Research Article

A Verifiable Steganography-Based Secret Image Sharing Scheme in 5G Networks

Shiyue Qin ¹, Zhenhua Tan,² Fucai Zhou ², Jian Xu,² and Zongye Zhang²

¹*School of Computer Science and Engineering, Northeastern University, Shenyang, China*

²*Software College, Northeastern University, Shenyang, China*

Correspondence should be addressed to Fucai Zhou; fczhou@mail.neu.edu.cn

Received 17 November 2020; Revised 11 December 2020; Accepted 29 December 2020; Published 28 January 2021

Academic Editor: Jinwei Wang

Copyright © 2021 Shiyue Qin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development and innovation of new techniques for 5G, 5G networks can provide extremely large capacity, robust integrity, high bandwidth, and low latency for multimedia image sharing and storage. However, it will surely exacerbate the privacy problems intrinsic to image transformation. Due to the high security and reliability requirements for storing and sharing sensitive images in the 5G network environment, verifiable steganography-based secret image sharing (SIS) is attracting increasing attention. The verifiable capability is necessary to ensure the correct image reconstruction. From the literature, efficient cheating verification, lossless reconstruction, low reconstruct complexity, and high-quality stego images without pixel expansion are summarized as the primary goals of proposing an effective steganography-based SIS scheme. Compared with the traditional underlying techniques for SIS, cellular automata (CA) and matrix projection have more strengths as well as some weaknesses. In this paper, we perform a complimentary of these two techniques to propose a verifiable secret image sharing scheme, where CA is used to enhance the security of the secret image, and matrix projection is used to generate shadows with a smaller size. From the steganography perspective, instead of the traditional least significant bits replacement method, matrix encoding is used in this paper to improve the embedding efficiency and stego image quality. Therefore, we can simultaneously achieve the above goals and achieve proactive and dynamic features based on matrix projection. Such features can make the proposed SIS scheme more applicable to flexible 5G networks. Finally, the security analysis illustrates that our scheme can effectively resist the collusion attack and detect the shadow tampering over the persistent adversary. The analyses for performance and comparative demonstrate that our scheme is a better performer among the recent schemes with the perspective of functionality, visual quality, embedding ratio, and computational efficiency. Therefore, our scheme further strengthens security for the images in 5G networks.

1. Introduction

Nowadays, a huge amount of data is available in multimedia forms, such as images and videos. With the growing popularity of multimedia data, multimedia sharing has become one of the most popular Internet services. Meanwhile, the emergence of fifth-generation networks (5G) brings many advantages to supply power to such multimedia sharing services. Compared to the actual 4G technologies, 5G will be more flexible and will provide significantly higher bandwidth, as well as robust integrity, more capacity, and very low latency [1]. Such features are fundamental for facilitating information flow and timeliness of data, thus improving sharing services quality. 5G will undoubtedly drive people

and organizations to interact with others more actively and exchange more information in a greater open network environment [2]. However, it may exacerbate the privacy problems intrinsic to multimedia transfer in networks as a result. As image sharing is one of the basic multimedia sharing services, this paper aims to achieve secure image share and storage in 5G networks.

Based on the 5G technique advantages, it is foreseen that 5G will have great potential to handle challenges in various fields, such as smart cities [3], healthcare [4], and industrial control [5], and traffic congestion [6]. In such scenarios, medical images, design drawings, military images, and financial reports [7] always contain massive sensitive information. Hence, the sharing and storing of these images can

be more vulnerable towards several kinds of attacks, such as eavesdropping and tampering. Secret image sharing (SIS) [8, 9] developing from the traditional secret sharing is a promising way to ensure the privacy and integrity of the secret image for distributed storing and sharing in the network. However, ordinary SIS will generate n shadows in the form of noise-like images [10, 11] which might arise suspicious of the invaders [12] during the shadow dissemination. Therefore, steganography-based SIS will further improve the security of SIS systems in a more open 5G network.

A general (k, n) -threshold steganography-based SIS scheme enables a dealer to distribute its secret image among a set of untrusted participants via the public channel. Firstly, the dealer generates n noise-like shadows for the secret image. Then, n shadows are embedded into the preselected meaningful images (called cover images) so as to generate n meaningful stego images. Finally, each of the participants is allocated a stego image. When someone requests the secret's reconstruction, they need to extract enough shadows from the stego images. Only the combination of at least k shadows can perform the lossless reconstruction, and less than k shadows give no clues about the secret image in contrast. Therefore, steganography-based SIS can protect the secret image with higher security because the eavesdroppers cannot detect secret information from meaningful images. However, most of the existed steganography-based SIS schemes have a problem with the pixel expansion, for example, the stego images generated in the schemes of [13–15] are expanded four times the original secret image to realize high-quality steganography. Here, the challenge of proposing steganography-based SIS schemes is to create high-quality stego images so that the modifications are not visually perceptible.

Moreover, the verification ability is necessary to check the validity of the stego images for the secret image reconstruction. If a fake stego image is submitted, the reconstructed image will not be exactly the same as originally outsourced. Cheating detection is one of the methods to locate a set of potential invalid shadows. It is easy to design SIS with verification ability by using hash codes [16–18]. However, most steganography-based SIS with cheating detection ability needs to embed these extra authentication bits into the cover image, which unfortunately leads to high recovery (authentication) complexity and pixel expansion. Therefore, an efficiency verification mechanism is needed to be designed.

Additionally, in 5G network scenarios, a natural extension of such schemes is to consider the attached proactive feature and dynamic feature. The proactive feature is essential in some circumstances that the secret needs to be kept for a very long time, such as medical image records [19]. It can resist persistent adversaries by updating the shadows periodically. The secret cannot be discovered even from enough shadows, which are mixed with past and present shadows. Especially in 5G network environments, the persistent adversary will be more general who can stay in the network all the time. Moreover, the dynamic feature is also practical which supports efficient secret updating without

shadow distribution again. Such a feature is necessary for an SIS scheme to adapt the data flow rate in 5G networks. However, these features are attracted very little attention to SIS.

Therefore, in this paper, we are willing to propose a verifiable steganography-based secret image sharing scheme for 5G networks that achieves the following goals: (1) high-quality stego images without pixel expansion; (2) an efficient cheating verification ability to handle the dishonest participant; (3) lossless reconstruction and low reconstruct complexity; and (4) proactive feature and dynamic feature. To meet the design goals described above, we combine Two-Dimensional Reversible Linear Cellular Automata with Memory (2D-RLCAM) and matrix projection together to design the scheme. 2D-RLCAM is a kind of cellular automata additionally with memory and reversible abilities.

Our contributions are as follows:

- (i) Security enhanced: during the secret distribution procedure, CA is used to preprocess the secret image. Then, the matrix projection-based secret sharing scheme, as introduced in the typical work of Bai and Zou [11], is employed with some changes to generate small shadows. Increased by CA's security, the secret image security is significantly improved to solve the matrix projection's weaknesses.
- (ii) Needless of the consecutive shadows for reconstruction: the consecutive requirement for reversing in CA is embedded into the secret image's sub-matrices, but not directly for the secret image. Hence, the consecutive shadows in this paper are needless for secret reconstruction to overcome CA's weaknesses.
- (iii) High-quality stego images without pixel expansion: matrix encoding is using in this paper for steganography. Our scheme obtains enhancement in both the security of secret image and the visual quality of the stego image, benefiting from smaller shadows and the comparatively slight modification to the cover image.
- (iv) Feature optimization for 5G scenarios: for the verifiable feature, a separate verification matrix is used for cheating detection. It can achieve a relatively low verification complexity based on XOR operations. For proactive and dynamic features, they can be realized with only a few times of matrix operations.
- (v) Lossless reconstruction and low reconstruct complexity: the experiments over the test images demonstrate the effectiveness and efficiency of the proposed scheme via several indices.

The rest of this paper is organized as follows: the related work is given in Section 2. The preliminaries of 2D-RLCAM, the typical work of Bai and Zou [11], and matrix encoding are introduced in Section 3. The procedures of the proposed SIS scheme are discussed in detail in Section 4. The security analyses for persistent adversaries are studied in Section 5. The experimental results based on the real images and

comparative analysis are given in Section 6. Finally, the paper ends with a conclusion in Section 7.

2. Related Work

2.1. SIS. From the literature, Shamir's secret sharing [20] is one of the underlying techniques used to build SIS schemes mostly, but always has the pixel loss problem [21, 22]. In order to solve this problem, several new techniques have been used to devise a new (k, n) -threshold SIS scheme, such as cellular automata (CA) [23, 24] and matrix projection [25].

Compared with Shamir-based SIS, CA-based SIS [12, 15, 26, 27] has more advantages: (1) the computation complexity of CA-based SIS is only $O(n)$, which is more efficient while Shamir-based SIS needs $O(n \log n)$; (2) the consecutive properties in CA provide a stronger security guarantee for the secret image. Nevertheless, most CA-based SIS schemes also exist in some problems: (1) only consecutive shadows can reveal the secret image [15, 26, 27] which limited the availability and (2) the pixel expansion problem still exists. The scheme of Eslami et al. [15] is the first CA-based SIS, which improved tamper detection. However, in this scheme, the shadow's size is the same as the original secret image. If the steganography of these shadows is performed, the pixel expansion problem will be unavoidable. The scheme of Zarepour-Ahmadabadi et al. [12] is a multistage multiset image sharing scheme based on CA and Shamir-based sharing algorithm that each secret image has its own access structure. In this scheme, the secrets can be reconstructed based on their own prespecified order, which can apply to more general and flexible scenarios. However, this scheme executed the Shamir-based sharing algorithm multiple times during the secret distribution and reconstruction, which still made a higher computation complexity.

Matrix projection-based SIS [11, 16, 28] can significantly reduce the size of the shadows. In the basic matrix projection-based (k, n) secret sharing scheme [10], for a $m \times m$ secret matrix, the generated shadows are vectors with the size of only $m \times 1$. Based on it, Bai and Zou [11] construct a proactive secret sharing scheme. The generated shadows in their scheme are $(m + k) \times 1$ vectors. The size of the shadows is still small. Therefore, matrix projection-based SIS can effectively reduce the modifications over the cover images and even create high-quality stego images by avoiding the pixel expansion problem. However, the existing matrix projection-based SIS schemes only generate noise-like image shadows but do not consider combining steganography. Additionally, there are two problems with the existed matrix projection-based SIS schemes: (1) matrix projection-based (k, n) secret sharing scheme is only a strong ramp secret sharing but not perfect secret sharing [25], which may expose information about the secret proportional to the number of the obtained shadows till enough, and (2) without the verification ability [11, 28]. Although the scheme of Azzahra and Sugeng [16] realized cheating detection with the help of an additional authentication image, the dealer must be involved in the reconstruction process. Therefore,

the security and functionality of matrix projection-based SIS need to be improved.

In this paper, we combine Two-Dimensional Reversible Linear Cellular Automata with Memory (2D-RLCAM) and matrix projection together to avoid the weaknesses of these techniques but keeping the advantages.

2.2. Steganography-Based SIS. The least significant bits (LSB) method is one of the most common solutions for steganography. This method directly replaces the least significant bits of some pixels in the cover image with the shadow, such as in Yang et al.'s Shamir-based scheme [13], Chang et al.'s Chinese remainder-based scheme [14], and Eslami et al.'s linear cellular automata- (LCA-) based scheme [15]. These schemes enable the shadow embedding and concealed shadow extraction in a highly efficient way, without any cryptographic computation. However, the above schemes have a problem with the pixel expansion. One of the key reasons is that the generated shadows' size is relatively big. Another reason is that the requirement of the steganography space is relatively big for performing LSB so that the stego image generated in the above schemes is expanded four times the original secret image to realize high-quality steganography.

Matrix encoding (ME) method is another steganography method mainly based on some XOR operations, rather than direct replacement as in LSB. Hence, the information of the shadow does not directly appear in the pixels of the cover image, which increases the security of the concealed information. Moreover, to hide a 3-bit length secret, at most only 1 bit of a pixel is needed to be changed via the ME method, but usually 3 bits are needed in the LSB method. Hence, ME can realize the comparatively slight modification to the cover image. Compared with LSB, ME needs more computational cost because of some simple XOR operations, but it can obtain enhancement in both the security of secret data and the visual quality of stego images. Therefore, we use ME in our paper to hide the shadow into a cover image.

Moreover, Yan et al. [29] introduced the requirement of lossless reconstruction of the cover images in an SIS scheme. The reversible cover images are needed in several scenarios, such as law enforcement, experimental investigations, and remote sensing [30]. However, the traditional SIS approaches have some limitations for the cover image reconstruction, such as the restrictions of the cover image formats and kinds, or loss reconstruction of the cover image. In the scheme of Yan et al. [29], the lossless reconstruction is realized, but the format of cover images is restricted to the binary image. In this paper, we generate a submatrix for the grayscale cover image to recover it losslessly.

2.3. Verifiable SIS. It is easy to design SIS with verification ability by using hash codes [16–18] or information hiding [15, 26, 31]. Chang et al. [14] used the Chinese remainder theorem (CRT) to generate four authentication bits by using the hash function in order to obtain better authentication ability. Recently, Liu et al. [17] divided each stego image into nonoverlapping blocks with size 1×3 firstly and then

generated two authentication bits for each stego block. This scheme also achieved good visual quality and authentication ability. However, most of the above schemes need to embed these extra authentication bits into the cover image, which unfortunately leads to high recovery (authentication) complexity and pixel expansion. Besides the above solutions, the double verification mechanism [15], the random grid [32], and the extra authentication image [16] were also used to provide a powerful verification of the fake stego images. In the scheme of Azzahra and Sugeng [16], the dealer kept an extra authentication image privately. After the secret reconstruction, the dealer performed the cheating detection by checking if the authentication image is recovered correctly. However, this scheme suffers from drawbacks in that even enough shadows cannot reconstruct the secret image because the dealer must be involved in the reconstruction process. To some degree, the participation of the dealer makes this scheme diverge from the original intention of the secret sharing.

In this paper, we embed a verification matrix into the public known information by XOR operations. It can avoid the problems of high recovery complexity and pixel expansion. Moreover, the valid requester can perform an efficient cheating detection via some simple XOR operations but without the additional help from the dealer.

3. Preliminaries

3.1. Reversible Linear Cellular Automata with Memory. Cellular automaton (CA) is a deterministic and discrete system. This paper deals with two-dimensional CA (2D-CA)

with the cell space of $S_b = \{0, 1, \dots, 7\}$ ($b = 8$) and with transfer function F depending on Moore neighborhood N . 2D Reversible Linear Cellular Automata with Memory (2D-RLCAM) is a kind of CA additionally with memory and reversible abilities.

For a $r \times s$ 2D-CA, if $a_{i,j}^{(t)} \in S_b$ is taken to denote the state of one cell at the position (i, j) at a certain time t , the state of N of it can be represented as follows:

$$N_{i,j}^{(t)} = \begin{pmatrix} a_{i-1,j-1}^{(t)} & a_{i-1,j}^{(t)} & a_{i-1,j+1}^{(t)} \\ a_{i,j-1}^{(t)} & a_{i,j}^{(t)} & a_{i,j+1}^{(t)} \\ a_{i+1,j-1}^{(t)} & a_{i+1,j}^{(t)} & a_{i+1,j+1}^{(t)} \end{pmatrix}. \quad (1)$$

Denote $C^{(t)}$ as the CA's configuration of time t which consisted of all of the $a_{i,j}^{(t)}$ ($1 \leq i \leq r, 1 \leq j \leq s$). $C^{(0)}$ is called the initial configuration. When dealing with the iteration of CA, the periodic boundary condition $a_{i,j}^{(t)} = a_{x,y}^{(t)}$ ($i \equiv x \bmod r, j \equiv y \bmod s$) is used in this paper.

In 2D-RLCAM of capacity k (2D- k -RLCAM), the state of the configuration $C^{(t+1)}$ evolves as follows:

$$C^{(t+1)} = F(C^{(t)}, C^{(t-1)}, \dots, C^{(t-k+1)}). \quad (2)$$

More concretely, the state of each cell $a_{i,j}^{(t+1)} \in C^{(t+1)}$ can be computed as (3). Note that k denotes the capability of memory here but not the threshold value of SIS. In this paper, 2D-3-RLCAM is used.

$$\begin{aligned} a_{i,j}^{(t+1)} &= [f_{w_1}(N_{i,j}^{(t)}) + f_{w_2}(N_{i,j}^{(t-1)}) + \dots + f_{w_{k-1}}(N_{i,j}^{(t-k+2)}) + f_{w_k}(N_{i,j}^{(t-k+1)})] \bmod b \\ &= [f_{w_1}(N_{i,j}^{(t)}) + f_{w_2}(N_{i,j}^{(t-1)}) + \dots + f_{w_{k-1}}(N_{i,j}^{(t-k+2)}) + a_{i,j}^{(t-k+1)}] \bmod b. \end{aligned} \quad (3)$$

In equation (3), $N_{i,j}^{(t)} \in C^{(t)}, N_{i,j}^{(t-1)} \in C^{(t-1)}, \dots, N_{i,j}^{(t-k+1)} \in C^{(t-k+1)}$ are the Moore neighborhood of the cell $a_{i,j}$ in the time $t, t-1, \dots, t-k+1$, respectively. Besides, $\{w_1, \dots, w_k\}$ is the rule number of the transfer function F and f_w is computed by (4). Therefore, the value of w can be represented as $(w)_{10} = (\lambda_{-1,-1}, \lambda_{-1,0}, \lambda_{-1,1}, \lambda_{0,-1}, \lambda_{0,0}, \lambda_{0,1}, \lambda_{1,-1}, \lambda_{1,0}, \lambda_{1,1})_2$, where $w \in [0, 2^9]$. Notice that, if $f_{w_k}(N_{i,j}^{(t-k+1)}) = a_{i,j}^{(t-k+1)}$ is satisfied, w_k should be equal to 16.

$$\begin{aligned} f_w(N_{i,j}^{(t)}) &= \sum \lambda_{\alpha,\beta} * a_{i+\alpha,j+\beta}^{(t)}, \\ &\cdot (\text{where } \alpha, \beta = \{-1, 0, 1\} \text{ and } \lambda_{\alpha,\beta} \in \{0, 1\}). \end{aligned} \quad (4)$$

A simple example for $w = 69$ of (4): we can obtain $(69)_{10} = (001000101)_2$. Therefore, only the values of $\lambda_{-1,1}, \lambda_{1,-1}, \lambda_{1,1}$ are equal to 1 and the others are equal to 0. Hence, we can compute $f_w(N_{i,j}^{(t)})$ as follows:

$$f_w(N_{i,j}^{(t)}) = \sum \lambda_{\alpha,\beta} * a_{i+\alpha,j+\beta}^{(t)} = a_{i-1,j+1}^{(t)} + a_{i+1,j-1}^{(t)} + a_{i+1,j+1}^{(t)}. \quad (5)$$

Let $\tilde{C}^{(t)}$ denote a reversion state of time t and $\tilde{a}_{i,j}^{(t)}$ denote the state of one cell in it. $\tilde{N}_{i,j}^{(t)}$ denotes the neighborhood of it. During the reversion of 2D- k -RLCAM after n iterations, the final configuration $C^{(k+n-1)}$ is taken as the initial reversion state $\tilde{C}^{(0)}$. Therefore, the configuration $C^{(k+n-1-t)}$ is taken as the reversion state $\tilde{C}^{(t)}$. The state reverses as $\tilde{C}^{(t+1)} = F'(\tilde{C}^{(t-k+1)}, \tilde{C}^{(t-k+2)}, \dots, \tilde{C}^{(t)})$ by

$$\begin{aligned} \tilde{a}_{i,j}^{(t+1)} &= [f_{w_{k-1}}(\tilde{N}_{i,j}^{(t)}) + f_{w_{k-2}}(\tilde{N}_{i,j}^{(t-1)}) + \dots + f_{w_1}(\tilde{N}_{i,j}^{(t-k+2)})] \\ &\quad + \tilde{a}_{i,j}^{(t-k+1)} \bmod b. \end{aligned} \quad (6)$$

A simple example for 2D-3-RLCAM: assume $n = 5$ and assume the set of $\{C^{(0)}, C^{(1)}, C^{(2)}\}$ is the initial configuration. Therefore, $C^{(3)}$ is the state after the first iteration, and $C^{(7)}$ is the final state after 5 iterations after computing (7). During the reversible process, $\{C^{(7)}, C^{(6)}, C^{(5)}\}$ will be taken as the

initial reversion state $\{\tilde{C}^{(0)}, \tilde{C}^{(1)}, \tilde{C}^{(2)}\}$, and $C^{(4)}$ will be recovered by $\tilde{C}^{(3)} = C^{(4)}$ as in (8):

$$C^{(7)} = f_{w_1}(C^{(6)}) + f_{w_2}(C^{(5)}) + C^{(4)}, \quad (7)$$

$$\begin{aligned} \tilde{C}^{(3)} &= -[f_{w_1}(\tilde{C}^{(1)} + f_{w_2}(\tilde{C}^{(2)})) + \tilde{C}^{(0)}] \\ &= -f_{w_1}(C^{(6)}) - f_{w_2}(C^{(5)}) + C^{(7)} = C^{(4)}. \end{aligned} \quad (8)$$

3.2. Bai and Zou's Proactive Secret Sharing Scheme. Bai and Zou's (k, n) -threshold PSS scheme [11] can periodically renew n shadows without modifying the secret. The secrets cannot be discovered from enough shares, which are mixed with past and present shares. The scheme is based on the matrix projection method, and the proactive feature is achieved through Pythagorean triples.

Matrix projection: let A be an $m \times k$ matrix of rank k ($0 \leq k \leq m$) and $P_A = A(A^T A)^{-1} A^T$ is the $m \times m$ projection matrix of it. Give k linearly independent $k \times 1$ vectors x_i and compute $\theta_i = Ax_i$. The matrix $B = [\theta_1, \theta_2, \dots, \theta_k]$ can satisfy $P_B = B(B^T B)^{-1} B^T = P_A$.

Pythagorean triples: randomly choose $\{a, b\}$ ($a, b \in Z^*$, $a > b > 0$), and compute the Pythagorean triples $\{Z_1 = a^2 - b^2, Z_2 = 2ab, Z_3 = a^2 + b^2\}$ where $Z_1^2 + Z_2^2 = Z_3^2$. Based on randomly chosen $\{g, h\}$ ($1 \leq g \neq h \leq k$), an orthonormal $k \times k$ matrix LM can be constructed by (9) where $LM^{-1} = LM^T$. $LM_{i,j}$ denotes the element of position (i, j) in LM:

$$LM_{i,j} = \begin{cases} \frac{Z_1}{Z_3} \bmod p, & \text{if } i = j = g, \\ \frac{Z_1}{Z_3} \bmod p, & \text{if } i = j = h, \\ \frac{Z_2}{Z_3} \bmod p, & \text{if } i = g, j = h, \\ -\frac{Z_2}{Z_3} \bmod p, & \text{if } i = h, j = g, \\ 0, & \text{otherwise.} \end{cases} \quad (9)$$

Now suppose the dealer wants to share a secret $m \times m$ matrix S_0 . Then, Bai and Zou's [11] proactive scheme based on matrix projection method can be constructed in the following three phases. An , Bn , and Cn denote the n -th step in each phase A, B, C.

Construction of shadows for a secret matrix S_0 (with the size of $m \times m$) at the time period $t = 0$, where $m > 2k - 3$:

- (i) A1: filling S_0 into a matrix S with the size of $L_T \times L_T$ via random values, where $L_T = m + k$. Take $S_0 = [S]_{UL: m \times m}$ to denote that $m \times m$ matrix S_0 can be extracted from the upper left corner of the matrix S .
- (ii) A2: construct a set of $L_T \times 1$ shadow vectors $\theta_{i(i=1,2,\dots,n)} = Ax_i$ based on a random $L_T \times k$ matrix A and n linearly independent $k \times 1$ vectors x_i .

- (iii) A3: compute the remainder matrix $R = (P_A - S) \bmod p$, where P_A is the $L_T \times L_T$ projection matrix of A . The remainder matrix R is also with the size of $L_T \times L_T$.
- (iv) A4: distribute shadow vectors $\theta_{i(i=1,2,\dots,n)}$ to participants and make the remainder matrix R publicly known.

Update shadows at the beginning of $t + 1$ ($t \geq 0$):

- (i) B1: generate an $k \times k$ orthonormal matrix LM by (9) as the update matrix, and distribute it via a secure channel to each participant.
- (ii) B2: each participant updates its shadow $\theta_i^{(t)}$ to $\theta_i^{(t+1)}$ by (10) and erases the variables $\theta_i^{(t)}$ and LM:

$$\theta_i^{(t+1)} = \begin{bmatrix} [\theta_i^{(t)}]_{1:m} \\ LM * [\theta_i^{(t)}]_{m+1:m+k} \end{bmatrix}, \quad (10)$$

$[\theta_i^{(t)}]_{1:m}$ denotes the top part of $\theta_i^{(t)}$ which contains the first m elements and $[\theta_i^{(t)}]_{m+1:m+k}$ is the lower part which contains the remaining k elements.

Reconstruction of the secret matrix S_0 :

- (i) C1: compute the matrix $B = [\theta_1, \theta_2, \dots, \theta_k]$ based on any k valid shadows.
- (ii) C2: the secret $S_0 = [P_B - R]_{UL: m \times m} \bmod p$.

When the current time period $t > 0$, there exists $P_A \neq P_B$ because the shadows are updated. However, equation (11) is still holding based on the matrix projection and the orthonormal update matrix LM. The detailed explanation can be seen in [11].

$$[P_A]_{UL: m \times m} = [P_B]_{UL: m \times m}. \quad (11)$$

The proposed SIS scheme in this paper is constructed based on Bai and Zou's [11] scheme. The detailed analysis of the correctness and security of sharing and updating can be seen in [11].

3.3. Matrix Encoding. Matrix encoding (ME) is a technology for steganography. Generally, for a secret S , a ME process can be defined as a 3-tuple $\{C_{\max}, n, k\}$. It denotes that no more than $C_{\max}$ bits can be changed among $n = 2^k - 1$ modifiable bits when hiding a k -bit length secret S .

Let the set of $\{a_1, a_2, \dots, a_n\}$ denote the steganography cell, where a_i is a modifiable bit. Compute $f = (a_1 * 1) \oplus (a_2 * 2) \oplus \dots \oplus (a_n * n)$ and $p = f \oplus S$. The cell $\{a_1, a_2, \dots, a_n\}$ is changed into $\{a'_1, a'_2, \dots, a'_n\}$ by (12). In the secret extraction phase, the secret S can be directly extracted by $S' = (a'_1 * 1) \oplus (a'_2 * 2) \oplus \dots \oplus (a'_n * n) = S$.

$$\begin{cases} \text{if } p = 0: a'_i = a_i, & i = 1, \dots, n, \\ \text{if } p \neq 0: a'_p = 1 - a_p, a'_i = a_i, & i = 1, \dots, n (i \neq p). \end{cases} \quad (12)$$

(1, 7, 3)-ME is used in this paper. It means that the secret value is should be satisfied $S \in [0, 7]$. For example, assume

we want to hide $S = (6)_{10} = (100)_2$ into a pixel with the value of $(105)_{10} = (1101001)_2 = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ during a (1, 7, 3)-ME process. Compute $f = 0$ and $p = 6$ first. Then, change $a'_6 = 1 - a_6 = 1$ and obtain the pixel value = $\{a'_1, a'_2, a'_3, a'_4, a'_5, a'_6, a'_7\} = (1101011)_2 = (107)_{10}$ that embeds with the secret information. Finally, we can recover the secret $S' = 6 = S$.

Therefore, the secret S is hidden in a pixel, but not appears directly in this pixel. It shows stronger security than the standard least significant bit (LSB) method. Moreover, it at most changes 1 bit to hide a 3-bit length secret in a (1, 7, 3)-ME process. However, at most 7 bits need to be changed in a standard least significant bit (LSB) method. Therefore, the ME method can achieve a slighter modification than the LSB method for the same case.

Moreover, in order to achieve a better image steganography, the changed bit a_p should be controlled among the least significant bits of a pixel. Therefore, the steganography cell is assigned into three pixels X, Y, Z by $X = \{x_1, x_2, \dots, x_6, a_1, a_2\}$, $Y = \{y_1, y_2, \dots, y_6, a_3, a_4\}$, and $Z = \{z_1, z_2, \dots, z_5, a_5, a_6, a_7\}$, and take $\{X, Y, Z\} \rightarrow S$ to denote the embedding process in this paper.

4. Proposed Scheme

The proposed (k, n) -threshold verifiable SIS scheme is constructed based on 2D-3-RLCAM and matrix projection, and the steganography is realized based on (1, 7, 3)-ME. The system model consists of three entities: a dealer D , a set of participants $P \text{ Set} = \{P_1, P_2, \dots, P_n\}$, and a set of requesters $\{Q_1, Q_2, \dots\}$ (request for reconstructing the secret image). Moreover, there is a concept of "time period t " for that the entire lifetime of the secret is divided into many short time periods determined by the system-wide clock. The proposed scheme contains four procedures: the secret distribution procedure, the shadow update procedure, the secret reconstruction procedure, and the secret update procedure.

The overall procedure of the secret distribution and the secret reconstruction is listed in Figure 1. The serial numbers (n) in Figure 1 are corresponding to the serial numbers (n) in each section.

4.1. Secret Distribution Procedure. The dealer D owns an original secret image SI for distributed storage, which is an $m \times m$ grayscale image. D also owns a set of grayscale meaningful cover images $\text{CI Set} = \{\text{CI}_1, \text{CI}_2, \dots, \text{CI}_n\}$.

D generates shadow vectors $\theta \text{ Set} = \{\theta_1, \theta_2, \dots, \theta_n\}$ and embeds them into preselected CI Set so as to generate a set of stego images $\text{GI Set} = \{\text{GI}_1, \text{GI}_2, \dots, \text{GI}_n\}$. Then, D allocates each participant P_i with a unique stego image GI_i in the public channel and makes the public information publicly known.

4.1.1. Generation of Shadows via Matrix Projection. Firstly, Bai and Zou's scheme [11] is adopted to generate n shadow vectors via matrix projection as described in Section 3.2 (the step of A2). Construct $L_T \times k$ matrix A and n linearly independent vectors $x_1, x_2, \dots, x_n$, and then compute the

shadow vectors $\theta \text{ Set} = \{\theta_1, \theta_2, \dots, \theta_n\}$. The size of each shadow vector θ_i is $L_T \times 1$, where $L_T = m + k$.

4.1.2. Generation of Stego Images via Matrix Encoding and Distribution. In this step, we generate the stego image GI_i by hiding the shadow vector θ_i into the cover image CI_i . Let $m_c \times n_c$ denote the size of the cover image CI_i . We restrict $3L_T \leq m_c n_c$ because the cover image is needed to be large enough to hide the L_T -length shadow vector θ_i via (1, 7, 3)-ME in this paper.

First of all, construct a chaotic mapping [33] based on CI_i to select the steganography cells uniformly. The primary value of the chaotic mapping can be calculated as $X_0 = \sum_{i=1}^5 p_i / 2^{(8 \times i)}$ where p_1, p_2, p_3, p_4 , and p_5 are the first five pixels of CI_i and $X_0 \in [0, 1]$. Then, compute a l_1 -length chaotic sequence $X = \{X_1, X_2, \dots, X_{l_1}\}$ based on chaotic mapping function and X_0 , where $l_1 = m_c n_c - 5$. A pseudorandom sequence X' is the ascending order of X . Every three elements in X' is the positions of a steganography cell and a (1, 7, 3)-ME for θ_i can be performed as in Section 3.3. Finally, after embedding the shadow vector θ_i into the cover image CI_i , the stego image GI_i is generated.

A simple case of embedding the vector $\theta_1 = [v_1, v_2]$ into a 4×4 cover image CI is shown in Figure 2 (assume the chaotic mapping function is $X_{i+1} = \alpha^* X_i * (1 - X_i)$ and the parameter $\alpha = 4$ here, and assume $X_1 = 0.63$ directly). The five pixels in the grey blocks are used to compute the primary value X_0 for the chaotic mapping. The generated pseudorandom sequence X' is the position for the steganography cells. To skip the first five pixels, the pixel no. should be computed as $X' + 5$. Finally, the embedding is performed as $\{p_{14}, p_8, p_{15}\} \rightarrow v_1$ and $\{p_{12}, p_6, p_{10}\} \rightarrow v_2$.

After generating the stego image sets GI Set for the shadow vectors $\theta \text{ Set}$, distribute each stego image to each participant via a public communication channel.

From the description above, we can observe the following facts of the stego images:

- (i) Slight and decentralized modification: the steganography cells are chosen uniformly and decentralized over the cover image based on the sensitive chaotic mapping. On this basis, only a trifle statistical difference of cover images will be made via the comparatively slight and decentralized modification of the pixels by using the ME steganography method.
- (ii) The constraint for the cover image: the shadow size is only $m + k$, so we can assume the cover image is smaller than the secret image ($m_c, n_c \leq m$) because there is no pixel expansion in our scheme. Therefore, the larger cover image is not necessary for this paper.
- (iii) Extract the shadow independently: the positions of the steganography pixels can be directly obtained from the stego image (by using the grey blocks in Figure 2). Consequently, the requesters can perform the reconstruction, and the participants can perform the shadow update by themselves.

FIGURE 1: Overall procedure of secret distribution and secret reconstruction.

FIGURE 2: An example of embedding in a stego image via (1,7,3)-ME.

4.1.3. Preprocessing of the Secret Image. For the secret image SI, convert it into three $m \times m$ submatrices SIM_1, SIM_2 , and SIM_3 where $SIM_1 = SI/8^2, SIM_2 = SI/8$, and $SIM_3 = SI \bmod 8$, respectively. The submatrices SIM_1, SIM_2 , and SIM_3 can satisfy that $SIM_1 * 8^2 + SIM_2 * 8^1 + SIM_3 * 8^0 = SI$.

4.1.4. Generation of Secret Matrices via RLCAM. Construct a 2D-3-RLCAM with the discrete state set $S_b (b = 8)$. Firstly, define the iteration value u and the rule number $\{w_1, w_2, w_3\}$ of it (notice that $w_3 = 16$ in RLCAM). Then, take the three submatrices SIM_1, SIM_2 , and SIM_3 as the initial configuration $C^{(0)}, C^{(1)}, C^{(2)}$, and obtain the states of $C^{(u)}, C^{(u+1)}, C^{(u+2)}$ after u times of iteration by (3). Therefore, the secret image SI is encrypted into three secret matrices $C^{(u)}, C^{(u+1)}, C^{(u+2)}$.

Moreover, make $\{w_1, w_2, w_3\}$ and u to be privately known by each requester, which can be seeded like the internal secret key of the system.

4.1.5. Generation of the Separate Verification Part. For each cover image CI_i , the independent $m \times m$ verification matrix VM is generated as in (13). $CIM_i = CI \bmod 8$ is the submatrix for CI_i . Here, we call the matrices $C^{(u)}, C^{(u+1)}, C^{(u+2)}, CIM_i, VM$ are the secret matrices.

$$VM = (C^{(u)} \oplus C^{(u+1)} \oplus C^{(u+2)} \oplus CIM_i) \bmod 8. \quad (13)$$

4.1.6. Generation of the Public Information. As in Bai and Zou's scheme [11], a publicly known remainder matrix is needed to help with the following secret reconstruction. Notice that we have to additionally verify the secret image and the cover images, so we need to generate a remainder matrix for each cover image. To simplify the notation, take R denotes the remainder matrix for an arbitrary cover image. The same number of the remainder matrices is needed to be generated as the cover images actually.

First of all, convert the secret matrices into the $L_T \times L_T$ filling matrices $\overline{C^{(u)}}, \overline{C^{(u+1)}}, \overline{C^{(u+2)}}, \overline{CIM_i}, \overline{VM}$ by filling with

random values as (14). In (14), $C^{(u)} = [\overline{C^{(u)}}]_{UL: m \times m}$ represents that $m \times m$ matrix $C^{(u)}$ can be extracted from the upper left corner of the matrix $\overline{C^{(u)}}$:

$$\begin{aligned} C^{(u)} &= [\overline{C^{(u)}}]_{UL: m \times m}, \\ C^{(u+1)} &= [\overline{C^{(u+1)}}]_{UL: m \times m}, \\ C^{(u+2)} &= [\overline{C^{(u+2)}}]_{UL: m \times m}, \\ \text{CIM}_i &= [\overline{\text{CIM}_i}]_{UL: m_c \times n_c}, \\ \text{VM} &= [\overline{\text{VM}}]_{UL: m \times m}. \end{aligned} \quad (14)$$

Then, compute a projection matrix P_A of matrix A (A is already generated in Step 1), where P_A is a $L_T \times L_T$ matrix. Calculate intermediate matrices R_0, R_1, R_2, R_3, R_4 by performing subtraction between P_A and $\overline{C^{(u)}}, \overline{C^{(u+1)}}, \overline{C}, \overline{\text{CIM}_i}, \overline{\text{VM}}$ as in the following equation:

$$\begin{aligned} R_0 &= P_A - \overline{C^{(u)}}, \\ R_1 &= P_A - \overline{C^{(u+1)}}, \\ R_2 &= P_A - \overline{C^{(u+2)}}, \\ R_3 &= P_A - \overline{\text{CIM}_i}, \\ R_4 &= P_A - \overline{\text{VM}}. \end{aligned} \quad (15)$$

Finally, the remainder matrix R is computed via $R = \sum_{i=0}^4 R_i * 8^{4-i}$, and make the remainder matrices for all cover images publicly known.

4.2. Shadow Update Procedure. Let $\{\theta_1^{(t)}, \theta_2^{(t)}, \dots, \theta_n^{(t)}\}$ denote the shadow vectors during time period t . The update process to generate $\{\theta_1^{(t+1)}, \theta_2^{(t+1)}, \dots, \theta_n^{(t+1)}\}$ is similar to Bai and Zou's scheme [11] in Section 3.2.

At the beginning of time period $t+1$, the dealer D generates a $k \times k$ orthonormal matrix LM and distributes it via a secure channel to each participant. After receiving LM , each participant P_i extracts the shadow vectors $\theta_i^{(t)}$ from its stego image and derives its new shadow vector $\theta_i^{(t+1)}$ by (10). Then, P_i embeds $\theta_i^{(t+1)}$ into its stego image again and erases all the variables except its current stego image. Because steganography is based on the computationally efficient XOR operation, the shadow updating is efficient even over the stego images.

Note that the correctness of the fact that the update shadow vectors generated during the same time period can reconstruct the secret matrix is illustrated clearly in Bai and Zou's scheme [11]. Moreover, a mixture of the shadows with different time periods cannot recover the secret, while equation (11) in Section 3.2 cannot be obtained. The explanation of this is also described in detail in Bai and Zou's scheme [11].

4.3. Secret Reconstruction Procedure. A requester Q_i can reconstruct SI as long as obtaining enough valid stego

images $\{\text{GI}_1^{(t)}, \text{GI}_2^{(t)}, \dots, \text{GI}_k^{(t)}\} \in \text{GI Set}$ during a single time period as follows.

4.3.1. Extraction of the Shadow Vectors via Matrix Encoding. The requester computes the steganography cells firstly and then extracts the embedding shadow vectors $\{\theta_1^{(t)}, \theta_2^{(t)}, \dots, \theta_k^{(t)}\} \in \theta \text{ Set}^{(t)}$ from the stego images by themselves as in Section 3.3. We omit the details here due to space limitations.

4.3.2. Reconstruction of the Secret Matrices via Matrix Projection. The requester selects a remainder matrix R from the public board which corresponds to one of the obtained stego images GI_i . The secret image SI and the corresponding cover image CI_i can be simultaneously reconstructed.

Split R back into submatrices R_0, R_1, R_2, R_3, R_4 and generate a project matrix P_B over shadow vectors $\{\theta_1^{(t)}, \theta_2^{(t)}, \dots, \theta_k^{(t)}\}$. Then, perform the subtraction as steps C1 and C2 in Section 3.2 between P_B and R_0, R_1, R_2, R_3, R_4 . Finally, extract the reconstructed secret matrices $R_{C^{(u)}}, R_{C^{(u+1)}}, R_{C^{(u+2)}}, R_{\text{CIM}_i}, R_{\text{VM}}$ from the obtained matrices as follows:

$$\begin{aligned} R_{C^{(u)}} &= [P_B - R_0]_{UL: m \times m}, \\ R_{C^{(u+1)}} &= [P_B - R_1]_{UL: m \times m}, \\ R_{C^{(u+2)}} &= [P_B - R_2]_{UL: m \times m}, \\ R_{\text{CIM}_i} &= [P_B - R_3]_{UL: m_c \times n_c}, \\ R_{\text{VM}} &= [P_B - R_4]_{UL: m \times m}. \end{aligned} \quad (16)$$

As shown in Section 3.2, the equation $[P_B]_{UL: m \times m} = [P_A]_{UL: m \times m}$ is satisfied if there do not exist fake shadows. Therefore, the equation $R_{C^{(u)}} = [P_B - R_0]_{UL: m \times m} = [P_A - R_0]_{UL: m \times m} = C^{(u)}$ will also be satisfied.

4.3.3. Verification for Cheating Detection. The separate cheating detection can be performed by the following equation:

$$R_{\text{VM}} = (R_{C^{(u)}} \oplus R_{C^{(u+1)}} \oplus R_{C^{(u+2)}} \oplus R_{\text{CIM}_i}) \bmod 8. \quad (17)$$

If (17) holds, the requester proceeds with the following steps or stops in this step. The effectiveness of the verification mechanism is proved in Theorem 3.

4.3.4. Reconstruction of the Secret Image via RLCAM. After passing the cheating detection, the requester can recover the secret image with $\{R_{C^{(u)}}, R_{C^{(u+1)}}, R_{C^{(u+2)}}\}$ via 2D-3-RLCAM. Take it as the initial state $\{\tilde{C}^{(0)}, \tilde{C}^{(1)}, \tilde{C}^{(2)}\}$ for the reversion process, and the configurations of $\{\tilde{C}^{(u)} = \text{SIM}'_1, \tilde{C}^{(u+1)} = \text{SIM}'_2, \tilde{C}^{(u+2)} = \text{SIM}'_1\}$ can be obtained by (6) after u iterations.

Finally, the reconstructed secret image $\text{SI}' = \text{SIM}'_1 * 8^2 + \text{SIM}'_2 * 8^1 + \text{SIM}'_3 * 8^0$ can be obtained.

4.3.5. Reconstruction of the Cover Image. As described previously, the last three bits of some pixels in GI_i are changed for steganography, and the secret matrix CIM_i just maintains them. Therefore, the cover image C'_i can be recovered as $C'_i = [GI_i - (GI_i \bmod 8)] + R_{CIM_i}$.

Notice that, in most of the existed traditional steganography-based SIS schemes, there have some limitations in the reconstruction of the cover images: (1) they input the same cover image for embedding all of the shadows [14, 34], which results in shares with similar content; (2) they cannot losslessly reconstruct the cover image; and (3) the cover recovery method requires more computation. Such limitations make these schemes inapplicable to some scenarios. For example, losslessly reconstructing the cover image can help to share searching with image recognition since a hash function-based searching method is generally sensitive to cover image content including even a slight distortion [29].

4.4. Secret Updating Procedure. When a new secret image is to be shared, the dealer D only needs to update the $L_T \times L_T$ public remainder matrix R for each cover image. Intuitively in the secret distribution part in Figure 1, only steps (1), (5), and (6) are needed but without the requirement for steps (3) and (4). Therefore, secret updating is very efficient because communication between the dealer and the participants is not required.

5. Security Analysis

In the proposed scheme, we consider the dealer and the requesters are fully trusted. Assume parts of the participants can be compromised by a statistical and persistent adversary.

A statistical and persistent adversary: in 5G network scenarios, the network environments are more open and flexible. Therefore, we need to consider a stronger potential adversary instead of an ordinary adversary. The ordinary adversary at most can corrupt up to $k - 1$ shadows during the entire lifetime of the secret. In this paper, we consider the adversary can stay on the networks for several time periods and move among the objects.

The adversary attempts to reconstruct or destroy the secret image illegally during several time periods. Within a time period t , the adversary at most can corrupt up to $k - 1$ participants among n participants (restrict that $n \leq 2k - 1$). If a participant is corrupted, the adversary can learn or tamper with its shadow vector during this time period. At the beginning of the next time period, all participants will be “rebooted” to the safe state, and their shadows are erased and alternated by the new ones. Because the adversary can corrupt up to $k - 1$ participants during each time period, it has more power than the ordinary adversary so that it can corrupt some participants multiple times throughout the entire lifetime of the secret image.

5.1. Collusion Attack

Theorem 1 (collusion attack). *During a time period, the adversary compromises $k - 1$ participants to obtain an*

unqualified group $\{\theta_1, \theta_2, \dots, \theta_{k-1}\}$ of shadow vectors, but the adversary still cannot explicitly learn about the secret image.

Proof 1. As proved in Bai and Zou’s scheme [11], the secret sharing using matrix projection is a strong ramp secret sharing (RSS) with k access levels, but not a perfect secret sharing (PSS) such as Shamir’s scheme. Strong RSS also does not reveal any part of the secret explicitly from any $k - 1$ shadows. However, the secret’s exposed information is proportional to the size of the unqualified group of the shadows.

As an improvement, the matrix projection is performed over the secret matrices of SI after the iterations of RLCAM. The secret matrices can seem like the encryption of SI with the RLCAM. Hence, the privacy-protecting for recovering SI is further protected under the irreversible property of RLCAM when without rule number, and the consecutive requirement of the configurations (secret matrices in this paper) with the correct order.

Therefore, the exposed information cause by the matrix projection is only relative to secret matrices. Based on the security of RLCAM, the configuration after iterations leaks nothing about the SI. Consequently, the adversary cannot get any information about the original secret image from any arbitrarily $k - 1$ shadows, much less the recovery.

Theorem 2 (persistent collusion attack). *During an adjacent time periods, the adversary compromises $k - 1$ participants during each time period, but the adversary still cannot explicitly learn about the secret image.*

Proof 2. Assume P'_1 denotes the set of k_1 participants compromised only in period $t - 1$, P'_2 denotes the set of k_2 participants compromised in both of the period $t - 1$ and t , and P'_3 denotes the set of k_3 participants compromised only in period t , where $k_1 + k_2 = k_2 + k_3 = k - 1$.

Additionally, the unqualified group of shadow vectors obtained during $t - 1$ from P'_1 and P'_2 is denoted as $\Theta_1^{(t-1)} = \{\theta_i^{(t-1)}\}_{i=1, \dots, k_1}$ and $\Theta_2^{(t-1)} = \{\theta_i^{(t-1)}\}_{i=1, \dots, k_2}$. The unqualified group of shadow vectors obtained during t from the set P'_2 and P'_3 is denoted as $\Theta_2^{(t)} = \{\theta_i^{(t)}\}_{i=1, \dots, k_2}$ and $\Theta_3^{(t)} = \{\theta_i^{(t)}\}_{i=1, \dots, k_3}$.

Based on $\Theta_2^{(t-1)}$ and $\Theta_2^{(t)}$, we can construct an equation for the unknown updating matrix LM as follows:

$$\begin{aligned} \underbrace{LM}_{k \times k} * \underbrace{\begin{bmatrix} \theta_{1[m+1: m+k]}^{(t-1)}, \dots, \theta_{k_2[m+1: m+k]}^{(t-1)} \end{bmatrix}}_{M_1: k \times k_2} \\ = \underbrace{\begin{bmatrix} \theta_{1[m+1: m+k]}^{(t)}, \dots, \theta_{k_2[m+1: m+k]}^{(t)} \end{bmatrix}}_{M_2: k \times k_2}. \end{aligned} \quad (18)$$

However, updating matrix LM cannot be determined by (18) because the matrices M_1 and M_2 are not full rank matrices (the rank of M_1 and M_2 is k_2 but not k). Since LM cannot be determined, $\Theta_1^{(t-1)}$ cannot be turned into $\Theta_1^{(t)}$ and also $\Theta_3^{(t)}$ cannot be turned into $\Theta_3^{(t-1)}$. Thereby, enough

shadows θ_i for the same time period cannot be inferred and also the matrix B which is necessary for secret reconstruction cannot be determined.

Consequently, the persistent adversary cannot obtain enough shadows even for multiple time periods, and the privacy of the secret image can be effectively guaranteed.

5.2. Shadow Tampering

Theorem 3. Assume a requester obtains a set of shadow vectors $\{\theta_1, \theta_2, \dots, \theta_k\}$. If each of the shadow vectors is valid, (17) will be explicitly holding, or holding in a negligibility probability if there exists at least one invalid shadow.

Proof 3. First of all, consider the case that all of the shadow vectors are valid. As proof in [11], there exist $[P_B]_{UL: m \times m} = [P_A]_{UL: m \times m}$, and the remainder matrix R is left to be publicly known which cannot be modified by anyone. Hence, the reconstructed secret matrices will be equal to the original secret matrices, obviously. Therefore, equation (17) can be explicitly holding.

In contrast, if there exists at least one invalid shadow vector (whether an older one or a tampered one), $[P_B]_{UL: m \times m}$ will be a meaningless matrix, which has no relevance with $[P_A]_{UL: m \times m}$. Therefore, the reconstructed secret matrices $R_{C(u)}, R_{C(u+1)}, R_{C(u+2)}, R_{CIM}, R_{VM}$ can also seem like random meaningless matrices. Therefore, we should discuss if the probability $\text{Prob}_{(VM)}$ of holding (17) is nearly zero, in this case. For each element $x_1, x_2, x_3, x_4, x_5 \in [0, 7]$ in each reconstructed secret matrices, there exists $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = x_5$ as the same form of (17). The probability of holding this equation is $1/8$. Hence, $\text{Prob}_{(VM)} = (1/8)^{m^2}$ which is effective for verification. For a 10×10 secret image, $\text{Prob}_{(VM)} = 1/2^{300}$ is small enough to be ignored. Therefore, the proposed scheme can effectively detect the tampered shadows.

6. Experimental Results and Performance Evaluation

6.1. Implementation. The scheme is implemented in Visual C# 2017 on a computer with an Intel Core i7 1.8 GHz CPU processor and 8 GB RAM that runs a Windows 10 operating system. Different sizes of cover images are considered in this paper, which includes 30×30 images chosen from the CIFAR-10 dataset [35], 96×96 images chosen from the STL-10 dataset [36], and the 256×256 standard images Baboon, Lena, and Pepper. Besides, a 256×256 standard image Boat is considered as the secret image. As described above, we do not discuss the case for the larger cover images.

6.2. Simulation Experiments. First of all, the effectiveness of the proposed scheme is shown in Table 1, where Diff denotes the different pixels between the output image and its corresponding original one. The 256×256 standard image Boat is taken as the secret image (SI). The 256×256 standard images Lena, Pepper, and Baboon are taken as the cover

images (CI01, CI02, and CI03). The experimental threshold is set as (2, 3).

The results of the generated stego images are shown as ste01, ste02, and ste03. It can be seen that there exists no significant difference between the stego image and its corresponding cover image. The indices of PSNR and SSIM of the stego images are good enough (the detailed analyses of PSNR and SSIM are shown in Section 6.3). Therefore, the stego images generated in our proposed scheme have a high quality.

The reconstruction results are also shown in Table 1 (assume we use the remainder matrix of CI01). Table 1 shows the reconstructed secret image Rec-SI for the secret image SI and the reconstructed cover image Rec-CI01 for the cover image CI01. These reconstructed images are lossless (where $\text{PSNR} = \infty$ and $\text{SSIM} = 1$).

Moreover, we also test if there is a tampered shadow for reconstruction. As shown in the image Rec-SI ($\times$), the secret image recovery will be totally failed with a tampered shadow.

6.3. Visual Quality. The general criteria to check the visual quality of the stego images are the peak-signal-to-noise ratio (PSNR) and structural similarity (SSIM). Table 2 lists the mean value of PSNR and SSIM produced by the proposed scheme for different sizes of the cover images with threshold $k = 2, 3, 7, 15$, respectively.

PSNR has explicit physical meanings, which evaluates the similarity between the original image and the output image. The value of $\text{PSNR} = +\infty$ for completely identical images. From Table 2, PSNR is larger than 55 dB for 96×96 and 256×256 cover images, which is almost indistinguishable from the human visual system (HVS).

Additionally, the details of the SSIM algorithm can be found in [37]. SSIM is used to estimate the dependencies between neighboring pixels. $\text{SSIM} = 0$ for extremely dissimilar, and $\text{SSIM} = 1$ for completely identical. From Table 2, SSIM shows 90% structural similarity between the original cover image and stego image of the proposed scheme, which is very close to the upper bound.

6.4. Embedding Ratio (ER) and Detection Ratio (DR). Embedding ratio (ER) shows the amount of information embedded in each cover pixel, which is the ratio of the number of share bits to the number of all pixels of a cover image. For resistance against steganography, ER should be less than 0.25 bpp. For 30×30 cover images, we can obtain $\text{ER} = 0.2867$ ($k = 2$) and $\text{ER} = 0.2922$ ($k = 7$). For 96×96 cover images, $\text{ER} = 0.0280$ ($k = 2$) and $\text{ER} = 0.0285$ ($k = 7$). Therefore, ER of the proposed scheme is effective enough.

Detection ratio (DR) shows the detecting ability of invalid shares, which is the ratio of detected tampered pixels to all tampered pixels. As described above, the verification of our proposed scheme is based on a separate $m \times m$ matrix, which is fully covering the stego image. Therefore, as the scheme of Eslami et al. [15], DR in this paper is approximately $256/256$, which is effective enough for cheating detection.

TABLE 1: The stego images and the reconstructed images.

Secret image		Cover image
Stego image
Rec image
			ste01	ste02	ste03
			66.40	67.03	66.71
			0.999996	0.999997	0.999996
			227/65536	223/65536	215/65536
			Rec-SI	Rec-CI01	Rec-SI (x)
			∞	∞	—
			1	1	—
			0/65536	0/65536	65420/65536

TABLE 2: PSNR and SSIM of different threshold and cover image.

	PSNR			SSIM		
	30	96	256	30	96	256
$k = 2$	47.21	57.29	66.60	0.9996	0.99997	0.999996
$k = 3$	47.39	57.29	66.35	0.9996	0.99997	0.999995
$k = 7$	47.92	57.88	65.92	0.9997	0.99997	0.999995
$k = 15$	48.10	57.97	65.63	0.9997	0.99996	0.999995

6.5. Comparative Analysis. In order to further illustrate the performance of the proposed scheme, we compared it with typical works ([10] (2006) and [15] (2010)) and some recent schemes ([16] (2018), [17] (2017), and [12] (2018)). The works described in [10, 15] are the classical schemes designed based on matrix projection method and CA, respectively. The comparative analysis is listed in Table 3.

The first five indices in Table 3 are the characteristics of these schemes:

- (1) If the shares are meaningful images
- (2) If it is a verifiable scheme
- (3) If it has the features of proactive and dynamic
- (4) The underlying techniques for SIS

- (5) The underlying techniques for steganography.
- (6) The size of the shadows
- (7) The average number of modified bits per pixel
- (8) PSNR
- (9) SSIM

Here in this part, the threshold $k = 3$. As shown in Table 3, our scheme achieves a clear advantage in the perspective of almost all indices.

Compared with the MP-based SIS schemes [10, 16], we achieve more functions. Meanwhile, we certainly not expand the shadows' size and even accomplish a smaller shadow than such schemes. The scheme of Eslami et al. [15] is the first steganography-based SIS constructed by using 1D-CA.

TABLE 3: The comparative analysis.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
[10]	×	×	×	MP and polynomial	—	$m^2/(k+m)$	—	—	—
[16]	×	√	×	MP and polynomial	—	$m^2/(k+m)$	—	—	—
[15]	√	√	×	1D-CA	LSB	m^2	1/4	47.12	0.99815
[17]	√	√	×	Polynomial	ME	$L_H/3k$	$L_H/(12 \text{ km}^2)$	49.47	—
[12]	√	√	×	2D-CA and polynomial	LSB	(Dynamic)	(Dynamic)	54.55	0.99996
Ours	√	√	√	2D-CA and MP	ME	$m+k$	$(m+k)/4 \text{ m}^2$	66.35	0.999996

It can achieve a higher computation complexity than our proposed scheme because we have the extra MP's operations. However, viewed from the indices listed in Table 3, we can achieve a better performance of the shadow size and the stego image quality than it. Moreover, this scheme realizes the secret protection based on CA's security, but only consecutive shadows can reveal the secret image that limits the practicality. As an improvement, our proposed scheme also benefits from the security provided by CA but avoids this weakness.

In the scheme of Liu et al. [17], L_H is the length of the Huffman code of the difference image of the secret image, where $L_H = m^2$ for the straightforward binary image. Hence, only when $m^2/3k - (m+k) > 0$ holding, its generated shadow will be smaller than ours. The solution of $m^2/3k - (m+k) > 0$ is restricted by $m \leq 4k$. It means that our scheme will get the stego images with higher quality when $m \leq 4k$ when both of us using (1,7,3)-ME for steganography.

The scheme of Zarepour-Ahmadabadi et al. [12] is a multiset image sharing scheme. Each secret image contains a specific threshold value, and the size of shadows is dynamically relative to it. So that the access structure in [12] is greater than ours. However, it needs to combine the hash values in each shadow, which helps to arrange the shadows according to the desired order to recover the secret image via 2D-CA correctly. These values need a relatively larger space for embedding.

Moreover, besides the scheme of Eslami et al. [15], all the other schemes may increase the computational complexity due to several times of Lagrange interpolation operations (Lagrange interpolation is the main operation of polynomial-based secret sharing). In our proposed scheme, the computation complexity is mainly based on matrix operations. Specifically, during the secret distribution procedure and the secret reconstruction procedure, we mainly have the matrix subtraction operations, the matrix XOR operations, and computing the projection matrix. Compared with the calculation of the projection matrix, the computation complexity of the matrix subtraction and the matrix XOR can be ignored because they are lightweight. The calculation of the projection matrix is the heaviest computation in our scheme. However, we only need to compute the projection matrix P_A only once during the secret distribution procedure and compute the projection matrix P_B only once during the secret reconstruction procedure. Therefore, our proposed scheme has a lower computation complexity than the other schemes.

In conclusion, compared with the above schemes, our scheme is more suitable for 5G network environments. First of all, our scheme can adapt to the rapid data changes in 5G

network environments with efficient secret distribution and secret updating. In contrast, the above schemes need to reprocess the distribution for the secret update. Secondly, for the potential adversary in the large-scale complex network environment, our scheme prevents the eavesdroppers via the higher quality steganography. Our scheme can also protect the secret against the persistent adversary through the efficient shadows update. We consider the stronger adversary than the above schemes.

7. Conclusion

In this paper, a verifiable secret image sharing scheme is proposed by employing the 2D-RLCAM and the matrix projection, which aims to provide a secure multimedia sharing and storing service in 5G network scenarios. In this paper, 2D-RLCAM and the matrix projection are combined together creatively in handling some existing weaknesses. The combination enhances the security of the secret image and the visual quality of stego image. Furthermore, a matrix encoding-based steganography approach is used to make our scheme more secure when sharing in a public network channel. The security analysis and the performance analysis demonstrate it. Therefore, the proposed scheme can simultaneously support verifiable, dynamical, and proactive features, which is superior to most existing SIS schemes. The efficient secret and shadow updating procedures make the proposed scheme more suitable for deployment in the 5G platform. We aim to optimize the size of public information for a more efficiently secret update in the future.

Data Availability

The image data used to support the findings of this study have been deposited in the Cifar-10 dataset and Stl-10 dataset repository (<http://www.cs.toronto.edu/kriz/cifar.html> and <https://cs.stanford.edu/acoates/stl10/>).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China under Grant nos. 62072090, 61872069, 61772127, 61703088, 61402097, and 61772125, the Fundamental Research Funds for the Central Universities under Grant no. N171704005, CERNET Innovation Project

under Grant no. NGII20190609, and the Shenyang Science and Technology Plan Projects (18-013-0-01).

References

- [1] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the internet of things era: an overview on security and privacy challenges," *Computer Networks*, vol. 179, p. 107345, 2020.
- [2] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G internet of things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, 2020.
- [3] Y. Liu, X. Ma, L. Shu et al., "Internet of things for noise mapping in smart cities: state of the art and future directions," *IEEE Network*, vol. 34, no. 4, pp. 112–118, 2020.
- [4] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, and C.-H. Youn, "5G-smart diabetes: toward personalized diabetes diagnosis with healthcare big data clouds," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 16–23, 2018.
- [5] L. Lyu, C. Chen, S. Zhu, and X. Guan, "5G enabled codesign of energy-efficient transmission and estimation for industrial IoT systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2690–2704, 2018.
- [6] W. Mazurczyk, P. Bisson, R. P. Jover, K. Nakao, and K. Cabaj, "Challenges and novel solutions for 5G network security, privacy and trust," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 6–7, 2020.
- [7] O. Chanu and N. Arambam, "A survey paper on secret image sharing schemes," *International Journal of Multimedia Information Retrieval*, vol. 8, pp. 195–215, 2019.
- [8] T. Chih-Ching and L. Ja-Chen, "Secret image sharing," *Computers and Graphics*, vol. 26, no. 5, pp. 765–770, 2002.
- [9] T. Chen and X. Wu, "Multiple secret image sharing with general access structure," *Multimedia Tools and Applications*, vol. 79, no. 19–20, pp. 13247–13265, 2020.
- [10] L. Bai, "A reliable (k, n) image secret sharing scheme," in *Proceedings of the 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, pp. 31–36, IEEE Computer Society, Indianapolis, IN, USA, October 2006.
- [11] L. Bai and X. Zou, "A proactive secret sharing scheme in matrix projection method," *International Journal of Security and Networks*, vol. 4, no. 4, pp. 201–209, 2009.
- [12] J. Zarepour-Ahmadabadi, M. E. Shiri-Ahmadabadi, and A. Latif, "A cellular automata-based multi-stage secret image sharing scheme," *Multimedia Tools and Applications*, vol. 77, pp. 24073–24096, 2018.
- [13] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076, 2007.
- [14] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.
- [15] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognition*, vol. 43, no. 1, pp. 397–404, 2010.
- [16] N. F. Azzahra and K. A. Sugeng, "Verifiable image secret sharing using matrix projection," *Journal of Physics Conference*, vol. 1108, pp. 1–6, 2018.
- [17] L. Liu, A. Wang, C. Chang, and Z. Li, "A secret image sharing with deep-steganography and two-stage authentication based on matrix encoding," *International Journal of Network Security*, vol. 19, no. 3, pp. 327–334, 2017.
- [18] G. Ulutas, M. Ulutas, and V. V. Nabyev, "Secret image sharing scheme with adaptive authentication strength," *Pattern Recognition Letters*, vol. 34, no. 3, pp. 283–291, 2013.
- [19] Z. Xia, L. Sun, B. Yang, Y. Zhou, and M. Zhang, "Verifiable secret sharing based on hyperplane geometry with its applications to optimal resilient proactive cryptosystems," *Information Security and Privacy*, Springer, Cham, Switzerland, pp. 83–100, 2018.
- [20] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [21] Y.-X. Liu, C.-N. Yang, C.-M. Wu, Q.-D. Sun, and W. Bi, "Threshold changeable secret image sharing scheme based on interpolation polynomial," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18653–18667, 2019.
- [22] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences*, vol. 453, pp. 21–29, 2018.
- [23] R. Alonso-Sanz, "Reversible cellular automata with memory: two-dimensional patterns from a single site seed," *Physica D: Nonlinear Phenomena*, vol. 175, no. 1–2, pp. 1–30, 2003.
- [24] H. V. McIntosh, *One Dimensional Cellular Automata*, John Wiley & Sons, Ltd., Hoboken, NJ, USA, 2009.
- [25] L. Bai, "A strong ramp secret sharing scheme using matrix projection," in *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)*, Buffalo-Niagara Falls, NY, USA, June 2006.
- [26] J. Zarepour-Ahmadabadi, M. Shiri Ahmadabadi, and A. Latif, "An adaptive secret image sharing with a new bitwise steganographic property," *Information Sciences*, vol. 369, pp. 467–480, 2016.
- [27] M. Ahmed and O. S. Younes, "Secret image sharing based on elementary cellular automata," in *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2017, AISI 2017*, pp. 832–843, Springer, Cairo, Egypt, September 2017.
- [28] L. Bai, "A reliable (K, N) image secret sharing scheme with low information overhead," *International Journal of Computers and Applications*, vol. 32, no. 1, pp. 9–14, 2010.
- [29] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3848–3858, 2020.
- [30] Z. Ni, Y. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.
- [31] Y. Liu and C.-C. Chang, "A turtle shell-based visual secret sharing scheme with reversibility and authentication," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25295–25310, 2018.
- [32] X. Yan, Q. Gong, L. Li, G. Yang, Y. Lu, and J. Liu, "Secret image sharing with separate shadow authentication ability," *Signal Processing: Image Communication*, vol. 82, p. 115721, 2020.
- [33] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU—International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, 2012.
- [34] M. Ulutas, G. Ulutas, and V. V. Nabyev, "Invertible secret image sharing for gray level and dithered cover images,"

Journal of Systems and Software, vol. 86, no. 2, pp. 485–500, 2013.

- [35] “Cifar-10 dataset,” <http://www.cs.toronto.edu/kriz/cifar.html>.
- [36] “Stl-10 dataset,” <https://cs.stanford.edu/acoates/stl10/>.
- [37] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.