LUPINE PUBLISHERS
Open Access

Current Trends in Computer Sciences & Applications

DOI: 10.32474/CTCSA.2018.01.000106

ISSN: 2643-6744

Research Article

An Image Secret Sharing Method Based on Shamir Secret Sharing

Selda Calkavur[1]* and Fatih Molla[2]

[1]*Department of Mathematics, Turkey*

[2]*Faculty of Information, Turkey*

Received: November 12, 2018; **Published:** November 20, 2018

***Corresponding author:** Selda Calkavur, Department of Mathematics, Turkey

Abstract

This paper presents an image secret sharing method based on Shamir secret sharing method. We use the matrix projection to construct secret sharing scheme. A secret image to be divided as n image shares such that:

i) Any k image shares (k ≤n) can be used to reconstruct the secret image in lossless manner and

ii) Any (k-1) or fewer image shares cannot get sufficient information too reveal the secret image.

It is an effective, reliable and secure method to prevent the secret image from being lost, stolen and corrupted. In comparison with other image secret sharing method this approach's advantages are its strong protection of the secret image and its ability for real time processing.

Keywords: Image secret sharing; Finite field; Matrix projection

Introduction

The effective and secure protection for important message is a primary concern in commercial and military applications. Numerous techniques, such as image hiding and watermarking, were developed to increase the security of the secret. The secret image sharing approaches are useful for protecting sensitive information [1]. The main idea of secret sharing is to transform an image into n shadow images that are transmitted and stored separately. The original image can be reconstructed only if the shadow images that participated in the revealing process from a qualified set [2]. The (k; n)-threshold image sharing schemes were developed to avoid the single point failure. Hence the encoded content is corrupted during transmission. In these schemes, the original image can be revealed if k or more of these n shadow images are obtained. Moreover, the users who with complete knowledge of k 1 shares cannot obtain the original image. Blakley [3] & Shamir [4] independently proposed original concepts of secret sharing in 1979. In these (k; n)-threshold schemes encode the input data D into n shares, which are then distributed among k recipients. D can be reconstructed by anyone who obtains a predefined number k, where 1 k n, of the images.

Noar & Shamir [5,6] extended the secret sharing concept into image research and referred it as visual cryptography. Visual cryptography requires stacking any k image shares (or shadow images) to show the original image without any cryptographic computation. The disadvantages are

i) Image shares have larger image size compared to the size of the original secret image and

ii) The contrast ratio in the reconstructed image is quite poor [7].

A better image secret sharing approach was presented by Thien & Lin [1]. They used Shamir's secret sharing scheme to share a secret image with some cryptographic computation. The method significantly reduces the size of the secret image and the secret image can be reconstructed with good quality. Ramp secret sharing schemes are another types of secret sharing schemes [8-11]. In ramp schemes, a secret can be shared among a group of participants in such way that only sets of at least k participants can reconstruct the secret and k1 participants cannot [12]. The rest of this paper is organized as follows. Section II reviews the Shamir's scheme. The proposed secret image sharing method and experimental results are given in Section III. It is also explained the advantages of proposed scheme in this section. The last section collects concluding remarks.

Review of shamir's secret sharing scheme

Shamir [4] developed the idea of a (k, n)-threshold based secret sharing technique (k ≤n). The technique allows a polynomial function of order (k -1) constructed as,

$f(x) = s_0 + s_1(x) + s_2(x^2) + ... + s_{k-1}x^{k-1} (\text{mod } p)$, where the value of s0 is the secret and p is a prime number. The secret shares are the pairs of values (x_i, y_i) where, $y_i = f(x_i), 1 \le i \le n$ and $0 \le x_1 1 \le x_2 \le .....x_n \le p-1$. The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (xi, yi) so that no single shareholder knows the secret value s_0 [7]. Actually, no groups of (k 1) or fewer secret shares can discover the secret s_0. That is when k or more secret shares are available, then we may set at least k linear equations $y_i = f(x_i)$ for the unknown s_i's. The unique solution to these equations shows that the secret value s_0 can be easily obtained by using Lagrange interpolation [4].

Proposed Method

In this section, we examine the application of some secret sharing schemes. We have worked a new approach to construct secret sharing schemes based on field extensions in [13]. In this paper, we generalise the results of [13].

The application of some secret sharing schemes

Digital image consists of by transporting images in the nature through the agency of sensors to the computer. Digital images are sampled signals at regular intervals. These sampling points are called the pixel. The image is a two dimensional matrix which consists of pixels. It should be determined that how many bits of each pixel value will be stored when this matrix is constructed. This value is called the bit depth. For an image with a bit depth of 8, the maximum value that a pixel can have is 255. In general, it is used 3 bands to obtain a color picture. These bands have same size and each matrix represents a different color component. Each color component corresponds to red, green and blue.

Proposed scheme

Consider the matrix I is an image with height of h and wideness of w. The height corresponds to row number of matrix and the wideness corresponds to column number. Let the secret space be Mq for a pixel, where

$M_q = \{a \mid 0 \le a \le q-1, a \in Z\}$. This set consists of the elements of the matrix I. Let the secret be the image I and the threshold structure be (k; n). In this case, it can be constructed a secret sharing scheme as follows.

$$I = \left[a_{ij}\right] = \begin{bmatrix} a_{11} & a_{12}..... & a_{1w} \\ \vdots & \vdots & \vdots \\ a_{h1} & a_{h2}..... & a_{hw} \end{bmatrix}_{h \times w}, a_{ij} \in M_q$$

The matrix P(x) is generated which consisting of height of h and wideness of $\left[\frac{w}{k-1}\right]$ by using I.

$$p(x) = \left[p_{ij}(x)\right] = \begin{bmatrix} p_{11}(x) & p_{12}(x)\cdots & p_{1w'}(x) \\ \vdots & \ddots & \vdots \\ p_{h'1}(x) & p_{h'2}(x) & p_{h'w'}(x) \end{bmatrix}, h' = h, w' = \left[\frac{w}{k-1}\right]$$

$$p_{ij}(x) = rx^{k-1} + \sum_{t=0}^{k-2} a_{i'j'}x^t \in M_q[x], i' = i, j' = (j-1).(k-1) + (k-t), r \in M_q - \{0\}$$

The a_{ij} entry corresponds to i th row and j th column of matrix I. It is clear that the degree of polynomial pij is (k -1). The columns of the matrix I are divided into pieces that has length of (k -1). j th piece in the i th row is represented by the vector $H_{ij} = \{h_1; h_2.... h_{k-1}\}$. It is used the vector H_{ij} to construct the element $p_{ij} = (1 \le i \le h', 1 \le j \le w')$ of the matrix p(x). The first entry of H_{ij} is located i th row and [(j - 1) (k - 1) + 1] th column of the matrix I. The leading coefficient of polynomial $p_{ij}(x)$ is randomly chosen from Mq – {0}. The coefficient of term which is the degree of $t = (0 \le t \le k-2)$ of polynomial pij(x) is chosen as (k - t -1) th element of H_{ij}. This corresponds to [(j - 1) (k - 1) + (k - t)] th column in the i^{th} row. The matrix P(x) is written as the elements of matrix T(x) by using Algorithm 1 [13].

$$T(x) = \begin{bmatrix} t_{11}(x) & t_{12}(x)..... & t_{1w'}(x) \\ \vdots & \ddots & \vdots \\ t_{11}(x) & t_{11}(x)..... & t_{11}(x) \end{bmatrix}, t_{ij}(x) \in \left(GF(q)\right)[x]$$

It is determined an ID number for each participant. The secret piece is obtained by equality (5) for each participant and $u_i = M_q (1 \le i \le n)$. These ID numbers are transformed to the $v_i = GF(q) (1 \le i \le n)$.

by Algorithm 1 [13]. Then the matrix $R_i = ((1 \le i \le n))$. is transformed to the matrix T(x) as follows. $R_i = T(v_i), 1 \le i \le n$

$$R_i = \begin{bmatrix} t_{11}(v_i) & t_{12}(v_i)..... & t_{1w'}(v_i) \\ \vdots & \ddots & \vdots \\ t_{h'1}(v_i) & t_{h'2}(v_i)..... & t_{h'w'}(v_i) \end{bmatrix}_{h' \times w'}$$

This polynomial matrix is written as the matrix Yi by using Algorithm 2 [5].

$$Y_i = \begin{bmatrix} a_{11} & a_{12}.... & a_{1w'} \\ \vdots & \ddots & \vdots \\ a_{h'1} & a_{h'2} & a_{h'w'} \end{bmatrix}_{h' \times w'}$$

Secret retrieval procedure

To reach the secret, at least k pieces of secret must be known. On the other hand, the number of elements of $W = \{u_i \mid t_i \in M_q - \{0\}, 1 \le i \le n\}$ must be at least k. In the ordered pair $(u_{t_i}; Y_{u_{t_i}})$; the ordered of participant in the W is denoted by i, the order of the set of participant of t_i th participant in the W is denoted

by u_{t_i}. $Y_{u_{t_i}}$ is the secret piece which is given to participant with ID of u_{t_i}. These ordered pairs are transformed to the ordered pairs $(v_{t_i}; R_{u_{t_i}})$ by using algorithm 1 in [13]. It is used to Lagrange Interpolation for the ordered pairs $(v_{t_i}; R_{u_{t_i}})$. Hence it is obtained the matrix T(x) again. Then it is found the matrix P(x). The image is constructed with the coefficients of this polynomial.

Example. Let the secret space be M256 and the irreducible polynomial be $f(x) = x^8 + x^4 + x^3 + x^2 + 1 \in (GF(2))[x]$ to construct GF (256). It can be constructed a (3; 5)-threshold schemes by using the following matrix I.

$$I = \begin{bmatrix} 254 & 241 & 189 & 189 & 241 & 254 \\ 254 & 189 & 254 & 254 & 189 & 254 \\ 197 & 210 & 210 & 210 & 210 & 197 \\ 178 & 192 & 209 & 209 & 192 & 178 \\ 172 & 186 & 196 & 196 & 186 & 172 \\ 157 & 168 & 168 & 168 & 168 & 157 \end{bmatrix}_{6\times 6}.$$

The matrix P(x) can be constructed as follows. The leading coefficient is randomly selected and the other coefficients are chosen from matrix I.

$$P(x) = \begin{bmatrix} (2x^2 + 254x + 241) & (8x^2 + 189x + 189) & (64x^2 + 241x + 254) \\ (128x^2 + 254x + 189) & (x^2 + 254x + 254) & (8x^2 + 189x + 254) \\ (16x^2 + 197x + 210) & (128x^2 + 210x + 210) & (28x^2 + 210x + 197) \\ (196x^2 + 178x + 192) & (57x^2 + 209x + 209) & (59x^2 + 192x + 178) \\ (x2 + 172x + 186) & (159x^2 + 196x + 196) & (56x^2 + 186x + 172) \\ (244x^2 + 157x + 168) & (209x^2 + 168x + 168) & (170x^2 + 168x + 157) \end{bmatrix}$$

The coefficient of polynomial in the matrix P(x) is moved to GF(256). Therefore, it is obtained the elements of matrix T(x) = [tij(x)]; (t(x) 2 (GF(q))[x]).

$$t_{11}(x) = (\theta)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + 1)$$
$$t_{12}(x) = (\theta^3)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)x + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)$$
$$t_{13}(x) = (\theta^6)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + 1)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{21}(x) = (\theta^7)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)$$
$$t_{22}(x) = (1)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{23}(x) = (\theta^3)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{31}(x) = (\theta^4)x^2 + (\theta^7 + \theta^6 + \theta^2 + 1) + (\theta^7 + \theta^6 + \theta^4 + \theta)$$
$$t_{32}(x) = (\theta^7)x^2 + (\theta^7 + \theta^6 + \theta^4 + \theta)x + (\theta^7 + \theta^6 + \theta^4 + \theta)$$
$$t_{33}(x) = (\theta^4 + \theta^3 + \theta^2)x^2 + (\theta^7 + \theta^6 + \theta^4 + \theta)x + (\theta^7 + \theta^6 + \theta^2 + 1)$$
$$t_{41}(x) = (\theta^7 + \theta^6 + \theta^2)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta)x + (\theta^7 + \theta^6)$$
$$t_{42}(x) = (\theta^5 + \theta^4 + \theta^3 + 1)x^2 + (\theta^7 + \theta^6 + \theta^4 + 1)x + (\theta^7 + \theta^6 + \theta^4 + 1)x$$
$$t_{43}(x) = (\theta^5 + \theta^4 + \theta^3 + \theta + 1)x^2 + (\theta^7 + \theta^6)x + (\theta^7 + \theta^5 + \theta^4 + \theta)$$
$$t_{51}(x) = (1)x^2 + (\theta^7 + \theta^5 + \theta^3 + \theta^2) + (\theta^7 + \theta^5 + \theta^3 + \theta)$$
$$t_{52}(x) = (\theta^7 + \theta^4 + \theta^3 + \theta^2 + \theta + 1)x^2 + (\theta^7 + \theta^6 + \theta^2) + (\theta^7 + \theta^6 + \theta^2)$$
$$t_{53}(x) = (\theta^5 + \theta^4 + \theta^3)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta)x + (\theta^7 + \theta^5 + \theta^3 + \theta^2)$$
$$t_{61}(x) = (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^2)x^2 + (\theta^7 + \theta^4 + \theta^3 + \theta^2 + 1)x + (\theta^7 + \theta^5 + \theta^3)$$
$$t_{62}(x) = (\theta^7 + \theta^6 + \theta^4 + 1)x^2 + (\theta^7 + \theta^5 + \theta^3)x + (\theta^7 + \theta^5 + \theta^3)$$
$$t_{63}(x) = (\theta^7 + \theta^5 + \theta^3 + \theta)x^2 + (\theta^7 + \theta^5 + \theta^3)x + (\theta^7 + \theta^4 + \theta^3 + \theta^2 + 1)$$

Let the IDs of participants be $u_1 = 1$, $u_2 = 2$, $u_3 = 3$, $u_4 = 4$ and $u_5 = 5$. These elements correspond to $v_1 = 1, v_2 = \theta, v_3 = \theta + 1, v_4 = \theta^2$ and $v_5 = \theta^2 + 1 \in GF(256)$

The pieces of participants are as follows.

$$R_1 = T(1)$$
$$R_2 = T(\theta)$$
$$R_3 = T(\theta + 1)$$
$$R_4 = T(\theta^2)$$
$$R_5 = T(\theta^2 + 1)$$

These elements correspond to the following matrices in M256.

$$Y_1 = \begin{bmatrix} 13 & 8 & 79 \\ 195 & 1 & 75 \\ 7 & 128 & 11 \\ 182 & 57 & 73 \\ 23 & 159 & 46 \\ 193 & 209 & 159 \end{bmatrix}, Y_2 = \begin{bmatrix} 24 & 250 & 28 \\ 102 & 27 & 185 \\ 5 & 81 & 12 \\ 142 & 138 & 195 \\ 251 & 23 & 37 \\ 120 & 134 & 66 \end{bmatrix}, Y_3 = \begin{bmatrix} 228 & 79 & 173 \\ 24 & 228 & 12 \\ 208 & 3 & 194 \\ 248 & 98 & 56 \\ 86 & 76 & 167 \\ 17 & 255 & 64 \end{bmatrix}$$

$$Y_4 = \begin{bmatrix} 14 & 243 & 105 \\ 138 & 49 & 176 \\ 252 & 85 & 119 \\ 238 & 5 & 2 \\ 32 & 246 & 217 \\ 29 & 163 & 117 \end{bmatrix}, Y_5 = \begin{bmatrix} 242 & 70 & 216 \\ 244 & 206 & 5 \\ 41 & 7 & 185 \\ 152 & 237 & 249 \\ 141 & 173 & 91 \\ 116 & 218 & 119 \end{bmatrix}$$

At least 3 participants can recover the image by combining their shares by using Lagrange Interpolation in [13]. It is seen that the original secret image in Figure (1a) and the secret pieces are seen (1b-1d). Reconstructed image is seen in Figure (1f).

Advantages

It is known that a file in the computer environment can be expressed with a bit string. A bit string consists of 8 bits is called a byte. A byte gets value in the range (0-255) and is an element of M256. A file D consisting of m bytes can be expressed as a vector such that D = (a_1 a_2..... am) $(a_i \in M_q)$. Consider any file (text, image, video, etc.) by using the proposed scheme, the file is also secret. The operations an secret sharing schemes can be applied to this file. The participants know that the secret is the image. The secret sharing scheme is defined over GF(256). So it is a lossless scheme. As in the Shamir's scheme if the operations were done in GF(251), then the large values of 250 would be lost. That is the file will be corrupted. So, the entire file could be lost. At result the image could not reconstruct again.

Conclusion

We proposed an image secret sharing method based on Shamir secret sharing. We have two techniques. i) Secret sharing scheme using matrix projection and ii) Shamir's secret sharing scheme. A secret image can be successfully reconstructed from any k image shares but cannot be revealed from any (k-1) or fewer image shares. The size of image shares is smaller than the size of the secret image. Our scheme is defined over GF(256). So it is a lossless scheme. This is another advantage of our scheme. So the proposed scheme stands well, in terms of security.

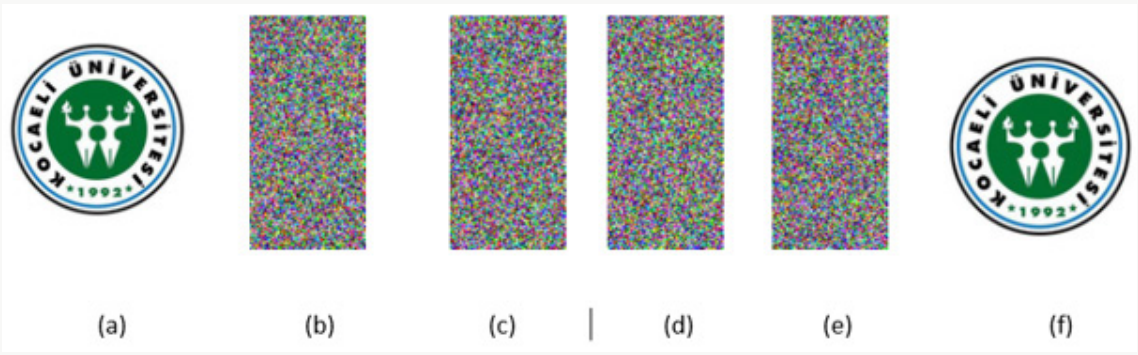

Figure 1: (3; 4) Secret image sharing scheme.

References

1. Thien CC, Lin J C (2002) Secret image sharing. Computer Graphics 26(5): 765–770.
2. Wu KS (2013) A secret image sharing scheme for light images. EURASIP Journal of Advantages in Signal Processing.
3. Blakley GR (1979) Safeguarding cryptographic keys. In: Proceedings of AFIPS 1979 National Computer Conferance. USA, pp. 313–317.
4. Shamir A (1979) How to share a secret. Commun. ACM 22(11): 612–613.
5. Naor M, Shamir A (1997) Visual cryptography ii: Improving the contrast via the cover base. In Security Protocols 1189: 197-202.
6. Naor M, Shamir A (1995) Visual cryptography. In Advances in Cryptology - EUROCRYPT'94. Berlin.
7. Bai L, Biswas S, Ortiz A, Dalessandro D (2006) An image secret sharing method. In 9th International Conference on Information Fusion. Italy.
8. Kurosawa K, Okada K, Sakano K, Ogata W, Tsujii S (1994) nonperfect secret sharing schemes and matroids. In Advances in Cryptology. Berlin.
9. Ogata W, Kurosawa K (1998) Some basic properties of general nonperfect secret sharing schemes. Journal of Universal Computer Science 4(8): 690-704.
10. Paillier P (1997) On ideal non-perfect secret sharing schemes. In Security Protocols Workshop: 207-216.
11. Srinathan K, Rajan NT, Rangan CP (2002) Non-perfect secret sharing over general access structures. In Progress in Cryptology -INDOCRYPT 2002: 409-421.
12. Jackson WA, Martin K (1996) A combinatorial interpretation of ramp schemes.
13. Molla FC, Alkavur S (2018) A new approach to construct secret sharing schemes based on field extensions. European Journal of Pure and Applied Mathematics.

DOI: 10.32474/CTCSA.2018.01.000106