43–48.
[17] C. C. Thien, J. C. Lin, Secret image sharing, Comput. Graph. 26(5) (2002) 765–770.
[18] G. Ulutas, M. Ulutas, V. Nabiyev, Secret sharing scheme based on Mignotte's scheme, 2011 IEEE 19th Signal Processing and Communications Applications Conference (2011) 291–294.
[19] R. Z. Wang, C. H. Su, Secret image sharing with smaller shadow images,Pattern Recognition Lett. 27(6) (2006) 551–555.
[20] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Transactions on Image Processing 13(4) (2004) 600–612.