IRSTI 28.23.37
UDC 004.93 **DOI 10.70239/arsu.2025.t82.n4.03**

MULTILEVEL COMPARTMENT THRESHOLD SECRET IMAGE SHARING SCHEME

NABIYEV V.[1*], SOLEYMANZADEH K.[2]

[*]**Nabiyev Vasif[1]** — PhD, professor, faculty of engineering, department of computer engineering, Karadeniz Technical university, Trabzon, Turkey
E-mail: vasif@ktu.edu.tr, https://orcid.org/0000-0003-0314-8134
Soleymanzadeh Katira[2] — PhD, teacher, faculty of engineering and natural sciences, software engineering department, Istanbul health and technology university, İstanbul, Turkey
E-mail: katira.soleymanzadeh@istun.edu.tr, https://orcid.org/0000-0002-7557-2877

Abstract. Traditional secret sharing schemes assume that all participants within a group or compartment possess equal authority in reconstructing the secret. However, in many real-world applications, such as hierarchical organizational structures or secure multi-party collaborations, this assumption does not hold. To address this limitation, we propose a novel Multilevel Compartment Threshold Secret Image Sharing (MCT-SIS) scheme that introduces hierarchical privileges within each compartment. Our scheme is based on a combination of Tassa's hierarchical access structure and Ghodosi's compartment model, and utilizes Birkhoff interpolation and polynomial-based techniques to achieve robust and flexible secret image sharing. Participants are grouped into disjoint compartments, each with multiple levels of access, and the secret image is shared such that it can only be reconstructed when both compartmental and hierarchical threshold conditions are satisfied. The scheme ensures perfect secrecy, lossless reconstruction, and reduced storage overhead. Experimental results validate its feasibility and demonstrate its applicability to environments requiring fine-grained access control, such as collaborative data vaults, medical imaging systems, and secure multi-agency operations.

Key words: secret image sharing, threshold scheme, multilevel compartment, Birkhoff interpolation, hierarchical security.

Introduction

A (t,n)-threshold secret sharing scheme distributes a secret S among n participants so that any subset of at least **t** participants ($t \le n$) can reconstruct S, whereas any coalition of fewer than t (i.e., at most $t-1$) learns nothing about it; such schemes are perfect when this zero-information property holds. The family of all authorized subsets is called the access structure and is denoted Γ. An access structure is monotone: if $A \in \Gamma$ and $A \subseteq B$ then $B \in \Gamma$.

Secret sharing is a vital cryptographic primitive that allows a secret to be distributed among multiple participants such that only predefined subsets of participants, defined by an access structure, can recover the original secret. This concept was first introduced independently by Shamir [1] and Blakley [2] in 1979. Shamir's scheme utilizes polynomial interpolation over finite fields, while Blakley's method is based on geometric constructions. These foundational methods are both perfect (no information leakage to unauthorized subsets) and ideal (each share has the same size as the secret).

Classical threshold secret sharing assumes equal authority among all participants within the authorized sets. However, in real-world applications such as secure military coordination, inter-agency document access, corporate key management, and e-health systems, participants often hold different roles and levels of authority. This limitation motivated the introduction of compartment-based access structures, pioneered by Simmons [3], where participants are grouped into disjoint compartments, each with its own threshold, along with a global threshold that must be satisfied to reconstruct the secret.

Despite this advance, the assumption that all participants within a compartment have the same authority is still unrealistic for many practical scenarios. To overcome this, multilevel compartment threshold secret sharing schemes (MLCT-SSS) were proposed, combining compartmental and hierarchical structures. Tassa [13] and Ghodosi et al. [6] provided seminal contributions in this direction, proposing schemes that handle intra-compartment hierarchy using interpolation techniques such as Birkhoff interpolation.

Recent studies have increasingly focused on applying these advanced access structures to multimedia data, especially secret image sharing (SIS). For instance, Thien and Lin [7] proposed a reduced-share-size image sharing scheme using 8-bit gray images and polynomial interpolation. More recently, Guo et al. [14] developed hierarchical threshold SIS methods for multi-user secure image distribution. Pakniat and Eslami [15] introduced a hierarchical threshold image sharing scheme with enhanced robustness. Additionally, Chen et al. [16] and Zhou et al. [17] have explored convolutional neural network (CNN)-based and hybrid encryption techniques to incorporate AI and deep learning into secret image sharing.

Therefore, in this study, we propose a perfect and ideal multilevel compartment threshold secret image sharing scheme. This scheme: partitions participants into distinct compartments; assigns them different levels of authority within each compartment; enforces both local (compartment-level) and global threshold conditions; uses Birkhoff interpolation and polynomial-based schemes for share generation; reduces the size of the shadow images, thereby lowering storage and transmission costs; and prevents lower-level participants from substituting higher-level ones during reconstruction.

This approach is particularly relevant in contemporary scenarios such as federated security systems, cloud-based confidential image exchange, and collaborative medical diagnostics. Our method ensures that only authorized participant groups with proper hierarchical configuration can reconstruct the secret image.

Simmons has described compartment threshold access structure as follows:

Definition 1: Let C = {C_1, C_2,…, C_m} denote m disjoint compartments of n participants, where (U = {1,2, … , n}) and $C_i \cap C_j = \emptyset$ for all $1 \le i < j \le m$. Let $t_i \in N$,$1 \le i \le m$ is represent the threshold of each compartment, and $t \in N$ denote the global threshold such that $t \ge \sum_{j=1}^{m} t_j$. Compartment access structure is described as follows:

$$\Gamma = \left\{ \begin{matrix} \mathcal{A} \subseteq \mathcal{U} : \exists \mathcal{P} \subseteq \mathcal{V} \text{ such that } |\mathcal{P} \cap \mathcal{C}_i| \geq t_i, \\ 1 \leq i \leq m \text{ and } |\mathcal{P}| = t \end{matrix} \right\}$$

Several studies have addressed the realization of such compartment access structures. Tassa et al. [4], Brickell et al. [5], and Ghodosi et al. [6] have proposed secret sharing schemes supporting this model. Tassa and Dyn proposed an ideal and perfect secret sharing scheme for two types of compartment structures-lower and upper bounds-based on bivariate Lagrange interpolation. Brickell et al. proved that ideal secret sharing schemes exist for compartment structures and constructed an efficient implementation in the specific case where $t = \sum_{j=1}^{m} t_j$.

Ghodosi et al. introduced a perfect and ideal scheme for hierarchical and compartment-based structures. In their approach, the authority levels of participants within a company (or compartment) differ, meaning not all participants have equal power to reconstruct the secret. Their method first divides the overall secret into partial secrets**,** one for each compartment, and then distributes these partial secrets among participants. In the reconstruction phase, each compartment recovers its partial secret independently. The final secret is then obtained by combining all recovered partials.

In practical applications, secret images often need to be securely shared among participants who are organized into disjoint compartments. To address this, we propose a multilevel compartment threshold secret image sharing scheme**.**

In 2002, Thien and Lin [7] introduced a secret sharing scheme for 8-bit grayscale images based on Shamir's method. Their method allowed slight truncation for pixel values in the range 251–255 to meet the modulus requirement of a prime number. To achieve **lossless reconstruction**, they proposed a minor extension that marginally increased the data size, which was acceptable due to the limited number of affected pixels.

Secret image sharing has since been widely studied [8–11]. However, most of these schemes are based on classical (t,n)-threshold structures and do not support hierarchical or compartmental constraints. In 2012, Guo et al. [12] proposed a hierarchical threshold secret image sharing scheme

based on Tassa's hierarchical model [13]. In their scheme, the secret image is embedded into cover images and can only be reconstructed if the hierarchical threshold conditions are satisfied. However, they identified certain security weaknesses in their approach.

To address these concerns, Pakniat et al. [14] developed a secure hierarchical threshold secret image sharing scheme using cellular automata and Birkhoff interpolation**,** overcoming the limitations found in Guo et al.'s method.

The structure of this paper is organized as follows: Section 2 reviews Shamir's (t,n) threshold secret sharing scheme and Tassa's hierarchical model; Section 3 presents the proposed multilevel compartment secret image sharing scheme**;** Section 5 demonstrates experimental results. Finally, Section 6 provides conclusions and future directions.

Materials and methods of research

2.1 Review of Shamir Secret Sharing Scheme

(t,n) threshold Shamir scheme is based on Lagrange polynomial interpolation. Let s ∈ GF(q) be the secret where GF(q) is a finite Galois field with q elements. The dealer selects a random polynomial of degree (t − 1) as follows:

$$f(x) = s + \sum_{i=1}^{t-1} a_i\, x^i \; mod\; q$$

where a_1, a_2, ..., a_{t-1} are chosen randomly over GF(q). For sharing the secret n distinct real numbers x_1, x_2, ..., x_n are selected and the shares $s_i = f(x_i)$ are calculated for each participant. In the reconstruction phase, at least t participants can reconstruct the secret by using Lagrange interpolation:

$$p(x) = \sum_{i=1}^{t}\left(p_i(x_i) \prod_{1\le j\le t, j\ne j} \frac{x - x_j}{x_i - x_j}\right) (\mathrm{mod}\, q)$$

2.2 Review of Tassa's Conjunctive Hierarchical Threshold Secret Sharing Scheme

Assume $U = U_{i=0}^{m}$, G_i, $U_i \cap U_j = \emptyset$, $0 \le i < j \le m$, 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 $t = \{t_i\}_{i=0}^{m}$ be the threshold on different levels that is monotically increasing sequence of integers, $0 < t_1 < \cdots < t_m$. The conjunction hierarchical threshold access structure is:

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

Tassa proposed a hierarchical threshold secret sharing scheme which is based on Birkhoff interpolation that is perfect and ideal. I such a setting, the set of all participants is divided into disjoint levels. Let the shared secret s be taken from GF(q). The dealer generates a random polynomial $F(x) \in GF(q)$ of degree at most t_m - 1 as follows:

$$F(x) = s + a_1 x + a_2 x^2 \ldots + a_{t_m - 1} x^{t_m - 1}$$

The shares s_i, $s_i = F^{t_i - 1}(x)$ are calculated for each participants of *i* th level of hierarchy where $F^{t_i - 1}(.)$ is the $(t_i - 1)$th derivation of $F(x)$ and $t_{-1}=0$.

2. A multilevel compartment threshold access structure

In order to reconstruct the secret image based on our proposed access structure, the provided shadow images must satisfy the threshold requirement of each compartment, their internal hierarchical levels**,** and the global threshold**.** First, the partial secret corresponding to each compartment is recovered. Then, the complete secret image is reconstructed by combining these partial secrets**.** A single compartment cannot reveal any meaningful information about the secret on its own, as it can only recover its partial secret. Furthermore, the partial secret of a compartment cannot be reconstructed unless the hierarchical threshold conditions within that compartment are also satisfied.Therefore, the secrecy of the proposed scheme is ensured no information about the original secret is leaked unless all access conditions are met.

Definition 2: $C = \{C_1, C_2, \ldots, C_m\}$ are m distict compartments of n participants, ($U = \{1,2, \ldots, n\}$) and $C_i \cap C_j = \emptyset$ for all $1 \le i < j \le m$. $T = \{t_1, t_2, \ldots, t_m\}$, $1 \le t_i \le |C_i|$, $1 \le i \le m$ are threshold

value of each compartment and $\sum_{i=1}^{m} t_i$, $t_i \leq t \leq n$ is global threshold. Participants of each compartment, Ci , are distributed into l distinct level in it, that means, $C_i = \cup_{j=0}^{i} U_{i,j}$ and $U_{i,j} \cap U_{i,j+1} = \emptyset$, $0 \leq j \leq l$, $1 \leq i \leq m$. $k = \{k_{i,j}\}_{j=0}^{i}$ are monotonically increasing threshold value for each levels of compartments, $0 < k_{i,0} < \cdots < k_{i,l}$ and $t_i = k_{i,l}$. The proposed multilevel compartment threshol access structure is given in Eq.(1) and are illustrated in Fig.1:

$$\Gamma = \left\{ \begin{array}{l} A \subseteq U \left| \left\{ \left| A \cap \left(\bigcup_{z=1}^{j} U_{i,z} \right) \right| \geq k_{i,j} \ , \forall j \in \{1,\ldots,l\} \right\} \right. \\ \left. \forall i \in \{1,\ldots,m\} \text{ and } |A| \geq t \right. \end{array} \right\} \quad (1)$$

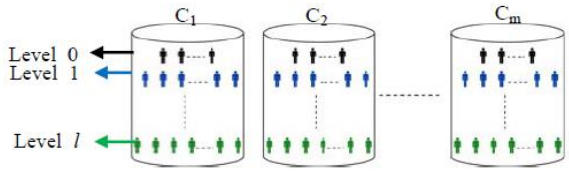


Figure 1 The multilevel compartment threshold scheme

3.1. Ideal secret sharing scheme for multilevel compartment threshold access structure

In this section, we propose a secret sharing scheme based on the approaches of Ghodosi and Tassa for the access structure described in Definition 2**.** The participants are distributed into disjoint compartments, with different levels of authority assigned within each compartment by the dealer. The secret G is an element of the finite field GF(q). Let t ≥ $\sum_{i=1}^{m} t_i$ be the global threshold, where mmm denotes the number of compartments. Let $k = \{k_{i,j}\}_{j=0}^{l}$ represent the threshold values of each hierarchical level within a compartment (where l is the number of levels in a compartment) and $t_i = k_{i,l}$ denote the total number of participants required within compartment C_i to reconstruct the partial secret of that compartment. In this phase, the dealer performs the following steps**:**

Step 1: Define the polynomial

$$g(x) = G + c_1 x + \cdots + c_{m-1} x^{m-1} \in \text{GF(q)} ,$$

$c_1,\ldots,c_{m-1}$ are randomaly selected to produce partial secret for each compartment $g_i = g(x_i)$, i=$1,\ldots,m$. $G=g(0)$ is the secret value.

Step 2: Select randomly t_i - 1 values $\alpha_{i,1}, \ldots, \alpha_{i,t_i-1}$ to define m polinomial $f_i(x)$ coressponding to each compartment as follows:

$$f_i(x) = g_i - \sum_{j=1}^{t_i-1} \alpha_{i,j} x^j, \qquad i = 1, \ldots, m$$

Step 3: Since $\sum_{i=1}^{m} t_i \leq t$ we select randmly $R = t - \sum_{i=1}^{m} t_i$ values $b_0,\ldots,b_{R-1}$ to determine $f(y)$ polinomial as follows:

$$f(y) = \sum_{i=t_i}^{t_i+R-1} b_{i-t_i} y^i$$

Step 4: Define $f_{i,j}(x, y)$ polinomial for each compartment as follows:

$f_{i,j}(x, y) = \left(f_i(x)\right)^{k_{i,j-1}} + f(y)$, $i = 1, \ldots, m$ (m is number of compartment) and $j=0,\ldots,l$ (l is the number of levels of a compartment), $(k_{i,-1} = 0)$ and $\left(f_i(x)\right)^{k_{i,j-1}}$ means $k_{i,j-1}$th derivation of $f_i(x)$.

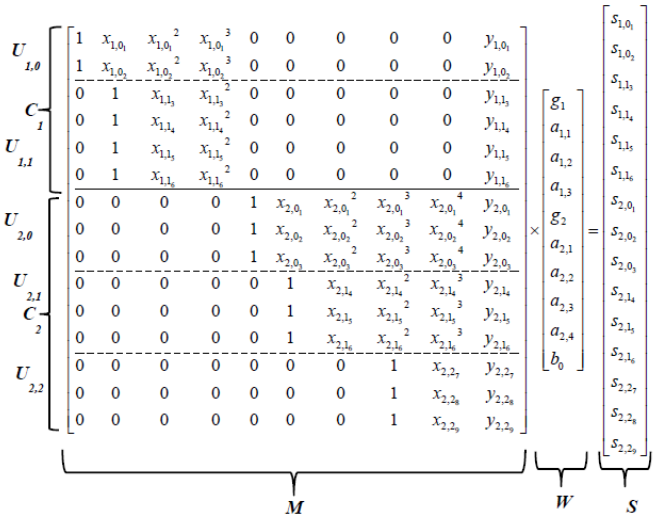
Step 5: Choose $(x_{i,j_z}, y_{i,j_z}) \neq 0$ value for each participant $u_{i,j_z} \in U_{i,j} \in C_i, 1 \leq z \leq n_i$ (n_i is the number of participants of each compartment). The pair value of (x_{i,j_z}, y_{i,j_z}) is differnet for two distict participants. $f_{i,j}(x_{i,j_z}, y_{i,j_z})$ is the shared value of each participant.

Corollary: The proposed multilevel compartment secret sharing scheme is perfect and ideal, which is only, A ∈ Γ can recover the secret.

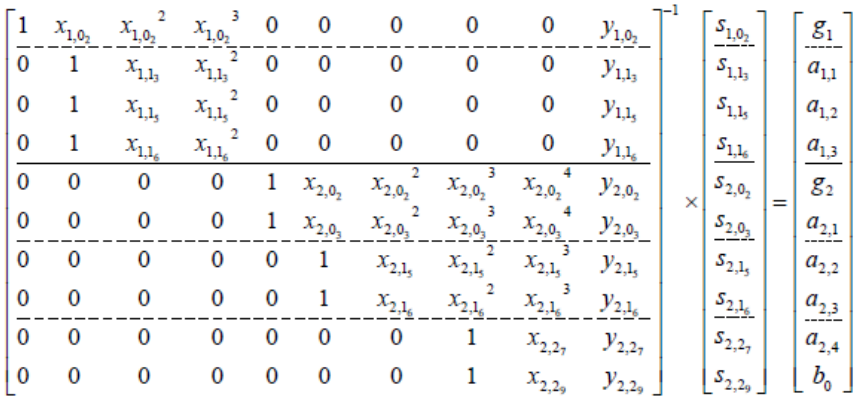
Proof: An authorized subset A ∈ Γ can reconstruct the secret G while an unauthorized subset A∉Γ obtain any information about it. According to the predetermined threshold value t_i for each compartment, at least **tit_iti** participants from each compartment must participate in order to reveal the secret. Suppose $\{n_1, \dots, n_m\}$ be the number of participant of an authorized subset A where $n_i \geq t_i$ and $\sum_{i=1}^{m} n_i \geq t$. Hierarchical threshold requirements $n_i \cap (\cup_{z=1}^{j} U_{i,z}) \geq k_j$ must be satisfied by n_i participants of each compartment. That means $\cup_{i=1}^{m} C_i$ is an authorized subset of participants if |A| = t , $|A \cap C_i| \geq t_i$, $t_i \in \{1, \dots, m\}$ and $C_i \cap \cup_{z=1}^{j} U_{i,z}) \geq k_j$, *j=0,...,l.* To reconstruct the secret, all participants of A ∈ Γ must pool together their shares to calculate a linear equation system. In this linear system, the number of equations are at least the number of unknown that means each compartment has t_i unknown coefficient g_i , $a_{i,j}$ and R unknown common b_i in all compartment. These equations are linearly independent, i.e, given coefficient values of each compartment form one row of a matrix that are not the same and none of the rows can be a combination of other rows or columns of a matrix. Therefore determinant of the reconstruction matrix cannot be zero. Then the equation system has a unique solution since there are at least *t* equations with *t* unknowns. The secret *G* can be recovered after recovering the partial secret, g_i of each compartment.

An unauthorized subset A ∉ Γ can not reveal any information about the secret. First, If the number of participants of each compartment be $\alpha_i < t_i$, then the number of equations of the linear system is lesser than unknowns coefficient so the system does not have any unique solution to recover the partial secret of each compartment. Second, if the number of participants of each compartment be $\alpha_i \geq t_i$ but $\sum_{i=1}^{m} \alpha_i < t$ then the values of $b_1, \dots, b_R$ cannot recover. Third, suppose the number of participants of each compartment be $\alpha_i \geq t_i$ and $\sum_{i=1}^{m} \alpha_i \geq t$ but the participants of each compartment do not satisfy the hierarchical threshold requirement of each level, i.e., there are not participants of higher level from a compartment. In this case the secret cannot be recovered since there are not any participants of higher level that cause the determinant of linear equation zero. So the coefficient matrix is not invertible. Secret accessibility by authorized and inaccessibility of unauthorized subset of participants satisfy the perfectness of secret sharing scheme. This scheme is ideal, since every participants has one share value over GF(q) and information rate is equal to one.

Example 1: Suppose there are two compartments with distinct participants in which the threshold value of each compartment and global threshold are $t_1=4$, $t_2=5$, $t=10$ respectively. Compartment one have two distinct levels that threshold of each level are $k=(k_{1,1}, k_{1,2})=(1,4)$. There are three level in compartment two with threshold $k=(k_{2,1}, k_{2,2}, k_{2,3}) = (1,3,5)$. Total number of participants of an authorized subset A must be at least 10. Of these ten, at least four are from compartment one and five are from compartment two. However since there are hierarchy authority among participants of a compartment, then at least one participant in compartment one must be from first level, $U_{1,1}$, and at least four from $U_{1,1} \cup U_{1,2}$. Collaborating participants of compartment two must be at least five. Of these five, at least one from $U_{1,1}$ level, three participants from $U_{1,1} \cup U_{1,2}$ and five from $U_{1,1} \cup U_{1,2} \cup U_{1,3}$. Since $R = t - \sum_{i=1}^{m} t_i = 10 - 9 = 1$, at least one participant can be from any of compartments and any of levels. The dealer constructs the following linear system to shares secret among participants. In this system, g_1 and g_2 values of matrix *W* are partial secrets of each compartment, matrix *M* is the coefficient matrix and matrix *S* is the shared value of each participants.



In the reconstruction phase at least 10 participants pool together their shares to solve the following linear system to calculate partial secrets, g_1 and g_2 . Then these partial secret are used to reveal the secret G.



4. A multilevel compartment secret image sharing scheme

In this section we propose a multilevel compartment secret image sharing scheme for multilevel compartment access structure described in section.3 which involve two phases: sharing and reconstructing. At first, the secret image S is divided among each compartment and then the partial secret images are shared between participants according to their privilege in each compartment. In the reconstructing phase, the threshold requirement of each compartment and their levels as well as global threshold of multilevel compartment access structure must be satisfied to reveal the secret image. Our main goal in this study is to reducing the size of storage requirement which cause decrease in computational effort needs. Moreover, providing secrecy is foremost concern addressing in this paper. That means in the reconstructing phase participants of higher level of each compartment cannot be substituted by the lower levels.

4.1. Secret image sharing phase

In this phase we shared NxM secret image among a set of n participants of m compartment. *t* (t is global threshold) pixels of secret image are taken as coefficient to produce partial shared values for each compartment. Therefore these partial values are used as coefficient of defined equation of each compartment to produce the shares for each participant of levels of compartments. The size of shares is reduced by *MxN/t* in which storage requirement are decreased significantly. Sharing algorithm is given in the following steps:

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 $(p_i - 250)$ and store these values respectively.

3. The secret image is divided into t disjoint groups, $c_0, \ldots c_{t-1}$, as the coefficient of the following equation:

$$g(x) = \left(\sum_{j=0}^{t-1} c_j x^j\right) \%251, \quad (t \text{ is global threshold })$$

4. The **s**olution set , $x=(x_0, \ldots x_{t-1}) \in GF(q)$ is selected randomly by dealer to produce t partial shared values as each compartment secret, $a_i = g(x_i)$, $i=1,\ldots,t-1$. Afterwards, these are used as the coefficient for the following equations:

$$f_i(\mathrm{x}) = \sum_{z=\sum_{j=1}^{i} t_{j-1}+t_i-1,\ p=t_i-1} a_z x^p \quad , i = 1, \ldots, m \text{ and } t_0 = 0,$$

$$z=\sum_{j=1}^{i} t_{j-1},\ p=0$$

$$f_i(\mathrm{y}) = \sum_{p=1,z=t-R}^{p=R,z=t-1} a_z y^p \quad , (R = t - \textstyle\sum_{i=1}^{m} t_i)$$

5. For each compartment we define equation, $f_{i,j}(x,y) = ((f_i(x))^{k_{i,j-1}} + f_i(y)) \%251$. ($k_{i,j}$ is each level threshold of a compartment)

$i= 1, \ldots, m$ (m is number of compartment) and $j = 0, \ldots, l$ (l is the number of levels of a compartment), ($k_{-1} = 0$) and $(f_i(x))^{k_{i,j-1}}$ means (k_{j-1}) th derivation of $f_i(x)$).

6. $(x_{i,j_z}, y_{i,j_z}) \neq 0$are selected for i^{th} compartment of j^{th} level's z^{th} participants to produce the shares of each participants as $s_{i,j_z}(x_{i,j_z}, x_{i,j_z}) = \left(f_i(x_{i,j_z})\right)^{k_{i,j-1}} + f(y_{i,j_z})$

7. Take succseesive pixels of unprocessed groups to obtain n shared images.

4.2. Secret image reconstructing phase

In order to reconstruct the secret image based on our proposed access structure, the provided shadow images must satisfy the threshold requirement of each compartment**,** their internal hierarchical levels, and the global threshold**.**

First, the partial secret corresponding to each compartment is recovered. Then, the complete secret image is reconstructed by combining these partial secrets**.** A single compartment cannot reveal any meaningful information about the secret on its own, as it can only recover its partial secret.

Furthermore, the partial secret of a compartment cannot be reconstructed unless the hierarchical threshold conditions within that compartment are also satisfied.

Therefore, the secrecy of the proposed scheme is ensured- no information about the original secret is leaked unless all access conditions are met.

Results and its discussion

In order to demonstrate the correctness and feasibility of our scheme, we report some implementation results. We used a grayscale image of a Dahlia flower, sized 210 × 210 pixels, as the secret image, as shown in Fig. 2. The secret was shared among fifteen participants divided into two compartments: the first compartment consists of nine participants**,** and the second includes the remaining six participants**.** The shadow images assigned to each participant are depicted in Fig. 3**.** The first compartment contains two hierarchical levels**,** while the second compartment consists of three levels**.**We assume a threshold sequence of $t_1 = 4$, $t_2 = 5$, and a global threshold $t = 11$, with the detailed hierarchical access structure defined as:

$$k_1 = (k_{1,1}, k_{1,2}) = (1, 4) \text{ and } k_2 = (k_{2,1}, k_{2,2}, k_{2,3}) = (1, 3, 5).$$

A reduction in the shadow image size by one-eleventh significantly decreases the storage

requirements**.** During the reconstruction phase**,** the secret image can be recovered only if the access structure requirements of authorized subsets are satisfied. Conversely, any unauthorized subset fails to reconstruct the secret image, thereby ensuring that the scheme maintains perfect secrecy and fidelity of the image.

Fig. 2. The secret image

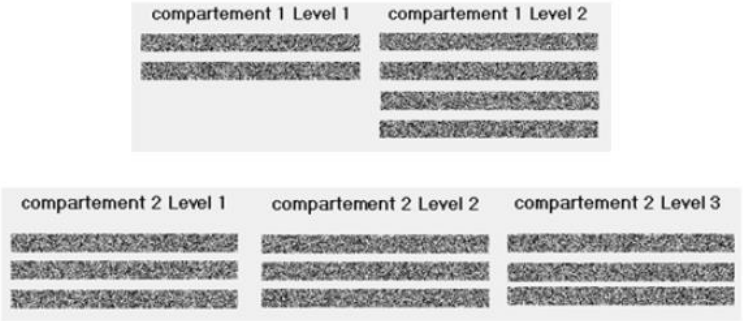


Figure 3. (a) Shadow images of first (b) Shadow images of second compartment of scheme

By selecting multiple pixels of the secret image as secret values in each step, the storage requirements are significantly reduced. Additionally, reducing the size of the shadow images further decreases the computational effort required for reconstruction.

Distortion is a critical factor in evaluating the quality of the reconstructed secret image. The Peak Signal-to-Noise Ratio (PSNR) is commonly used for this purpose and is defined as:

$$PSNR = 10 \times log_{10} (255^2 / MSE)\ dB, \qquad (2)$$

where MSE (Mean Square Error) is defined as:

$$MSE = (1 / M \times N) \sum_{i=1}^{MxN} (S_i - R_i)^2 \qquad (3)$$

Here, S_i and R_i are the pixel values of the original and reconstructed images, respectively.

In our proposed scheme, we adopt Thien and Lin's method to ensure distortion-free reconstruction of the secret image. The slight increase in the size of shadow images is negligible and does not impact overall efficiency. Notably, when the MSE value is zero, the PSNR tends to infinity, indicating a perfectly reconstructed image.

Conclusion

The main objective of this paper is to introduce a novel concept called the multilevel compartment access structure**.** Our proposed scheme incorporates hierarchy within the compartmental access model, resulting in a perfect multilevel secret sharing scheme. In this structure, an authorized subset of participants can successfully reconstruct the secret image, whereas any unauthorized subset gains no information–thus ensuring the security and confidentiality of the shared data.

In this study, we present a multilevel compartment secret image sharing scheme inspired by the works of Tassa and Ghodosi et al., employing Birkhoff interpolation and polynomial-based techniques**.** By selecting multiple pixels of the secret image as secret values at each step of the

proposed scheme, the overall storage requirements are significantly reduced**.** Moreover, the reduction in shadow size leads to **a** substantial decrease in the computational effort required for secret reconstruction.

References

1. Shamir A. How to share a secret. Communications of the ACM, 22(11), 1979, 612–613.

2. Blakley G. R. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, 1979, 313–317.

3. Simmons G. J. How to (really) share a secret. Advances in Cryptology–CRYPTO'88, 1988, 390–448.

4. Tassa T., & Dyn N. Multipartite secret sharing by bivariate interpolation. Journal of Cryptology, 22(2), 2009, 227–258.

5. Brickell E. F., Gordon D. M., McCurley K. S., & Wilson D. B. Fast exponentiation with precomputation. In Advances in Cryptology–EUCRYPT'87, 1987, 200–207.

6. Ghodosi H., Pieprzyk J., & Safavi-Naini R. Secret sharing in multilevel and compartmented groups. Information Security and Privacy, 1998, 367–378.

7. Thien C. C., & Lin J. C. Secret image sharing. Computers & Graphics, 26(5), 2002, 765–770.

8. Lin C. C., & Tsai W. H. Secret image sharing with steganography and authentication. Journal of Systems and Software, 73(3), 2003, 405–414.

9. Wang R. Z., Lin C. F., & Tsai J. C. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34(3), 2000, 671–683.

10. Wu H. C., & Shih F. Y. A simple image sharing scheme. Pattern Recognition Letters, 25(8), 2004, 979–992.

11. Chin-Chen Chang, Tsai-Yang Lin, & Chia-Chen Chang. A novel secret image sharing scheme for true-color images with size constraint. IEEE Transactions on Circuits and Systems for Video Technology, 16(5), 2004, 587–592.

12. Guo J., Chen C. C., & Qin Y. A hierarchical threshold secret sharing approach. Pattern Recognition Letters, 33(1), 2012, 83–91.

13. Tassa T. Hierarchical secret sharing. Journal of Cryptology, 20(2), 2007, 237–264.

14. Pakniat N., & Eslami Z. An improved secret image sharing scheme with hierarchical threshold access structure. Journal of Information Security and Applications, 58, 2021, 102770.

15. Jin Y., Wang S., & Zhang X. A deep learning-based secure image sharing scheme with adaptive thresholding. IEEE Access, 9, 2021, 107246–107258.

16. Zhang M., Liu Y., & Yang H. Blockchain-based secret image sharing for Internet of Things security. Future Generation Computer Systems, 141, 2023, 56–68.

17. Kim H., Park J., & Kim Y. Federated threshold secret sharing in privacy-preserving medical applications. Computers in Biology and Medicine, 149, 2022, 106003.

Список литературы

1. Shamir A. How to share a secret. Communications of the ACM, 22(11), 1979, 612–613.

2. Blakley G. R. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, 1979, 313–317.

3. Simmons G. J. How to (really) share a secret. Advances in Cryptology–CRYPTO'88, 1988, 390–448.

4. Tassa T., & Dyn N. Multipartite secret sharing by bivariate interpolation. Journal of Cryptology, 22(2), 2009, 227–258.

5. Brickell E. F., Gordon D. M., McCurley K. S., & Wilson D. B. Fast exponentiation with precomputation. In Advances in Cryptology–EUCRYPT'87, 1987, 200–207.

6. Ghodosi H., Pieprzyk J., & Safavi-Naini R. Secret sharing in multilevel and compartmented groups. Information Security and Privacy, 1998, 367–378.

7. Thien C. C., & Lin J. C. Secret image sharing. Computers & Graphics, 26(5), 2002, 765–

770.

8. Lin C. C., & Tsai W. H. Secret image sharing with steganography and authentication. Journal of Systems and Software, 73(3), 2003, 405–414.

9. Wang R. Z., Lin C. F., & Tsai J. C. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34(3), 2000, 671–683.

10. Wu H. C., & Shih F. Y. A simple image sharing scheme. Pattern Recognition Letters, 25(8), 2004, 979–992.

11. Chin-Chen Chang, Tsai-Yang Lin, & Chia-Chen Chang. A novel secret image sharing scheme for true-color images with size constraint. IEEE Transactions on Circuits and Systems for Video Technology, 16(5), 2004, 587–592.

12. Guo J., Chen C. C., & Qin Y. A hierarchical threshold secret sharing approach. Pattern Recognition Letters, 33(1), 2012, 83–91.

13. Tassa T. Hierarchical secret sharing. Journal of Cryptology, 20(2), 2007, 237–264.

14. Pakniat N., & Eslami Z. An improved secret image sharing scheme with hierarchical threshold access structure. Journal of Information Security and Applications, 58, 2021, 102770.

15. Jin Y., Wang S., & Zhang X. A deep learning-based secure image sharing scheme with adaptive thresholding. IEEE Access, 9, 2021, 107246–107258.

16. Zhang M., Liu Y., & Yang H. Blockchain-based secret image sharing for Internet of Things security. Future Generation Computer Systems, 141, 2023, 56–68.

17. Kim H., Park J., & Kim Y. Federated threshold secret sharing in privacy-preserving medical applications. Computers in Biology and Medicine, 149, 2022, 106003.

КӨПДЕҢГЕЙЛІ СЕКЦИЯЛЫҚ ҚҰРЫЛЫМДА ШЕКТІ ҚОЛЖЕТІМДІЛІГІ БАР ҚҰПИЯ КЕСКІНДІ БӨЛУ СҰЛБАСЫ

НАБИЕВ В.[1*], СУЛЕЙМАНЗАДЕ К.[2]

[*]**Набиев Васиф**[1] – PhD, профессор, Инженерия факультеті, компьютерлік инженерия кафедрасы, Қаратеңіз техникалық университеті, Трабзон қ., Түркия,
E-mail: vasif@ktu.edu.tr, https://orcid.org/0000-0003-0314-8134
Сулейманзаде Катира[2] – PhD, оқытушы, инженерия және жаратылыстану ғылымдары факультеті, Бағдарламалық жасақтама инженериясы кафедрасы, Ыстамбұл денсаулық және технология университеті, Ыстамбұл қ., Түркия
E-mail: katira.soleymanzadeh@istun.edu.tr, https://orcid.org/0000-0002-7557-2877

Аңдатпа. Дәстүрлі құпияны бөлу схемалары топ немесе бөлім ішіндегі барлық қатысушылардың құпияны қалпына келтіруде бірдей өкілеттілікке ие екенін болжайды. Алайда шынайы өмірде – мысалы, иерархиялық ұйымдарда немесе қауіпсіз көпжақты ынтымақтастықта – бұл болжам сәйкес келмейді. Осы шектеуді жою үшін біз иерархиялық деңгейлерге ие көпдеңгейлі бөлімдік шекті құпия кескінді бөлу (MCT-SIS) атты жаңа схеманы ұсынамыз. Бұл схема Тасса ұсынған иерархиялық қол жеткізу құрылымына және Гходоси секциялық моделіне негізделіп, Биркгофф интерполяциясы мен полиномдық әдістерді қолдана отырып, сенімді және икемді кескін бөлу мүмкіндігін ұсынады. Қатысушылар өзара қиылыспайтын бөлімдерге бөлінеді, олардың әрқайсысында қол жеткізудің бірнеше деңгейі бар. Құпия кескін тек бөлімдік және иерархиялық шекті талаптар орындалғанда ғана қалпына келтіріледі. Бұл схема мінсіз құпиялылықты, ақаусыз қалпына келтіруді және сақтау көлемінің азаюын қамтамасыз етеді. Эксперименттік нәтижелер бұл тәсілдің тиімділігін көрсетіп, оны деректерді бірігіп басқару, медициналық бейнелеу жүйелері және қауіпсіз көпагентті ортада қолдануға болатынын дәлелдейді.

Түйін сөздер: құпия кескінді бөлу, шекті схема, көпдеңгейлі бөлім, Биркгофф интерполяциясы, иерархиялық қауіпсіздік.

СХЕМА РАСПРЕДЕЛЕНИЯ СЕКРЕТНОГО ИЗОБРАЖЕНИЯ С ПОРОГОВЫМ ДОСТУПОМ В МНОГОУРОВНЕВОЙ СЕКЦИОННОЙ СТРУКТУРЕ

НАБИЕВ В.[1*], СУЛЕЙМАНЗАДЕ К.[2]

[*]**Набиев Васиф**[1] – PhD, профессор, факультет инженерии, кафедра компьютерной инженерии, Черноморский технический университет, г. Трабзон, Турция
E-mail: vasif@ktu.edu.tr, https://orcid.org/0000-0003-0314-8134
Сулейманзаде Катира[2] – PhD, преподаватель, факультет инженерии и естественных наук, кафедра программной инженерии, Университет здравоохранения и технологий Стамбула, г. Стамбул, Турция
E-mail: katira.soleymanzadeh@istun.edu.tr, https://orcid.org/0000-0002-7557-2877

Аннотация. Традиционные схемы распределения секрета предполагают, что все участники в группе или секции обладают равными правами на восстановление секрета. Однако во многих реальных приложениях, таких как иерархические организационные структуры или безопасное многопользовательское сотрудничество, это предположение не выполняется. Для преодоления этого ограничения мы предлагаем новую многоуровневую схему секционного распределения секретных изображений с порогом (MCT-SIS), которая вводит иерархические привилегии внутри каждой секции. Наша схема основана на сочетании иерархической структуры доступа Тассы и секционной модели Гходоси, с использованием интерполяции Биркгофа и полиномиальных методов для достижения надёжного и гибкого распределения изображений. Участники распределяются по непересекающимся секциям, каждая из которых имеет несколько уровней доступа. Секретное изображение может быть восстановлено только при соблюдении как секционных, так и иерархических пороговых условий. Схема обеспечивает идеальную секретность, безошибочное восстановление и снижение объёма хранения. Экспериментальные результаты подтверждают её эффективность и применимость в условиях, требующих детализированного управления доступом, таких как совместные хранилища данных, медицинские системы визуализации и безопасные межведомственные операции.

Ключевые слова: секретное распределение изображений, пороговая схема, многоуровневая секция, интерполяция Биркгофа, иерархическая безопасность