Mathematical Biosciences and Engineering

MBE, 21(1): 1286–1304.
DOI: 10.3934/mbe.2024055
Received: 17 September 2023
Revised: 10 December 2023
Accepted: 21 December 2023
Published: 26 December 2023

http://www.aimspress.com/journal/MBE

Research article

A global progressive image secret sharing scheme under multi-group joint management

Lina Zhang*, Jing Zhang, Jiaqi Sun and Qingpeng Chen

College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710600, China

* **Correspondence:** Email: zhangln@xust.edu.cn; Tel: +8617795724270.

Abstract: Diverging from traditional secret sharing schemes, group secret sharing schemes enable the recovery of secret information through collaborative efforts among groups. Existing schemes seldom consider the issue of the secrecy level of image information between different groups. Therefore, we propose a global progressive image secret sharing scheme under multi-group joint management. For inter-group relations, multiple groups with different priority levels are constructed using the approach of bit-polar decomposition. In this arrangement, higher-level groups obtain clearer secret image information. For intra-group relations, a participant-weighted secret sharing scheme is constructed based on Chinese Remainder Theorem and Birkhoff interpolation, in which the participants' secret sub-shares are reusable. During the recovery process, the sub-images can be recovered within the intragroup with the corresponding level. Groups collaborate through lightweight overlay operations to obtain different layers of secret images, achieving a global progressive effect. Analysis results show that the scheme is both secure and practical for group secret sharing.

Keywords: group secret sharing; priority; Chinese Remainder Theorem; Birkhoff interpolation; global progressive

1. Introduction

With the rapid development of global network and communication technologies, we have entered the era of networking and informationization [1]. In this era, a vast number of images carrying personal information are rapidly spreading across the Internet. Even seemingly meaningless communication data can inadvertently leak important information. Therefore, protecting the confidentiality and integrity of image data has become an important research topics both domestically and internationally.

Currently, image security techniques mostly include image information hiding, image encryption and image secret sharing. Among them, image secret sharing (ISS) [2], as a specific application direction of secret sharing scheme [3] in image information security protection, provides a higher level of security and confidentiality for image security protection. It applies the concept of secret sharing to the storage and transmission of image information, effectively solving the problem of image secret information leakage and tampering.

ISS can be divided into two categories: Threshold secret sharing scheme (TSS) [4–9] and progressive image secret sharing scheme (PISS). However, some inherent defects have in existing TSS schemes. The size of the shares at least twice that of the secret image due to the high pixel expansion ratio. Also, the reconstructed image may exhibit low quality. To solve these problems, researchers have proposed many PISS schemes.

The fundamental concept of PISS is to accomplish secret sharing by progressively unveiling various layers of an image. Liu and Yang [10] proposed three sharing models to construct a scalable image secret sharing scheme. Yan et al. [11] constructed a generalized progressive image secret sharing scheme with pixel non-expansion. Guo et al. [12] proposed a progressive image secret sharing scheme that divides the generated shared copies into multiple tiers, and there is a risk of partial reconstruction due to the fact that an attacker can try to recover the overall secret image information by using part of the acquired image information. To overcome this drawback, Bhattacharjee et al. [13] introduced a progressive image secret sharing scheme utilizing compression-aware generation of fixable shares. Expanding upon this groundwork, references [14,15] have proposed a progressive image secret sharing scheme based on compressive sensing (CS) and multi-level access control, respectively. In [14], the encoding and measurement of the image were implemented, while in [15], the secret image was divided into multiple layers with varying access permissions. Moreover, both [14] and [15] present techniques for gradually recovering different levels of the secret image, which provides valuable references for achieving secure image secret sharing.

As the need for information sharing continues to grow, the traditional solution of sharing secret images by a single group does not meet the needs of multiple groups. In order to provide a more flexible sharing mechanism, group secret sharing schemes [16–20] have emerged. This type of scheme allows multiple groups to share secret images at the same time for broader information sharing. In [17], Lagrange interpolation and the Chinese Remainder Theorem were utilized to construct a secret sharing scheme, which is the first time that the concept of asymptotic secret sharing is extended to multi-group secret sharing schemes. Li et al. [18] employed the Chinese Remainder Theorem to construct a group secret sharing scheme, but it cannot share a large number of secrets efficiently. Yang et al. [19] constructed an image secret sharing scheme based on group cooperation using homomorphic Lagrangian interpolation, which realizes the sharing of secret images within and between groups, however, the number of secrets is limited to one. Wu et al. [20] proposed a group-based image secret sharing scheme that only allows for all-or-nothing recovery, and once a participant provides a dishonest share, the secret image will not be recovered.

Existing group secret sharing schemes usually adopt an all-or-nothing approach to image secret sharing, which does not take into account the differences in the level and importance of image information, leading to inefficiencies in some cases. Secret image sharing is often accompanied by complex contexts, and group-based scheme [20] for all-or-nothing image recovery are inflexible and not applicable to complex application scenarios. Therefore, the diverse demands of various application scenarios necessitate the development of more adaptable progressive secret image sharing schemes, tailored to accommodate these evolving requirements.

To ensure the security of different level information in the images, we propose a global

progressive image secret sharing scheme based on multi-group joint management. Specifically, the present scheme utilizes bit-polar decomposition and priority assignment to give priority to groups, and the group with higher priority will receive a shared share of the image with higher pixel bits. Within each group, the Chinese Remainder Theorem is utilized to design an intra-group secret sharing scheme with participants having different weights. In the recovery phase, each group recovers the shared copies of the held images using Birkhoff interpolation and the Chinese Remainder Theorem, where Birkhoff interpolation can effectively fill in the missing image pixels. Intergroups utilize lightweight superposition operations for global progressive recovery of images. Even if a group is unable to fully recover an image, it is possible to recover the image gradually by cooperating with other groups, improving the efficiency of sharing.

The sections of this paper are organized as follows. The preparatory knowledge is presented in Section 2, the overall scheme design is presented in Section 3, the analysis and proof of the scheme is in Section 4 and the conclusion of the paper is given in Section 5.

2. Preliminaries

2.1. Explanation of notations

The notations in Table 1 are used throughout this paper.

Table 1. Notations.

Notation	Description
D	Secret distributor
S	Secret image
G_i	Secret participating group
n_i	The number of participants in G_i
$G_{i,j}$	The *j*-th participant in G_i
$W_{i,j}$	The weight of $G_{i,j}$
t_i	The threshold of G_i
P_i	The sub-image after bipolar decoding.
$s_{i,j}$	The secret share of $G_{i,j}$
I_i	Image restoration of G_i

2.2. Bit-polar decomposition

Lakac et al. [10] originally proposed the concept of bit-level decomposition for image sharing. Let $B(O) = \{b_{m-1}, \cdots, b_2, b_1, b_0\}$ be the set of bit-planes of a certain pixel in image O in Figure 1, where *m* is the depth of a pixel, and *m* belongs to $\{m \mid 1 \le m \le 8, m \in Z^+\}$. b_0 is the least significant bit (LSB), and $b_{m\text{-}1}$ is the most significant bit (MSB). Based on the characteristics of a pixel value, the bits in $B(O)$ follows a partial ordering $b_{m-1} > b_{m-2} > ... > b_0$, where $b_i > b_j$ means that b_i is more significant than b_j, or simply $i > j$. In general, in a binary system, the changing of higher bits has a significant impact on the value, while the changing of lower bits has a smaller impact on the value. The partial ordering of the bits in $B(O)$ by their significance implies the presence of priority among

the bits. According to the desired group priority criteria, this solution assigns decomposed secret images at bit-level to each group and then shares image pixels with different bit depths.

The priority decomposition divides the image O into *n* partitions $P_1, P_2, \cdots, P_n$ satisfying Eq (1).

$$\begin{cases} \bigcup_i B(P_i) = B(\mathrm{O}) \ for 1 \le i \le n \\ B(P_i) \cap B(P_j) = \phi \ for 1 \le i \ne j \le n \end{cases} \tag{1}$$

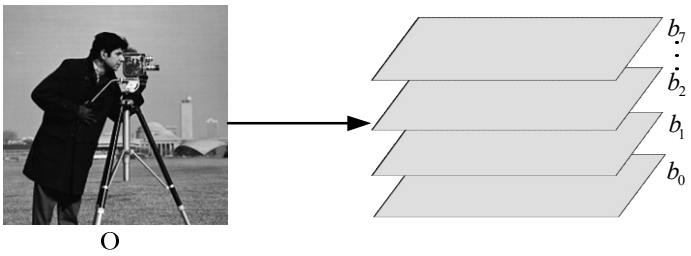


Figure1. The set of bit-planes of a certain pixel in image O.

2.3. Birkhoff interpolation

The secret sharing scheme based on Birkhoff interpolation uses a different polynomial interpolation method compared to Shamir's secret sharing scheme, which supports a higher number of polynomials, thus supporting a larger number of participants with higher efficiency and stronger security. Therefore, this scheme applies Birkhoff interpolation to the secret recovery process, which makes the scheme have better protection performance.

Definition 1. Definition that $X = \{x_1, x_2, ..., x_k\}$, where $x_1 < x_2 < ... < x_k$. $\boldsymbol{E}$ is a interpolation matrix with binary entries which is defined as $\boldsymbol{E} = (e_{i,j})_{1 \le i \le k, 0 \le j \le l}$, where $I(\boldsymbol{E}) = \{(i, j) : e_{i,j} = 1\}$ and $N = |I(\boldsymbol{E})|$. C is a set of *N* real values which is defined as $C = \{c_{i,j} : (i, j) \in I(E)\}$.

The corresponding Birkhoff interpolation problem [21] is $< X, E, C >$ a problem of finding a polynomial $P(X) \in R_{N-1}[x]$ satisfying N equations $P^{(j)}(x_i) = c_{i,j}(i, j) \in I(E)$. Where $P^{(j)}(x_i)$ is the $j - th$ derivative of $P(x)$ and $R_{N-1}[x]$ is the set of all possible polynomials of order at most $N - 1$.

Theorem 1. Let the Birkhoff interpolation problem corresponding to the triple $< X, E, C >$ be will posed, where E satisfies Eq (2).

$$\forall t, (0 \le t \le l) : \sum_{j=0}^{t} \sum_{i=1}^{k} e_{i,j} \ge (t+1) \tag{2}$$

where l is the highest derivative order in the data and k is the number of interpolation points.

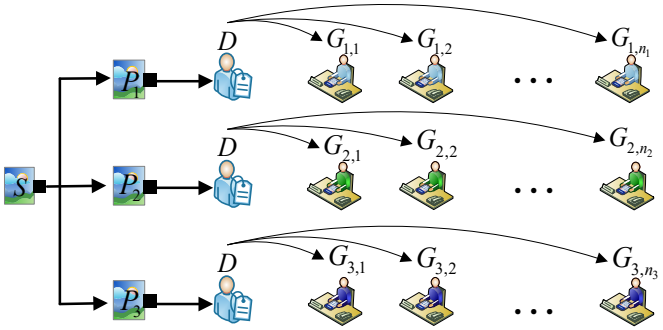
Theorem 2. This interpolation problem (Definition 1) has a unique solution if the interpolation matrix E satisfies Theorem 1 and does not contain supported *l*-odd length sequences.

Theorem 3. If the conditions in Theorem 2 and the following conditions co-exist, there exists a unique solution to the Birkhoff interpolation problem over the finite domain $GF(q)$ as shown in Eq (3). where l is the highest order derivative in the data.

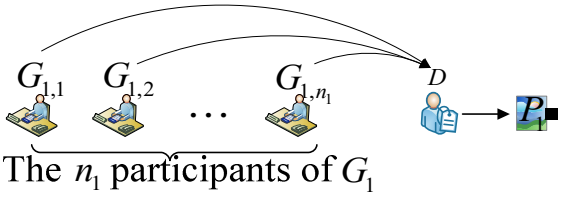
$$q > 2^{-l+2} \times (l-1)^{\frac{l-1}{2}} \times (l-1)! \times x_k^{\frac{(l-1)(l-2)}{2}} \tag{3}$$

3. The proposed scheme

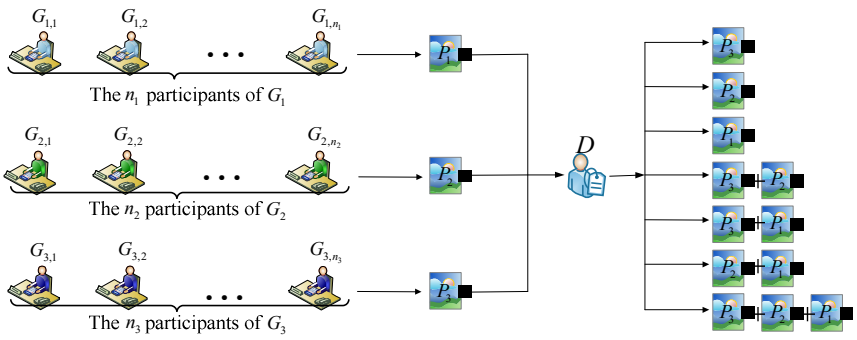
In this paper, a global progressive image secret sharing scheme based on multi-group joint management is developed, as shown in Figure 2. The secret image S is classified into secret levels using the bit-polar decomposition technique, and then different groups G_1, G_2 and G_3 are assigned to the sub-images P_1, P_2 and P_3 with different secret levels, respectively, such that each group is prioritized $G_1 > G_2 > G_3$. As shown in Figure 2(a), G_1 may utilize the group's sub-image P_1 to generate an intra-group secret share $s_{1,j}$ to be assigned to each participant within G_1. As shown in Figure 2(b), when the secret image is recovered, $G_{1,j}$ cooperate to fully recover P_1, and participants within G_2 and G_3 can fully recover P_2 and P_3. As shown in Figure 2(c), when cooperating between groups, each G_i can make the clarity of the recovered image gradually increase by overlaying the sub-image P_i, which realizes the global progressive recovery effect.



(a) Secret sharing



(b) Shared image P_1 recovery



(c) Secret image recovery

Figure 2. Schematic diagram of the scheme.

3.1. Parameter selection

Given a secret image S of size $m \times r$. The scheme contains a trusted secret distributor D, a bulletin board and three participant groups G_1, G_2 and G_3. D can post and update content on the bulletin board, and others can only read or download it. G_1 consists of n_1 participants, and so on. G_i consists of n_i participants, $n = n_1 + n_2 + n_3$. $G_{i,j}$ denotes the *j*-th participant of the *i*-th group, and the weight of each participant is $W_{i,j}$. In addition, each group has a corresponding threshold requirement, such that the threshold for G_1 is t_1, and the threshold for G_i is t_i. The corresponding sub-image can be reconstructed only if the sum of the weights of the participants in the group satisfies the threshold of the corresponding group. The sub-secrets of the participants in the group in this scheme are selected and saved by themselves and can be used multiple times.

D chooses two large prime numbers *p* and *q* at random and computes the product $N = pq$, satisfying the attacker that it is computationally infeasible to derive the sum *p* is *q* knowing *N*. D picks a random *g* in $\left[\sqrt{N}, N\right]$ satisfying $g^{\frac{(p-1)(q-1)}{2}} = 1 \bmod N$. Pick s_0 at random in $[2, N]$ such that s_0 and $(p-1)(q-1)$ are mutually prime, compute $p_0 = g^{s_0} \bmod N$, and compute the smallest positive integer *h* such that $s_0 h = 1 mod \varphi(N)$, which will keep s_0 secret and $\{g, N, p_0, h\}$ public.

3.2. Image preprocessing

For convenience, this section divides the secret image S into 3 different quality sub-images P_1, P_2 and P_3, as shown in Eq (4). The higher the hierarchy of the sub-image, the more information it contains. Distribute sub-images P_i to G_i, where priority $G_1 > G_2 > G_3$. In the image reconstruction pahse, the secret image can be reconstruction progressively by using sub-images from different groups.

$$\begin{cases} B(P_1) = \{b_7, b_6\} \\ B(P_2) = \{b_5, b_4\} \\ B(P_3) = \{b_3, b_2, b_1, b_0\} \end{cases} \tag{4}$$

3.3. Secret sharing

During the image preprocessing, the secret image generates authorized sub-images for different groups. During the pixel allocation process, D uses the pixel values of the sub-image as coefficients of a polynomial. Participants randomly select sub-secrets and perform computations using these sub-secrets to generate public identifiers. D verifies the participant identities to ensure that each participant's identity is unique. Once the uniqueness of the participant's identity is verified, D distributes to each participant a share of the computed secrets, which are generated based on a polynomial computation, to ensure the security of the secrets. The algorithm process is shown in Algorithm 1.

Algorithm1. Secret sharing algorithm

Input: Sub-image P_i.

Output: Secret share $S_{i,j} = y_{i,j}(k)$.

Step1: Iterate over each row of pixel a_i in the sub-image P_i in turn. Constructing polynomials $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$.

Step2: $G_{i,j}$ randomly selects $x_{i,j}$ as the private key to be saved, calculates the public identity $y_{i,j} = g^{x_{i,j}} \bmod N$, and sends $y_{i,j}$ to D.

Step3: After receiving $y_{i,j}$, D assesses the public identity identifiers held by any two different participants $G_{i,j}$ and $G_{i,k}$. If $y_{i,j} = y_{i,k}$, an alarm is triggered, and both parties are required to resend. If $y_{i,j} \neq y_{i,k}$, proceed to step 4.

Step4: D computes $H_{i,j}(x) = f(x) \bmod (x - y_{i,j})^{w_{i,j}}$.

Step4: D computes $H_{i,j}(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{n_i - 1} x^{n_i - 1}$ and distributes $S_{i,j} = H_{i,j}(x)$ as a secret share to the $G_{i,j}$.

By collaborating between participating groups, the secret share generation process constructed using Algorithm 1 is shown in Figure 3.

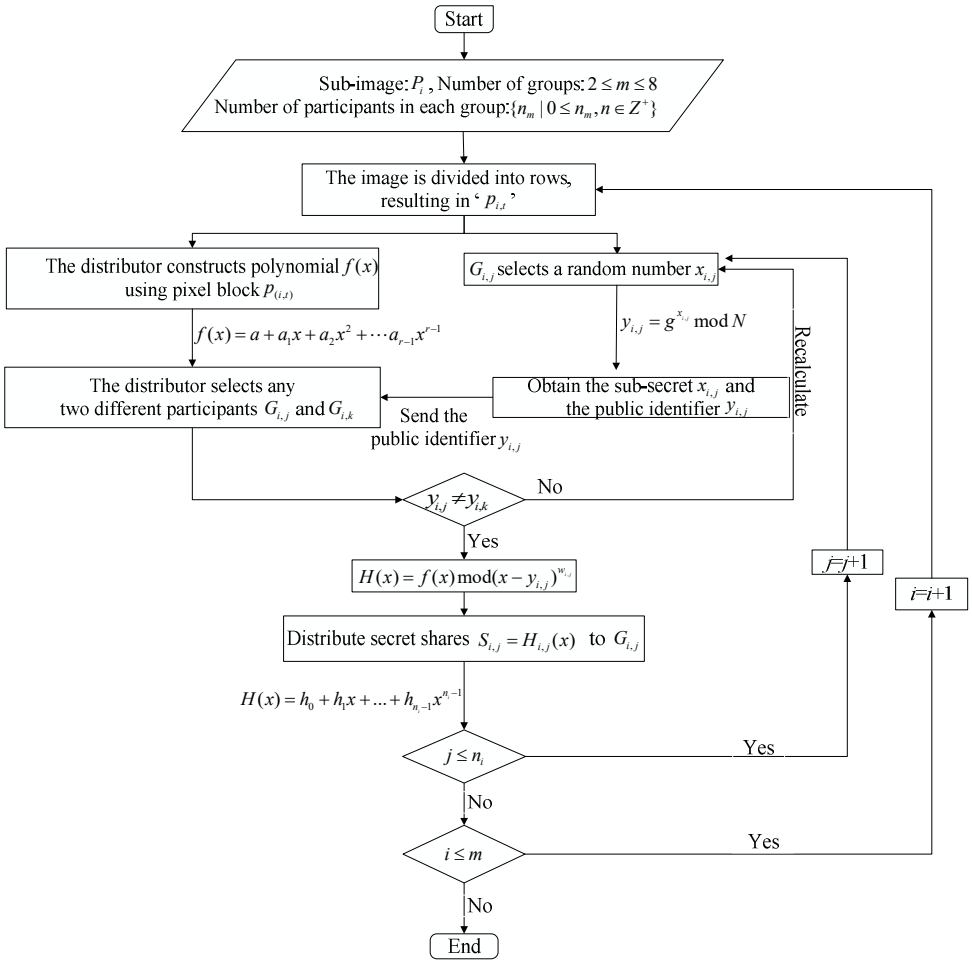


Figure 3. Secret share generation diagram.

3.4. Secret recovery

Secret recovery consists of two parts: Intra-group recovery and inter-group recovery. $G_{i,j}$ hold their own secret shares $s_{i,j}$ and restore the corresponding sub-image P_i by using the Chinese Remainder Theorem and Birkhoff interpolation, revealing partial information. During inter-group recovery, any group overlays their own sub-images P_i, and the image corresponding to pixel depth will be restored, while the remaining bit depths will remain in a noisy state. The algorithm process is shown in Algorithm 2.

Algorithm2. Secret reconstruction algorithm

Input: $S_{i,j} = H_{i,j}(x)$.

Output: Reconstruction Image I_i.

Step1: Identity verification process. Participant $G_{i,j}$ calculates $A_{i,j} = p_0^{x_{i,j}}$. D verifies if ${A_{i,j}}^h = y_{i,j}$ based on the public identity identifiers $y_{i,j}$ and *h* of the participants. If ${A_{i,j}}^h = y_{i,j}$, then $G_{i,j}$ is considered not deceiving, and the identity verification is passed. If ${A_{i,j}}^h \neq y_{i,j}$, an alarm will be sent to $G_{i,j}$, requesting a resend.

Step2: From the $S_{i,j}$ of $G_{i,j}$, the coefficients of $H_{i,j}(x)$ can be found according to the Birkhoff interpolation, which leads to $H_{i,j}(x)$.

Step3: D calculates $\sum_{ij=1}^{t'} w_{ij} \geq t_i$ and determines whether it is valid. If $\sum_{ij=1}^{t'} w_{ij} \geq t_i$, this means that the set of participants intending to participate in the recovery are qualified to participate in restoring the sub-image of their respective group. If $\sum_{ij=1}^{t'} w_{ij} < t_i$, it indicates that they are not qualified to participate in the recovery.

Step4: Under the condition that the identity of the participant is confirmed to be true and $\sum_{ij=1}^{t'} w_{ij} \geq t_i$ is judged to be valid, the Chinese Remainder Theorem is applied to uniquely solve $Y = \sum_{i=1}^{n} r_i \cdot M_i \cdot b_i (\mathrm{mod} M)$, where $M = \prod_{i=1}^{n} m_i$, $b_i = M_i^{-1} (\mathrm{mod}\, m_i)$ and the only polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$ with a number of times of $r-1$ is computed according to $H(x) = f(x) \bmod (x - y_{i,j})^{w_{i,j}}$, and the group can be recovered by the pixel value of the corresponding sub-image P_i.

Step5: By overlaying the recovered sub-images from each group in the inter-group operation, the reconstruction image I_i has a globally progressive recovery effect.

Using Algorithm 2 for intra-group and inter-group image restoration, the restoration process is shown in Figure 4.

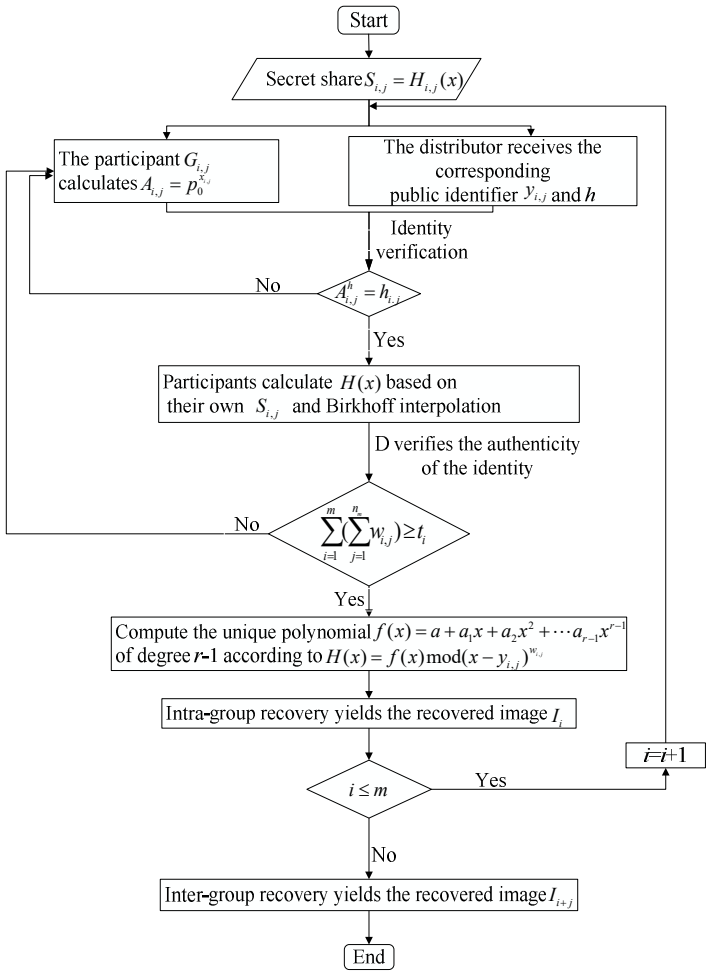


Figure 4. Image reconstruction schematic.

3.5. Correctness

3.5.1. Identity verification

The identity verification step described in Section 3.4 of this paper, constant Eq (5) holds.

$$A_{i,j}{}^{h} = y_{i,j} \tag{5}$$

Proof. During the secret recovery phase, it is not possible for $G_{i,j}$ to provide fake shares $A_{i,j}$ to D. Because D verifies whether the equation $A_{i,j}{}^{h} = y_{i,j}$ holds after receiving the shares $A_{i,j}$ provided by $G_{i,j}$, where $A_{i,j}{}^{h} = p_0{}^{x_{i,j}h} = g^{s_0 x_{i,j} h} = \left(g^{s_0 h}\right)^{x_{i,j}} = g^{x_{i,j}} = y_{i,j}$. Only proceeds to the next step if the verification passes.

3.5.2. Secret recovery

In this paper, in the secret recovery algorithm in Section 3.4, the secret share $S_{i,j} = H_{i,j}(x)$, the secret image can be recovered efficiently using the designed Algorithm 2.

Proof. The secret share $S_{i,j} = H_{i,j}(x)$ held by the authenticated $G_{i,j}$ is derived from the coefficients

of $H_{i,j}(x)$ based on Birkhoff interpolation, which leads to $H_{i,j}(x)$. Then applying the Chinese Remainder Theorem, calculate *f(x)* (The coefficients of *f(x)* are the pixel values of the corresponding region of the recovered image).

1) Find $H_{i,j}(x)$ based on the secret share $S_{i,j} = H_{i,j}(x)$.

The basic idea of Birkhoff interpolation is to construct an interpolation polynomial based on known data points, which can approximate and interpolate between these points. The key of this method is to transform the known data points into a coefficient matrix and solve for the coefficients of the polynomial through matrix operations. As shown in Eq (6), this scheme constructs a vector $\boldsymbol{S} = [S(x_0), S(x_1), ..., S(x_r)]$ consisting of the secret shares $S_{i,j}$ of $G_{i,j}$. Construct a Vandermonde matrix $\boldsymbol{V}$ by arranging the pairs $(x_i, S(x_i))$ as rows or columns of the matrix. Where *r* is the number of pixel points, n_i is the degree of the polynomial $H_{i,j}(x)$ being solved, and G_i is the number of participants involved. Assuming that the coefficient matrix of the polynomial $H_{i,j}(x)$ is C, solves for $\boldsymbol{C}$ in $\boldsymbol{C} = \boldsymbol{V}^{-1} \cdot \boldsymbol{S}$, and then obtain $H_{i,j}(x)$ by solving the equation.

$$\boldsymbol{V} = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n_i} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n_i} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & x_r & x_r^2 & \cdots & x_r^{n_i} \end{bmatrix} \tag{6}$$

2) After obtaining $H_{i,j}(x)$, *f(x)* can be solved by the Chinese Remainder Theorem through $H(x) = f(x) \bmod (x - y_{i,j})^{w_{i,j}}$, where the coefficients of *f(x)* correspond to the pixel values of the image in the corresponding region.

The Chinese Remainder Theorem is a mathematical method used to solve a system of congruent equations. According to the congruent equation $H(x) = f(x) \bmod (x - y_{i,j})^{w_{i,j}}$, obtain $f(x) = H(x) \bmod (x - y_{i,j})^{w_{i,j}}$. Therefore, by solving $H_{i,j}(x)$ modulo $(x - y_{i,j})^{w_{i,j}}$, determine the function *f(x)*. First, calculate the modulus *m*. According to the given condition, $m = (x - y_{i,j})^{w_{i,j}}$. Then, calculate the value of the function $H_{i,j}(x)$ and perform modulo *m* operation on it, which is $H(x) \bmod m$.

According to the mathematical definition, $H(x) \bmod m = H(x) - m \times floor(\frac{H(x)}{m})$, where $floor(\frac{H(x)}{m})$ represents the floor of $\frac{H(x)}{m}$. By substituting $m = (x - y_{i,j})^{w_{i,j}}$ into the equation, get $H(x) \bmod m = H(x) - (x - y_{i,j})^{w_{i,j}} \times floor(\frac{H(x)}{(x - y_{i,j})^{w_{i,j}}}) = f(x)$, where the coefficient of *f(x)* represents the pixel value of the corresponding region in the restored image.

3.6. Security analysis

1) Protects against external attacks. It is infeasible for an attacker to try to derive a sub-secret $x_{i,j}$ of $G_{i,j}$ through the open $y_{i,j}$.

Proof. It is not possible for an attacker to download the information $y_{i,j}$ of $G_{i,j}$ from the bulletin board and try to obtain the participant's sub-secret $x_{i,j}$. Due to the difficulty of solving discrete logarithms, it is computationally infeasible to calculate $x_{i,j}$ given $y_{i,j}$ and g, as $y_{i,j} = g^{x_{i,j}} \bmod N$.

2) Reusable sub-secrets. When it is necessary to reassign the secret image, D randomly selects s_0 from $[2, N]$ again and constructs a new polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$ with degree r-1. Meanwhile, D calculates $H(x) = f(x) \bmod (x - y_{i,j})^{w_{i,j}}$ for each participant and updates their secret shares $s_{i,j}$ without changing their sub-secrets $x_{i,j}$, so each participant can use their sub-secret multiple times.

3) During the recovery process, when the number of participants in G_i does not satisfy the threshold condition t_i, G_i may not recover the corresponding sub-image to ensure the security of the scheme.

Proof. In this scheme, to recover the shared sub-image P_i, it is necessary to reconstruct an r-1 degree polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$. During the secret recovery process, it is required that the sum of weights of participants in $G_{i,j}$ reaches the threshold value t_i, in order to guarantee accurate calculation of $m = (x - y_{i,j})^{w_{i,j}}$. Then, the r-1 degree polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$ can be further calculated using the pixel values of the sub-image P_i. For sub-images P_i with different priorities, if the sum of weights of the participants in $G_{i,j}$ does not reach the threshold value t_i, it will not be possible to calculate $m = (x - y_{i,j})^{w_{i,j}}$, and hence the correct r-1 degree polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1}$ cannot be obtained, resulting in unsuccessful image recovery in the group recovery process of the image I_i. In this case, the cooperation between this authorized group and other groups cannot successfully recover the image I_{i+j}, and hence it is not possible to perform inter-group recovery.

4. Experiment and analysis

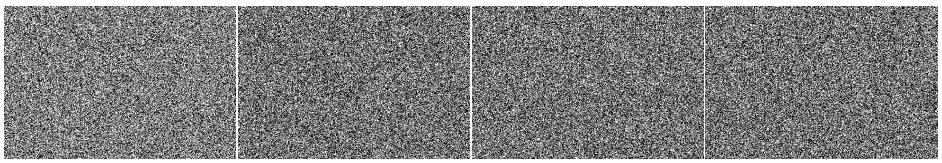
This chapter presents the experimental results of our proposed approach, and we evaluate the effectiveness of the scheme through experiments and analysis.

4.1. Experimental result

This section provides an example of this scheme to illustrate the generation of secret shares and the reconstruction of images. This section verifies the proposed scheme by taking, for example, three groups, and suppose there are three separate groups $G_i (i = 1, 2, 3)$, where the priority of $G_1 > G_2 > G_3$. The secret message obtained from G_1 is the clearest, while the secret message obtained from G_3 is the closest to black, making the secret message almost unobservable through the visual system. Figure 5(a) serves as the secret image, and Figure 5(b)–(d) shows each group of sub-image. Figures 6–8 show the secret shares sent to participants within the G_1, G_2, G_3.

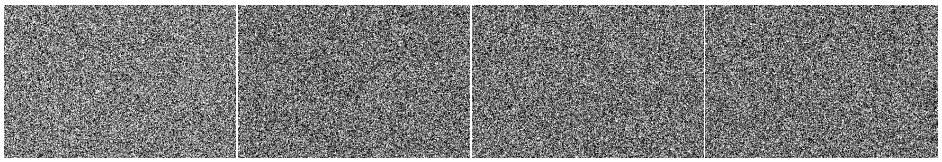
(a) S (b) P_1 (c) P_2 (d) P_3

Figure 5. (a) Secret image, (b)–(d) Sub-images distributed to G_1–G_3.



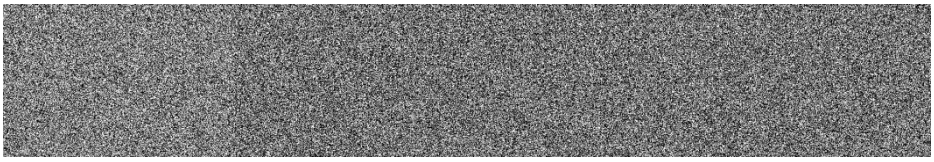
(a) $s_{1,1}$ (b) $s_{1,2}$ (c) $s_{1,3}$ (d) $s_{1,4}$

Figure 6. Secret shares of $G_{1,j}$.



(a) $s_{2,1}$ (b) $s_{2,2}$ (c) $s_{2,3}$ (d) $s_{2,4}$

Figure 7. Secret shares of $G_{2,j}$.



(a) $s_{3,1}$ (b) $s_{3,2}$ (c) $s_{3,3}$ (d) $s_{3,4}$

Figure 8. Secret shares of $G_{3,j}$.

The security of secret image in this scheme is demonstrated by experimental results. In Figure 9(a), when the secret shares of the 3 participants, denoted as $G_{1,j}$, do not satisfy the threshold condition, the reconstructed image appears as a random pattern. However, in Figure 9(b), when the secret shares of the 4 participants, also denoted as $G_{1,j}$, meet the threshold condition, the corresponding sub-images can be successfully reconstructed. In other words, only the participants who satisfy the threshold condition can participate in the effective image recovery process, while those who do not satisfy the threshold condition cannot be involved in image reconstruction.

(a) (b)

Figure 9. (a) Three participants from G_1 participated in the recovery; and (b) Four people from G_1 participated in the recovery.

After obtaining the corresponding sub-images P_i, cooperation between different groups was carried out to recover the secret image. Specifically, in Figure 10(a)–(c), the image restoration process was completed through cooperative efforts between the pairs G_2+G_3, G_1+G_3 and G_1+G_2, respectively. It is worth noting that these cooperative methods are determined based on the selection of participants. In addition, in Figure 10(d), three groups, $G_1+G_2+G_3$, participated in the restoration process simultaneously, and the secret image was successfully reconstructed. This result indicates that cooperation among multiple groups can significantly improve the efficiency and robustness of image restoration.

(a) I_{2+3} (b) I_{1+3} (c) I_{1+2} (d) I_{1+2+3}

Figure 10. (a)–(c) Two groups participated in the recovery; and (d) Three groups participated in the recovery.

The groups involved in the recovery are G_1, G_2 and G_3, where the priority is $G_1 > G_2 > G_3$. During the recovery process, the group with higher priority will restore a higher quality image. As shown in Figure 10(b),(c), the restored images I_{1+2} and I_{1+3}, which were restored through the collaboration of G_2 and G_3, respectively with G_1, demonstrate clear outlines but fail to fully recover and have lost some details. Additionally, G_2 has higher priority over G_3. Under the premise of G_1 participation, the image I_{1+2}, restored through the collaboration of G_1 and G_2, is clearer than the image I_{1+3}, restored through the collaboration of G_1 and G_3. Due to the lower priority of G_2 and G_3, their collaborative restoration results in a less prominent feature in the restored image I_{2+3}, as illustrated in Figure 10(a). When all three groups, G_1, G_2 and G_3, participate in the restoration simultaneously, as shown in Figure 10(d), the restored image I_{1+2+3} exhibits the best image quality. At this point, the detailed information in the image has been nearly fully restored, resulting in a higher level of clarity and accuracy in the overall image.

During the secret restoration process, different collaborative groups have varying priorities and restoration effects. The quality of the restored image is influenced by the number of participating groups and their priorities. As the number of participating groups gradually increases, the clarity and accuracy of the secret image improves, gradually moving away from its initial blurry state. When the

number of groups is the same, the degree of improvement in clarity depends on the priority assigned to each group, with higher-priority groups helping to obtain clearer image information. In particular, when collaborating groups have a higher collective priority, the clarity and accuracy of the restored secret image are enhanced. Optimizing collaborative restoration strategies can significantly improve the quality and accuracy of the restored image.

4.2. Noise attack

Image data is inevitably affected by various subjective and objective factors that cause pixel interference during transmission. To verify the impact of pixel interference on secret images before recovery, this section uses "Lena" and "Peppers" with a size of 264 × 173 as secret images, as shown in Figure 11. The results of the recovery process are shown in Figures 12 and 13. The recovered images were also tested after adding salt-and-pepper noise with a strength of 2% to the secret shares, as shown in Figures 14 and 15.

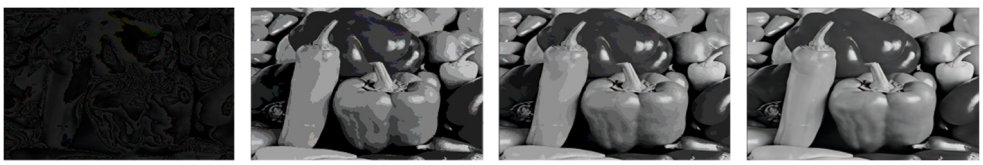
Since the naked eye system has limitations in determining the quality of image restoration, precise computational methods are needed to measure the quality of image restoration. This section uses the mean square error (MSE) and peak signal to noise ratio (PSNR) to analyze the image recovery performance under noise.

(a) Lena (b) Peppers

Figure 11. The secret image.

(a) I_{2+3} (b) I_{1+3} (c) I_{1+2} (d) I_{1+2+3}

Figure 12. (a)–(c) Two groups participated in the recovery; and (d) Three groups participated in the recovery.

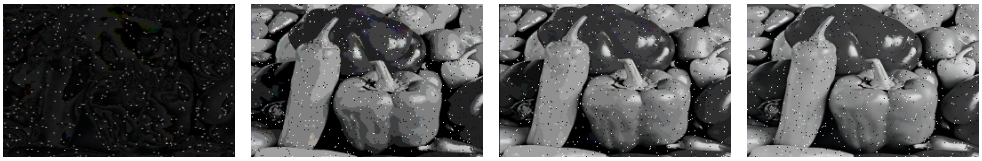


(a) I_{2+3} (b) I_{1+3} (c) I_{1+2} (d) I_{1+2+3}

Figure 13. (a)–(c) Two groups participated in the recovery; and (d) Three groups participated in the recovery.

(a) I_{2+3} (b) I_{1+3} (c) I_{1+2} (d) I_{1+2+3}

Figure 14. Recovered image after intensity 2% noise attack.



(a) I_{2+3} (b) I_{1+3} (c) I_{1+2} (d) I_{1+2+3}

Figure 15. Recovered image after intensity 2% noise attack.

By analyzing experimental data, when the MSE value is smaller and the PSNR value is larger, the reconstructed image is more similar to the original image and the difference between the two is smaller. When the PSNR is higher than 40 dB, it indicates that the quality of the recovered image is extremely good and very close to the secret image. When the PSNR is between 30~40 dB, it indicates that the image quality is good. The MSE and PSNR between two given images P_1 and S, with sizes of $m \times n$, are defined as Eqs (7) and (8).

$$\mathrm{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left| P_1(i,j) - S(i,j) \right|^2 \tag{7}$$

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{255^2}{\mathrm{MSE}} \right) \tag{8}$$

According to Tables 2 and 3, it can be observed that with inter-group collaboration, the PSNR of the recovered images is between 30 dB and 59 dB, while the MSE remains between 0.007 and 0.010. This indicates that the higher the priority of G_i involved in the recovery, the better the quality and PSNR of the corresponding recovered image. With the increase in noise attack intensity and cooperation group, it is inevitable that there will be some impact on the reconstruction of the secret, but it is within the visible range. Therefore, this scheme exhibits good robustness to noise attacks.

Table 2. MSE comparison of the secret images before and after recovery.

Image	MSE						
	I_1	I_2	I_3	I_{1+2}	I_{1+3}	I_{2+3}	I_{1+2+3}
School	0.0086762	0.0101109	0.0102801	0.0083329	0.0085976	0.0092178	0.0077101
Lena	0.0092364	0.0097547	0.0098518	0.0084010	0.0085517	0.0094234	0.0081386
Peppers	0.0088518	0.0089732	0.0096518	0.0082565	0.0086374	0.0088647	0.0078360

Table 3. PSNR comparison of the secret images before and after recovery.

Image	PSNR						
	I_1	I_2	I_3	I_{1+2}	I_{1+3}	I_{2+3}	I_{1+2+3}
School	47.7	31.6	27.5	58.0	57.6	46.3	58.3
Lena	49.4	35.6	22.0	57.5	54.0	48.1	58.1
Peppers	47.6	35.9	29.3	58.8	56.6	44.0	59.0

4.3. Performance analysis

The comparison between some related progressive image secret sharing schemes and the proposed scheme is shown in Table 4.

Table 4. Comparison of this scheme with the existing ISS schemes.

Scheme	Security level	Identity verification	Sub-secret reusable	Participant characteristics	Inter-group characteristics	Intra-group characteristics	Progressive
[9]	High	No	No	One group	No	Equally	No
[12]	Low	No	No	One group	No	The importance of difference	Yes
[13]	High	No	No	One group	No	Equally important	Yes
[14]	High	No	No	One group	No	Equally	Yes
[15]	Low	No	No	One group	No	Equally	Yes
[20]	High	No	No	Multiple group	No prioritization	Equally important	No
This scheme	High	Yes	Yes	Multiple group	Priority exists	The importance of difference	Yes

First, there is a comparison of the level of security, as shown in the first column of Table 4. This scheme is superior to the scheme of Guo et al. [12] in terms of safety. It embeds secret pixel values into all coefficients of a polynomial, which may lead to unauthorized participants recovering the secret image, thus resulting in lower security. In the proposed scheme in this article, the secret image is divided into sub-images with different priorities, and secret sharing operations are performed on these sub-images, thus enhancing the security level of the secret image.

Second, there is a comparison of the features used to verify the identity information of participants, as shown in the second column of Table 4. References [9,12–15,20] does not verify the identity of

participants, which cannot prevent internal fraud, allowing adversaries to infiltrate and obtain information about the secret image using incorrect information. In this scheme, D verifies the identity information of participants by using the publicly available $y_{i,j}$ to calculate $A_{i,j}{}^{h} = y_{i,j}$.

Third, as shown in the third column of Table 4, in this scheme, the secret share of each participant can be utilized for multiple secret sharing processes without necessitating any updates. References [9,12–15,20] has no reusable sub-secrets, and the secret shares need to be redistributed during each secret sharing process.

Fourth, there is a comparison of the characteristics of participants, as shown in the fourth column of Table 4. The participants in references [9,12–15] belong to a group, so the secret image is managed by a single group. In real life, secret images need to be managed by multiple groups. Therefore, the scheme in this paper is more suitable for visual passwords.

Fifth, only in this scheme there is prioritization among groups. In fact, it is unlikely that multiple groups co-managing mutual trade-offs can achieve complete equality in the true sense, and the priority assignment in this paper plays a decisive role in achieving global progressive recovery.

Sixth, the shares generated by [13,20] have equal importance. Typically, individuals within a group are further classified into management members and regular members. Different access levels to classified information are assigned to members based on their importance levels. As a result, the proposed scheme in this paper is more versatile. In this scheme, each group has a specific threshold. When the sum of participant weights reaches the threshold, the corresponding sub-image can be restored. Compared to traditional (k,n) threshold schemes, this solution offers enhanced security.

Finally, as shown in Table 4, Xie et al. [9] proposed a low-cost CS based multi-party secret image sharing scheme that enhances security through permutation and blurring, but it is not progressively recoverable. Guo et al. [12] resolved the issue of achieving only fully recovered or unrecovered images, and proposed non-expandable hierarchical shadowing for reconstructed images. Both [14] and [15] implemented a hierarchical structure, but without scalability. Wu et al. [20] is a joint multi-group image secret sharing scheme, but the reconstructed images are either fully recovered or not recovered at all. This scheme combines their strengths to achieve both hierarchy and progression, and secret images can be divided into arbitrary levels according to actual needs.

5. Conclusions

In this paper, we introduce a novel global progressive image secret sharing scheme that combines group secret sharing with a progressive secret sharing system. The proposed scheme utilizes multi-group joint management to allow for global progressive recovery with varying priorities. Throughout the sharing process, the scheme employs bit-polar decomposition to divide the depth of the secret image's pixels, enabling groups to establish diverse priorities. During the recovery process, Birkhoff interpolation ensures the recovery of secret images within groups. Using lightweight superposition operations, distinct layers of secret images can be recovered with global progressivity among groups. In addition, the reuse of participant secret shares can effectively prevent external attacks. The scheme, as presented in this paper, finds potential application in transmitting product design diagrams. Future research will focus on detecting potential spoofing on the distributor's end and exploring methods for decentralizing the distributor's rights based on the current scheme.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors thank the anonymous reviewers for their valuable comments. This work was supported by Xi'an Science and Technology Plan Project (No. 22GXFW0063); Shaanxi Provincial Department of Science and Technology Youth Project (Nos. 2021JQ-575 and 2021JQ-576); Shaanxi Provincial Department of Education Project (No. 19JK0526).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. Z. Yu, H. Gao, X. Cong, N. Wu, H. H. Song, A survey on cyber-physical systems security, *IEEE Internet Things J.*, **10** (2023), 21670–21686. https://doi.org/10.1109/JIOT.2023.3289625
2. P. Sarosh, S. A. Parah, G. M. Bhat, Utilization of secret sharing technology for secure communication: a state-of-the-art review, *Multimedia Tools Appl.*, **80** (2021), 517–541. https://doi.org/10.1007/s11042-020-09723-7
3. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613. https://doi.org/10.1145/359168.359176
4. M. Naor, A. Shamir, Visual cryptography, in *Advances in Cryptology — EUROCRYPT'94*, (1995), 1–12. https://doi.org/10.1007/BFb0053419
5. W. Liu, Y. Xu, J. Chen, C. Yang, A (*t*,*n*) threshold quantum visual secret sharing, *Int. J. Sens. Netw.*, **33** (2020), 74–84. https://doi.org/10.1504/IJSNET.2020.107863
6. C. Thien, J. Lin, Secret image sharing, *Comput. Graphics*, **26** (2002), 765–770. https://doi.org/10.1016/S0097-8493(02)00131-0
7. L. Tan, Y. Lu, X. Yan, L. Liu, L. Li, Weighted secret image sharing for a (*k*,*n*) threshold based on the Chinese Remainder Theorem, *IEEE Access*, **7** (2019), 59278–59286. https://doi.org/10.1109/ACCESS.2019.2914515
8. D. M. Huang, H. F. Xu, Q. He, Y. L. Du, Q. M. Wei, A secret sharing-based authentication scheme for ocean remote sensing images in cloud environment, *Comput. Eng. Sci.*, **39** (2017), 1410–1418. https://doi.org/10.3969/j.issn.1007-130X.2017.08.004
9. D. Xie, B. Wu, F. L. Chen, T. C. Wang, Z. B. Hu, Y. B. Zhang, A low-overhead compress sensing-driven multi-party secret image sharing scheme, *Multimedia Syst.*, **29** (2023), 1187–1202. https://doi.org/10.1007/s00530-023-01049-2
10. Y. Liu, C. Yang, Scalable secret image sharing scheme with essential shadows, *Signal Process. Image Commun.*, **58** (2017), 49–55. https://doi.org/10.1016/j.image.2017.06.011
11. X. Yan, Y. Lu, L. Liu, A general progressive secret image sharing construction method, *Signal Process. Image Commun.*, **71** (2019), 66–75. https://doi.org/10.1016/j.image.2018.11.002
12. C. Guo, C. C. Chang, C. Qin, A hierarchical threshold secret image sharing, *Pattern Recognit. Lett.*, **33** (2012), 83–91. https://doi.org/10.1016/j.patrec.2011.09.030

13. T. Bhattacharjee, S. P. Maity, S. R. Islam, Hierarchical secret image sharing scheme in compressed sensing, *Signal Process. Image Commun.*, **61** (2018), 21–32. https://doi.org/10.1016/j.image.2017.10.012
14. D. Xie, H. J. Zhu, F. L. Chen, B. Wu, J. H. Yang, A compressed sensing-based progressive secret image sharing scheme and security analysis, *Digital Signal Process.*, **143** (2023), 104273. https://doi.org/10.1016/j.dsp.2023.104273
15. X. L. Wang, D. Xie, F. L. Chen, B. Wu, Y. Y. Zen, Progressive and multi-level secret image sharing scheme with hierarchical shadows, *Multimedia Tools Appl.*, **81** (2022), 31039–31059. https://doi.org/10.1007/s11042-022-12951-8
16. R. Xu, X. Wang, K. Morozov, Group authentication for cloud-to-things computing: review and improvement, *Comput. Networks*, **198** (2021), 108374. https://doi.org/10.1016/j.comnet.2021.108374
17. K. Meng, F. Miao, W. Huang, Y. Xiong, Tightly coupled multi-group threshold secret sharing based on Chinese Remainder Theorem, *Discrete Appl. Math.*, **268** (2019), 152–163. https://doi.org/10.1016/j.dam.2019.05.011
18. H. X. Li, L. J. Pang, W. D. Cai, An efficient threshold multi-group-secret sharing scheme, in *Fuzzy Information and Engineering*, (2007), 911–918. https://doi.org/10.1007/978-3-540-71441-5_99
19. C. N. Yang, X. Wu, H. Y. Lin, C. Kim, Intragroup and intergroup secret image sharing based on homomorphic Lagrange interpolation, *J. Inf. Secur. Appl.*, **61** (2021), 102910. https://doi.org/10.1016/j.jisa.2021.102910
20. Z. Wu, Y. Liu, X. Jia, A novel hierarchical secret image sharing scheme with multi-group joint management, *Mathematics*, **8** (2020), 448. https://doi.org/10.3390/math8030448
21. W. G. Ge, Secret sharing scheme based on Birkhoff interpolating polynomial, *J. China Acad. Electron. Inf. Technol.*, **13** (2018), 170–173. https://doi.org/10.3969/j.issn.1673-5692.2018.02.011

AIMS Press