GU J Sci, Part A, 6(3): 51-60 (2019)

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Geometry Based Conjunctive Hierarchical Threshold Secret Image Sharing Scheme

Vasif V. NABIYEV[1], Katira SOLEYMANZADEH[2,*]

[1]*Karadeniz Technical University, Department of Computer Engineering, 61080, Trabzon, Turkey*
[2]*Ege University, International Computer Institute, 35100, İzmir, Turkey*

Article Info

Received: 12/04/2018
Accepted: 26/09/2019

Keywords

Geometry projective
Hierarchical access structure
Information security
Secret image sharing
Small shadow size

Abstract

In hierarchical secret sharing scheme (HSSS), the secret is shared among participants with different privileges that are distributed into distinct levels. Although HSSS has been proposed by several researchers, none of them have been used geometry characteristics to define conjunctive hierarchical secret image sharing (HSIS) scheme. Moreover, small shadow images have important role in transmission over the network and also in storage demand. The main objective of this paper is to propose conjunctive HSIS scheme based on generalized Blakley's projective geometry scheme with small size of shadow images.

1. INTRODUCTION

A secret sharing (SS) scheme is a method of sharing a secret among a finite number of participants. SS is applied when there is a lack of confidence in one person or when the absence of one person does not influence authorization of recovering the secret. Only the authorized subset of participants can reconstruct the secret by pooling together their shadows, while all unauthorized subsets of participants should not gain any information about the secret. The set of all authorized subsets of the participants is called the "access structure" (that is notated as Γ) of the SS scheme; it has the monotonic property, i.e., if $A \in \Gamma$ and $A \subseteq B$ then $B \in \Gamma$.

There is a type of SS, called threshold SS, where all participants have the same priority to reconstruct the secret. A *(t,n)* threshold SS is a way to share a secret between *n* participants, such that every *t* distinct participants $t \leq n$ could recover the secret while any *t-1* or fewer participants cannot do so, which means these schemes are perfect. The threshold scheme for secret sharing was introduced by G.R. Blakley [1] and A. Shamir [2] . Construction of these schemes is based on finite geometry and polynomial interpolation respectively.

Blakley and Shamir's schemes have found many applications in recent years and are suitable for groups of participants who have the same privilege of trust, i.e., sharing a map of treasure or sharing sensitive images which are transmitted via the internet. However, there are some other applications of SS schemes for which the access structures do not suitable for the model of *(t,n)* threshold schemes, in which case some participants have more authority due to their position. For example, consider shared password scenario of the classified documents folder of a government. The password is shared among government members; president, vice president and prime minister who are in highest level of governing system and other ministers who are in the second level. According to government policy,

[*] Corresponding author, e-mail: katirasole@gmail.com

three members are required for recovering the folder's password, but at least two of them must be from highest level. This special setting of SS is called the HSSS.

The problem of multilevel (or hierarchical) SS was considered by several authors. Shamir has suggested that some settings of HSSS can be accomplished by giving more shadows to higher level participants [2]. This scheme is called weighted threshold SS scheme. Simmons considered a general hierarchical SS scheme that is based on Blakley's geometric construction [3]. Consider again the scenario of the previously mentioned example; in the access structure defined by Simmons the participants of the highest level can be substituted by the lower level participants to recover the secret [3]. This scenario is called disjunctive HSSS. However, Tassa considered another scenario in which presence of pre-defined threshold number of higher-level participants are mandatory which is called conjunctive HSSS [4].

Visual SS scheme was proposed by Naor and Shamir based on the concept of threshold SS scheme, in which the secret is a black and white image that is shared into n shadows [5]. Afterwards, Thien and Lin proposed a secret image sharing scheme based on Shamir's scheme [6]. Since the authors split secret image into t disjoint group of pixel, the size of each shadow image is smaller than the secret image. However, the prime number requirement in Shamir's method lead us to use 251 since it is the greatest prime number less than 255 for 8-bit depth gray level images; all the gray values between 251 and 255 are truncated to 250. Every calculated number is the modulus result of this prime number. To get the lossless reconstructed image, Thien and Lin offer a method that slightly increases the size of the shadow image. After truncation, if the value of pixel p_i is bigger than 250, divide into two values 250 and p_i *-250* and store it in array and then share the secret image. However, the increase is usually small because quite often there are only a few pixels whose gray values are 251–255.

In this study, we propose HSIS scheme based on generalized Blakley's projective geometry scheme. Since small size of shadow images have advantages in both transmission time and storage space, we utilize XOR operation to reduce the shadows size. This paper is organized as follows: Related works are given in Section2. Section 3 reviews some preliminaries about disjunctive and conjunctive hierarchical access structure and Blakley's scheme. Section 4 describes our proposed geometry based hierarchical secret sharing scheme. A conjunctive hierarchical secret image sharing scheme is proposed in Section 5. Experimental results are given in Section 6. The security analysis of our proposed scheme are given in Section 7. Finally, in Section 8 we discuss our conclusions.

2. RELATED WORK

Two types of HSSS are mentioned in introduction: disjunctive and conjunctive. Tassa's conjunctive HSSS is based on Birkhoff interpolation. Tassa's scheme is generalized form of Shamir's scheme in which less information about the secret is given to the participants of lower levels. To reconstructing the secret, they need to solve a linear system. In such a setting, the set of all participants is divided into disjoint levels. The ith level contains n_i participants, and the secret is shared among them. Each level has certain threshold value t_i. The access structure is then determined by a sequence of threshold requirements: a subset of participants is authorized if it has at least t_i participants from ith level, as well as at least t_{i+1} participants from the other level, and so forth.

The shadow size has major impact in the network transmission time and bandwidth and storage space. Therefore, reducing shadow size is considered recently. Wang and Su applied differencing function to obtain difference image and then used Huffman coding in order to reduce the shadows size [7].

Blakley's concept for sharing secret image was applied by several researchers. Tso proposed secret image sharing scheme (SISS) based on Blakley's secret sharing with small shadow size [8]. Chen et.al presented simple but sufficient SISS by using Blakley's scheme [9]. Yang et.al modified Tso's scheme by using Galois field [10]. Ulutas et.al proposed SISS using Blakley's approach and steganography with same size in cover image with secret image [11].

Hierarchical threshold secret image sharing was first introduced by Guo et. al, employing Tassa's conjunction hierarchical secret sharing scheme [12]. In their scheme, the secret image can be shared into shadows by embedding into the cover images. The shadows are distributed among participants of each level. The secret image can be disclosed if and only if the shadow images involved satisfy the threshold requirements. However, they mentioned that there are some technical problems that have to do with improving embedding capacity and proposing a more secure approach. Since to increase the storing capacity, their scheme uses more than t_0 secrets, causes leaking out some information about the secret image for some non-authorized subsets of participants. Pakniat et.al proposed a new hierarchical threshold secret image sharing scheme by utilizing cellular automata and hash function [13]. Their proposed scheme prevents information leakage of secret image of Guo's scheme. Bhattacharjee et.al proposed a HSIS scheme with flexibility in shadow size by utilizing compressive sampling for gray scale images [14]. They mentioned that shadow size has important role in transmission over the network and also in storage demand. The quality of the reconstructed secret image is dependent on amount of shadows in reconstruction phase. For lossless reconstruction, all of the requisite number of shadow images must be participated.

Essential SISS (ESISS) is another type of sharing secret image that shadow's importance is different. Li et.al proposed an essential SISS (ESISS) based on differential polynomial and Birkhoff interpolation to overcome the security and reconstruction difficulty problems of traditional ESISS [15]. Liu and Yang employed both scalable SISS and ESISS to propose a first scalable SISS with essential shadows [16]. Size of general and essential shadows were reduced in their proposed scheme. In reconstruction phase, gathering some essential shadows can partially reconstruct the secret image. To obtain lossless secret image in reconstruction phase, Thien and Lin's method was applied. Pakniat et al. [13], Liu and Yang [16] and Bhattacharjee et.al [14] mentioned that the proposed schemes by Guo et.al [12] and Pakniat et.al [13] are not efficient from the viewpoint of security and shadows size respectively. Presence of some non-authorized subsets of participants lead to disclose some information about the secret image. Fathimal and Rani [17] proposed a disjunctive hierarchical SS scheme for color images with two level of hierarchy. In their proposed method, simple arithmetic calculations (e.g. Lagrange interpolation and XOR operation) are used in sharing and reconstruction phases. A secret image is divided into several pieces and lower-level participants can substitute the higher-level ones. To avoid pixel expansion, XOR operation is performed to reduce the size of secret image by eight times in pre and post processing the secret image. The complexity of the method is reduced from O(n^2) of exiting schemes to O(n).

3. PRELIMINARIES

Definition of disjunctive and conjunctive hierarchical access structure is given in the following:

3.1. Disjunctive Hierarchical Access Structure

Assume $U = \bigcup_{i=0}^{m} U_i$, $U_i \cap U_j = \phi, 0 \le i < j \le m$ is a set of n participants that is composed of m levels. The subset U_0 is the highest level of hierarchy while U_m is on the least privileged level. Let $t = \{t\}_{i=0}^{m}$ be the threshold on different levels that is monotically increasing sequence of integers, $0 < t_1 < ... < t_m$. Then disjunctive access structure is defined by (1)

$$\Gamma = \left\{ A \subset U : \left| A \cap (\bigcup_{j=0}^{i} U_i) \right| \ge t_i , \exists i \in \{0,1,\ldots,m\} \right\} \tag{1}$$

3.2. Conjunctive Hierarchical Access Structure

Tassa considered more rigid conditions for Simmon's hierarchical access structure. According to Tassa, although higher-level participants could be replaced by lower-level ones, a predefined number of higher-level participants would still need to be involved in recovery of the secret. The conjunctive hierarchical access structure is given by (2).

$$\Gamma = \left\{ A \subset U : \left| A \cap (\bigcup_{j=0}^{i} U_i) \right| \geq t_i , \forall i \in \{0,1,\ldots,m\} \right\} \quad (2)$$

3.3. Blakley's Scheme

Blakley used projective geometry to share the secret between n participants. In order to constructing shadows, a first coordinate of a point in a t-dimensional over GF(q) is defined as the secret by the dealer. Then the set solution $x = (x_1, x_2, ..., x_t)$ is generated as public to form an affine hyperplane, $a_1x_1 + a_2x_2 + ... + a_tx_t = b$ that go through the secret point. Afterwards the values of b are given to each participant as their shadows. In the reconstruction phase, the junction of any t or more of these hyperplanes is calculated to obtain the secret. Figure 1 shows an example of (2,3) Blakley's scheme. The secret is a point S, in a two-dimensional plane where the shadows are lines (L_1, L_2, L_3) that cross over the secret point. The secret can be revealed by calculating the intersection point of any two of the lines.

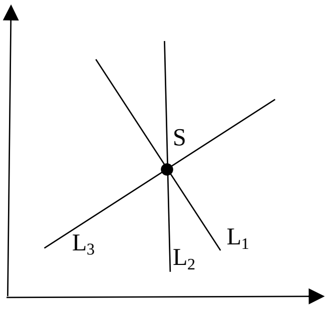


***Figure 1.** Blakley's secret sharing scheme*

4. THE PROPOSED HIERARCHICAL SECRET SHARING SCHEME

Our proposed scheme employs a generalized form of Blakley's threshold scheme, in which the secret S is shared between participants with different privileges. Consider the hierarchical threshold secret sharing scheme, $(t,n) = \{t_i\}_{i=0}^{m}$, as defined in Definition 2. The secret S is a point in a t-dimensional space that has been taken from the *GF(q)*, where *GF(q)* is a finite Galois field with q elements in which q is at least as large as the number of possible secrets. First of all, we want to explain the way of performing the scheme shortly. To perform this task, first the dealer takes the secret to generate n shadows and then distributes them among participants that do not have an equal degree of authority to recover the secret. The participants are divided into $m+1$ distinct levels $U = \{U_0, U_1, ..., U_m\}$, in hierarchical order where the first level of them has more power to reconstruct the secret. To construct the shadows between participants, the dealer performs the following steps:

Algorithm 1. The proposed hierarchical secret sharing scheme

1. Let the secret *S* be the first coordinate of a point in *(t-1)*-dimensional space over GF(q), $(a_0 = S, a_1, ..., a_{t-1})$.
2. The dealer defines a *(t-1)*-dimension hyperplane equation, $P(x) = \sum_{j=0}^{t-1} a_j x$ where $a_0 = S$.
3. For the participant $u \in U_i, (0 \le i \le m)$ of the *i*th level in the hierarchy, the dealer calculates $P_i(x) = \sum_{j=t_i-1}^{t-1} a_j x$, where (t_{-1}=*0*).
4. For every participant $u_{ij} \in U_i, ((0 \le i \le \alpha_i), \alpha_i$, is the number of participants of the *i*th level) from the *i*th level, the solution set, $x = (x_{i,j,z}, ..., x_{i,j,t-t_{i-1}-1}) \in GF(q)$, where $(0 \le z \le t - t_{i-1} - 1)$, is selected randomly by the dealer and then private shadows $s_{i,j} = P_i(x_{i,j,z}, ..., x_{i,j,t-t_{i-1}-1})$ are obtained. Only the value of $s_{i,j}$ is distributed to every participant. (*x* is known from the dealer).

Example 1. Assume that there are three levels in the hierarchy. The set of participants and the thresholds are $U = U_0 \bigcup U_1 \bigcup U_2$ an $t = (t_0, t_1, t_2) = (2, 4, 7)$ respectively. That means for reconstructing the secret, at least seven participants should pool their shadows together. Of these seven, at least four of them are from $U_0 \bigcup U_1$ and two of them are from U_0. Since $t = t_2 = 7$ then the dealer selects a hyperplane of degree 7-1=6, $P(x) = \sum_{j=0}^{6} a_j x_j, a_0 = S$. The secret is the first coordinate of a point in the space. The dealer selects $x_{i,j,z}, (0 \le i \le m, 0 \le j \le \alpha_i, 0 \le z \le t - t_{i-1} - 1)$, for each participant to calculate the value of *P(x*$_{i,j,z}$*)* as shadows. Thereafter, the shadows are distributed among participants $u \in U_i$ as in (3) ($x_{i,j,z}$ is known for dealer and participants):

$$
\begin{aligned}
&u \in U_0, P_0(x) = \sum_{j=0}^{6} a_j x = (a_0 + a_1 + ... + a_5 + a_6)x \\
&u \in U_1, P_1(x) = \sum_{j=2}^{6} a_j x = (a_2 + a_3 + a_4 + a_5 + a_6)x \\
&u \in U_2, P_2(x) = \sum_{j=4}^{6} a_j x = (a_4 + a_5 + a_6)x
\end{aligned}
\tag{3}
$$

In the reconstruction phase at least seven participants can build the linear equation (4) system to solve. If the participants cannot satisfy the predefined threshold requirements, then they cannot retrieve any information about the secret.

$$
\begin{bmatrix}
x_{0,1,0} & x_{0,1,1} & x_{0,1,2} & x_{0,1,3} & x_{0,1,4} & x_{0,1,5} & x_{0,1,6} \\
x_{0,2,0} & x_{0,2,1} & x_{0,2,2} & x_{0,2,3} & x_{0,2,4} & x_{0,2,5} & x_{0,2,6} \\
0 & 0 & x_{1,1,0} & x_{1,1,1} & x_{1,1,2} & x_{1,1,3} & x_{1,1,4} \\
0 & 0 & x_{1,3,0} & x_{1,6,1} & x_{1,3,2} & x_{1,3,3} & x_{1,3,4} \\
0 & 0 & 0 & 0 & x_{2,1,0} & x_{2,1,1} & x_{2,1,2} \\
0 & 0 & 0 & 0 & x_{2,2,0} & x_{2,2,1} & x_{2,2,2} \\
0 & 0 & 0 & 0 & x_{2,4,0} & x_{2,4,1} & x_{2,4,2}
\end{bmatrix}^{-1}
\times
\begin{bmatrix} b_1 \\ b_2 \\ b_4 \\ b_6 \\ b_8 \\ b_9 \\ b_{11} \end{bmatrix}
=
\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix}
\tag{4}
$$

5. CONJUNCTIVE HIERARCHICAL THRESHOLD SECRET IMAGE SHARING

Our proposed schemes consist of two phases: sharing and reconstructing phase.

5.1. Construction phase

In the sharing phase a set of participants are divided into *m+1* levels $U = U_0, U_1, ..., U_m$ according to their privilege. A sequence of threshold values $\{t_0, t_1, ..., t_m\}$, is defined by the dealer for each level. Afterwards, the dealer shares a secret image S into n shadow images s_i, for $i = 1, 2, ..., n$ and distributes them between participants of levels. In the reconstructing phase, according to the conjunctive hierarchical access structure, given shadow images must satisfy a sequence of threshold requirements to reveal the secret image.

Providing confidentiality is the most important factor that must be considered to propose the SS scheme especially in sensitive secret images. Moreover, reducing the capacity needs by decreasing the size of shares is another factor must be considered. In our proposed scheme, the secret image is divided into $t=t_m$ disjoint group of pixels. Then "XOR" operation is performed to pixels of every group. The size of shadows is $M \times N / t_m$ that are reduced significantly. Sharing algorithm is displayed in the Algorithm 2.

Proposed scheme ensures the perfectness properties of hierarchical secret sharing scheme; which restrict access only to authorized participants and non-authorized participant cannot reveal any information about the secret.

Algorithm 2. Proposed sharing approach

```
1. Scramble secret image by a permutation function.
2. If the value of pixel $p_i < 250$, then do nothing, or if $p_i \geq 250$, divide $p_i$ into two values
   250 and $(p_i - 250)$ to store these values consecutively.
3. For each levels we generate equation $P_i(x) = (\sum_{j=t_i-1}^{t-1} a_j .x)\%251,\ 0 \leq i \leq m$ (m is the
   number of levels).
4. The secret image is partitioned into t disjoint groups, $(k_0, k_1, k_2, ..., k_{t-1})$.
   $a_0 = k_0, a_j = k_j \oplus k_0, 1 \leq j \leq t-1$ are defined as coefficient of hyperplane equation,
   $(a_0, a_1, a_2, ..., a_{t-1})$.
5. The dealer randomly selects the values $x = (x_0, ..., x_{t_i-1})$ for each participant to obtain the
   shared values $s_i = P_i(x_0, ..., x_{t_i-1})$.
6. Successively take the pixels of unprocessed groups to obtain n shadows (shared images).
```

5.2. Reconstruction Phase

During the reconstruction phase, given shadow images must satisfy a sequence of threshold requirements based on conjunctive hierarchical threshold access structure. The details of reconstructing secret image are as in Algorithm 3.

6. EXPERIMENTAL RESULTS

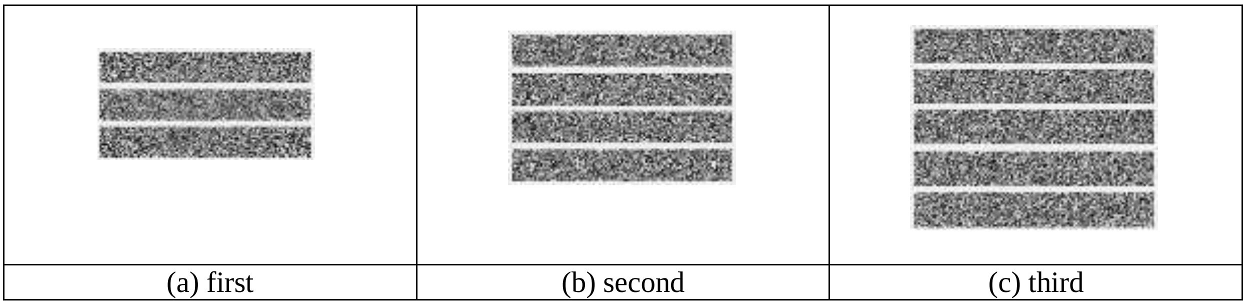
In this section we report some implementation results of our proposed scheme to examine the feasibility and efficiency of the proposed scheme. We use Lena grayscale image with size 210×210 pixels as secret image, as shown in Figure 2. A secret image is shared into participants of levels. For example, consider 12 participants that three of them are in the first (highest level), four of them are in the second level and five in the last (lowest) level. Assume a sequence of threshold requirement $(t_0, t_1, t_2) = (2, 4, 7)$.

Figure 2. *The secret image*

Algorithm 3. Proposed reconstruction approach

1. Take the first pixel from *t* participants shadows, $(s_0, s_1, ..., s_{t-1})$.
2. The pixels $(s_0, s_1, ..., s_{t-1})$ are set into Equation 1 to get pixel values of the first group of secret image, $(a_0, a_1, a_2, ..., a_{t-1})$. The solution set $x = (x_0, ..., x_{t_i-1})$ values are determined by dealer.
   $$s_i = P_i(x_0, ..., x_{t_i-1}) = (\sum\nolimits_{j=t_i-1}^{t-1} a_j x)\%251,\ 0 \le i \le m \qquad \text{(Eq.1)}$$
3. If $a_i < 250$, do nothing, or else if $a_i = 250$ then replace the value of a_i with $(a_{i+1} + 250)$ and remove a_{i+1}.
4. Successively take the pixels of unprocessed pixels of *t* shadows to calculate the coefficients $(a_0, a_1, a_2, ..., a_{t-1})$.
5. The dealer solves $k_0 = a_0, k_j = a_j \oplus a_0, 1 \le j \le t-1,$ to reconstruct secret values $(k_0, k_1, k_2, ..., k_t)$, until all pixels are processed.
6. Unscramble the image with the inverse permutation function to get the secret image.

The experimental results show that the secrecy of proposed scheme is satisfied and the size of shadow images is $M \times N / t_m = 1/7, (t_m = t)$ as shown in Figure 3. The reconstructed images, without presence of high level and with satisfying the hierarchical access structure are illustrated in Figure 4 (a) and (b) respectively.



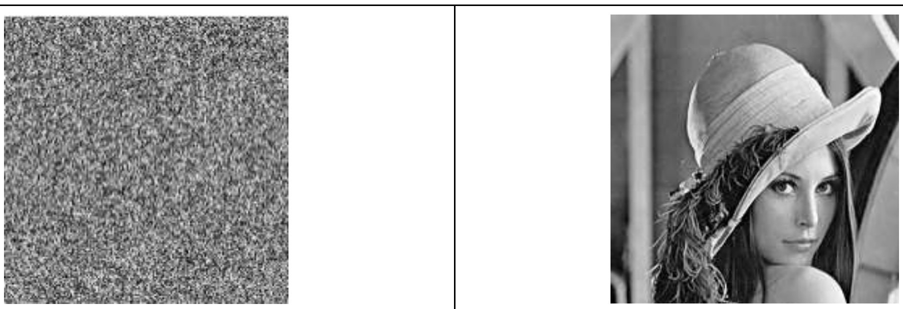
(a) first (b) second (c) third

Figure 3. *Shadow images of (a) first (b) second (c) third level of scheme.*

The Peak Signal to Noise Ratio (PSNR) is a measure to examine the distortion of reconstructed secret image with $M \times N$ pixels. PSNR is defined by the Mean Square Error (MSE) between the secret image and reconstructed image. Equation 5 describes PSNR and MSE where S_i is the pixel value of secret image and R_i is the pixel value of reconstructed secret image.

$$PSNR = 10\log 10(\frac{255^2}{MSE})\text{dB}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M \times N}(\mathrm{S}_i - R_i)^2 \tag{5}$$



(a) The reconstructed secret image without satisfying the hierarchical threshold access structure (the first level).

(b) The reconstructed secret image with satisfying the hierarchical threshold access structure.

Figure 4. *The reconstructed secret image*

In our proposed schemes, by the application of Thien and Lin’s method, the secret image can be reconstructed without distortion. As we mentioned in Section 1 this method slightly increases the size of shadow images but the increment is very small to emphasize. The zero value of MSE causes the value of PSNR to be infinity, and then the secret image and reconstructed image are identical. Figure 4 (b) demonstrates the reconstructed image with the infinity PSNR value.

7. SECURITY ANALYSIS

In this section, we describe statistical analysis in order to prove the validity of the proposed secret image sharing scheme. These tests are especially performed by calculating the histograms and the correlations of two adjacent pixels of the secret image and its shadows. First we perform a test by a histogram of secret image and its shadows of different levels that are given in Figure 5. An image histogram shows pixel intensity values which show how pixels in an image are distributed. The test results show that histograms of the shadows are fairly uniform and significantly different from the histogram of the secret image, which makes statistical attacks difficult.

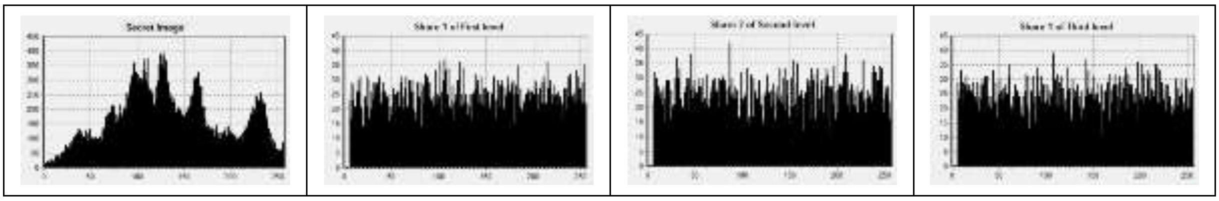


Figure 5. *Histograms of the secret image and its some shadows at different levels.*

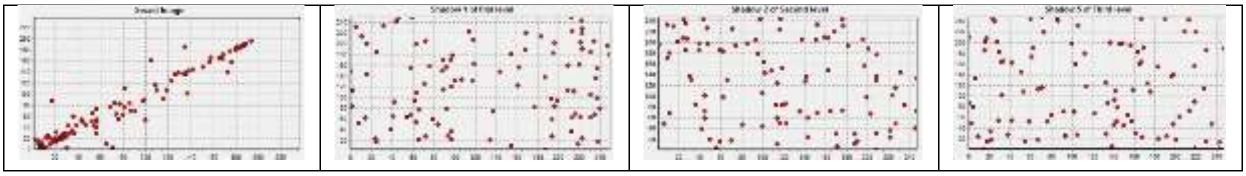


Figure 6. *Correlation of horizontally adjacent pixels.*

To analyze the power of our proposed scheme, the correlation of adjacent pixels of the secret image and its shadows have been calculated. In general, adjacent pixels of most secret images are highly correlated. In contrary, the correlation of two adjacent pixels of shadows must be low for effective SS scheme. To test the correlation of adjacent pixels of the secret image and its shadows, we have randomly selected 1000 pairs of two vertically adjacent pixels, 1000 pairs of two horizontally adjacent pixels, and 1000 pairs of two diagonally adjacent pixels, for the secret image as well as for its shadows after which we calculated correlation coefficient of each pair using the following Equation 6 two formulas and the results are shown in Table 1:

$$\operatorname{cov}(x,y) = E(x - E(x))(y - E(y))$$
$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{\operatorname{var}(x)}\sqrt{\operatorname{var}(y)}} \tag{6}$$

where *x* and *y* in Equation 6 are the value of two adjacent pixels in the images. As it is shown in Table 1, there is a weak correlation between the pixels of the shadows. For example, the correlation coefficient for two horizontally adjacent pixels of secret image is almost 1, as it was expected. However, these coefficients of shadows are very close to 0. Figure 6 illustrates the correlation distribution of two horizontally adjacent pixels in the secret image and its shadows of different levels. As it is demonstrated in Figure 6 the correlation between the pixels of the secret image are strong. In contrary, there are weak correlations between the pixels of the shadows since the points are distributed randomly.

8. CONCLUSION

The overall aim of this paper is to propose a new hierarchical threshold secret sharing based on Tassa's conjunctive hierarchical threshold access structure definition that utilized Blakley's projective geometry approach. We have proven in Section 3 that our proposed scheme is ideal and perfect. Our proposed method is performed to share the secret image among the participants with different privileges. Once the dealer generates the share images, these are distributed into distinct levels of hierarchy. The secret image can be reconstructed if and only if subset of authorized access structure satisfies the hierarchical threshold access structure which is defined by the dealer. In our method, PSNR value is infinity, thus the secret image and the reconstructed image are identical. The security analyses involve calculating histogram and correlation of two adjacent pixels of the secret image and its shadows, which indicates that the proposed scheme resists the statistical attacks.

***Table 1.** Correlation coefficients of two adjacent pixels*

	Secret Image	**Shadow 1 of First Level**	**Shadow 2 of Second Level**	**Shadow 5 of Third Level**
Horizontal	0.9262	0.0033	0.0008	0.0221
Vertical	0.9498	0.0329	-0.0423	0.0096
Diagonal	0.9659	0.0313	0.0043	0.0475

CONFLICT OF INTEREST

No conflict of interest was declared by the authors

REFERENCES

[1] Blakley, G. R. "Safeguarding cryptographic keys", *Proceedings of the national computer conference* 48, 313–317 (1979).

[2] Shamir, A. "How to share a secret", *Commun. ACM*, 22, 612–613 (1979).

[3] Simmons, G. J., "How to (really) share a secret", *Conference on the Theory and Application of Cryptography*, 390–448 (Springer, 1988).

[4] Tassa, T., "Hierarchical threshold secret sharing", *J. Cryptol.* 20, 237–264 (2007).

[5] Naor, M. & Shamir, A., "Visual cryptography", *Workshop on the Theory and Application of of Cryptographic Techniques*, 1–12 (Springer, 1994).

[6] Thien, C.-C. & Lin, J.-C., "Secret image sharing", *Comput. Graph.* 26, 765–770 (2002).

[7] Wang, R.-Z. & Su, C.-H., "Secret image sharing with smaller shadow images", *Pattern Recognit. Lett.* 27, 551–555 (2006).

[8] Tso, H.-K., "Sharing secret images using Blakley's concept", *Opt. Eng.* 47, 77001 (2008).

[9] Chen, C.-C., Fu, W.-Y. & Chen, C.-C. "A Geometry-Based Secret Image Sharing Approach", *J. Inf. Sci. Eng.*, 24, 1567–1577 (2008).

[10] Yang, C.-N., Wu, C.-C. & Chou, C.-W. A Comment on" Sharing Secret Images Using Blakley's Concept", *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference*, 383–386 (IEEE, 2013).

[11] Ulutas, M., Nabiyev, V. V & Ulutas, G., "Improvements in geometry-based secret image sharing approach with steganography", *Math. Probl. Eng.* 2009, (2009).

[12] Guo, C., Chang, C.-C. & Qin, C. "A hierarchical threshold secret image sharing", *Pattern Recognit. Lett.* 33, 83–91 (2012).

[13] Pakniat, N., Noroozi, M. & Eslami, Z. "Secret image sharing scheme with hierarchical threshold access structure", *J. Vis. Commun. Image Represent.* 25, 1093–1101 (2014).

[14] Bhattacharjee, T., Maity, S. P. & Islam, S. R. "Hierarchical secret image sharing scheme in compressed sensing", *Signal Process. Image Commun.* 61, 21–32 (2018).

[15] Li, P., Yang, C.-N. & Zhou, Z. "Essential secret image sharing scheme with the same size of shadows", *Digit. Signal Process.* 50, 51–60 (2016).

[16] Liu, Y. & Yang, C. "Scalable secret image sharing scheme with essential shadows", *Signal Process. Image Commun.* 58, 49–55 (2017).

[17] P, M. F. & P, A. J. R. "Hierarchical threshold secret sharing scheme for color images", *Multimed. Tools Appl.* 1–15 (2016). doi:10.1007/s11042-016-4074-y