IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 16, 2019, accepted May 22, 2019, date of publication May 30, 2019, date of current version June 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919294

Polynomial Based Progressive Secret Image Sharing Scheme With Smaller Shadow Size

YONGZHEN GUO[1,2], ZHUO MA[3], AND MENG ZHAO[3]
[1]School of Automation, Beijing Institute of Technology, Beijing 100081, China
[2]China Software Testing Center, Beijing 100048, China
[3]School of Cyber Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Zhuo Ma (mazhuo@mail.xidian.edu.cn)

This work was supported in part by the Application Demonstration of Security Protection Technology in Industrial Control System under Grant 2018YFB0803505, and in part by the National Natural Science Foundation of China under Grant 61872283.

ABSTRACT Progressive secret image sharing (PSIS) scheme attracts the interests of researchers in recent years. Many approaches have been proposed to construct PSIS schemes. In most of these schemes, the size of the shadow is expanded from the original image. On the contrary, polynomial-based PSIS can reduce shadow size from the original image. Recently, Yang and Huang proposed a polynomial-based (k, n) PSIS, where the image can be progressively reconstructed from k to n shadows. However, the problem of Yang–Huang's scheme is that the percentage of the recovered partial image from t shadows is extremely low when t is close to k. Later, Yang and Chu constructed another polynomial-based (k, n) PSIS with smooth property to solve this problem, but the size of the shadow is expanded greatly from Yang–Huang' scheme. In this paper, we propose a new (k, n) PSIS based on polynomial to overcome the drawbacks of these two schemes. In our scheme, t shadows (t is close to k) can recover more percentage partial image than Yang–Huang's scheme with a little shadow size expansion; comparing with Yang–Chu's scheme, our scheme achieves almost the same smooth property with much smaller shadow size.

INDEX TERMS Interpolated polynomial, progressive secret image sharing, shadow size, smooth.

I. INTRODUCTION

The Internet facilitates the exchange of information with others. However, information security has become a major issue in the communication via Internet. Many approaches can be employed to protect secret information. There are many ways to protect information from disclosure, such as using perceptual authentication [1], behavioral analysis [2], security protocol [3], [4] and combining machine learning with security [5], [6]. The research on information protection has great significance in various Internet based applications [7]–[9]. Public key cryptography has attracted the attention of many people as an important part of traditional cryptography [10]–[13]. It believes that using private keys to encrypt information to protect secret information is still one of the most effective methods. Without the appropriate key, unauthorized users cannot decrypt the information within a reasonable amount of time with the available resources. Therefore the private key is important for the encryption system, and the safely management on private key also becomes an important issue in information security. In [14], the concept of secret sharing scheme was introduced that is capable of safely keeping secret key among a group users. In a (k, n) secret sharing scheme, one secret key is divided into n shares in such a way that any k shares can recover the secret key, and less than k shares get no information on the secret key. The secret key may have various forms. For instance, an image can be a secret key, many applications adopt secret images as keys that contains crucial information in it. The requirement of protecting secret image has many applications, such as the backgrounds of medical science, geography, transportation and military, image is an important carrier that includes important information, which should be safely protected.

In [15], secret image sharing schemes were proposed that is extended from traditional secret sharing scheme and capable of protecting a secret image. In (k, n) secret image sharing (SIS) scheme, a secret image is encrypted into n shadows, such that any k or more shadows can recover the secret and less than k shadows get no information on the image.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

There are two main approaches in (k, n) SIS schemes, visual cryptography VC) schemes [16]–[18] and polynomial based SIS schemes [19]–[21]. In VC schemes, the image can be decrypted using human eyes without any mathematical computation, but the size of shadow is expanded from original image and the quality of recovered image can not be guaranteed. Polynomial based SIS schemes can reconstruct lossless image with reduced shadows. They are extended from Shamir's secret sharing scheme [14], that hide each block of k-pixels into all coefficients in a $k-1$ degree polynomial and thus the shadow size is $\frac{1}{k}$ times of the secret image. (k, n) SIS schemes satisfy a common threshold feature like (k, n) secret sharing scheme: a set of shadows can recover the entire secret image (k or more shadows) or get nothing (less than k shadows). This model of image reconstruction has its limitation, more than k shadows and exact k shadows have same effect in reconstruction, this causes a problem of redundance of shadows which have no contribution in reconstruction. In addition, the redundancy shadows would causes secure problem of safely storage and communication which increases the scheme cost. In some certain applications, a secret image would include information with different security levels in different areas, the area with higher importance level requires more shadows to recover. For instance, an image of traffic system contains the information of the car logo, the license plate and the face of driver, which have different security levels respectively. The driver face has most important level that needs highest authority to check, the license plate has lower importance level that needs medium authority and the car logo has lowest security level that needs lowest authority. In this case, the feature of traditional threshold is not fit for the applications.

A new type of (k, n) progressive secret image sharing (PSIS) scheme has an extended version of progressive threshold feature: (1) less than k shadows get nothing on secret image; k to n shadows can progressively reconstruct secret image. Due to the novel mode of recovering secret image, PSIS has attracted interests of many researchers in recent years. Lots of works have published to construct PSIS schemes. For instance, Wang [22] proposed a $(2, n)$ PSIS based on VC in which the secret image is divided into multiple regions, and more regions can be decoded by stacking more shadows, Shyu and Jiang [23] developed a novel and efficient construction for $(2, n)$ PSIS based on VC using linear programming. However, the above two $(2, n)$ PSIS schemes have the incorrect-color problem: the colors of reconstructed images may be reversed. In [24], Yang *et al.* solved the incorrect-color problem and extended the $(2, n)$ PSIS to (k, n) PSIS. These three PSIS schemes are all based on VC, the size of shadow is expanded largely from original image. There were also many PSIS schemes based on other approaches. For example, scheme [25] is based on linear congruence equation, scheme [26] is based on Gray code, scheme [27] is based on GEMD data hiding scheme and scheme [28] is based on Boolean operation. These four PSIS schemes [25]–[28] can recover lossless image with all n shadows, but the shadow size is still expanded from original image. On the contrary, polynomial based PSIS can reduce shadow size as polynomial based SIS. In 2007, Wang and Shyu [29] first introduced a polynomial based $(2, n)$ PSIS scheme, but this scheme did not fit for a general (k, n) case. In 2010, Yang and Huang [30] extended Wang-Shuy's work to a general (k, n) PSIS scheme where each shadow size is $\frac{|O|}{n}$. However, in this scheme, k to n shadows cannot progressively reconstruct the secret image in a smooth mode, which is not reasonable enough. In order to solve this problem, Yang and Huang proposed another polynomial based (k, n) PSIS scheme where the image can be gradually reconstructed from k to n shadows more smoothly, the size of shadow in this scheme is $\frac{|O|}{k}$, which is expanded from $\frac{|O|}{n}$. Later, Yang and Chu [31] introduced a new polynomial-based (k, n) PSIS with the perfect smooth reconstruction property. In [31], any t shadows ($k \leq t \leq n$) can recover proportion of $\frac{t}{n}$ on the entire image. However the drawback in [31] is that the shadow size is expanded greatly from the shadow size in [29] and [30]. Polynomial based PSIS can be also used in other secret image schemes, such as [32], where all the shadows are categorized into essential shadows and normal shadows.

In this paper, we propose a new polynomial based (k, n) PSIS scheme based on Thien-Lin's work[19]. In our scheme, the shadow size is a little larger than $\frac{|O|}{n}$ and less than $\frac{|O|}{k}$. The image can be reconstructed more smoothly from k to n shadows than the scheme [30]. Comparing with Yang-Chu's scheme [31], our scheme has almost the same smooth reconstruction property, and the shadow size is much smaller than Yang-Chu's scheme. The rest of this paper is organized as follows: In next section, we prepare some preliminaries, which includes Thien-Lin's scheme [19] and Yang-Huang's PSIS and Yang-Chu's PSIS. In section 3, we propose a new progressive secret image sharing scheme and analyze the property of progressive reconstruction. In section 4, experimental results are used to show the performance of proposed scheme and comparisons of shadow size and percentage of recovered image between several progressive secret image sharing schemes are used to show the superiority. The conclusion is included in section 5.

II. PRELIMINARIES

In this section, we prepare some preliminaries. First we introduce Thien-Lin's (k, n) SIS [19], the shadow generation algorithm in [19] is basis of all polynomial based SIS schemes. Next we describe Yang-Huang's (k, n) PSIS scheme [30] and Yang-Chu's (k, n) PSIS with smooth property [31].

A. THIEN-LIN'S (K, N) SIS SCHEME

In [19], Thien and Lin proposed a remarkable (k, n) SIS scheme based on interpolated polynomial. This scheme consists of two phases: ***Shadow generation phase*** and ***Image recover phase***. In shadow generation phase, a dealer takes a secret image O as input and invoke an algorithm

$\boldsymbol{ShadowGe}^1_{(k,n)}$ to output n shadows $S_1, S_2, \ldots, S_n$; during image recover phase, an algorithm $\boldsymbol{ImageRe}^1_t$ takes a set of m shadows $k \le t \le n$ as inputs and outputs a secret image O. The scheme is shown below.

SCHEME 1: Thien-Lin's scheme

Shadow Generation phase: On input secret image O, invoke $\boldsymbol{ShadowGe}^1_{(k,n)}(O)$

1 The dealer divides O into l-non-overlapping k pixel blocks, $B_1, B_2, \ldots, B_l$.
2 For k pixel values $a_{j,0}, a_{j,1}, \ldots, a_{j,k-1}$ in each block $B_j, j \in [1, l]$, the dealer generates a $k-1$ degree polynomial $f_j(x) = a_{j,0} + a_{j,1}x + a_{j,2}x^2 + ..., +a_{j,k-1}x^{k-1}$.
3 Using $f_j(x)$ to compute n shares $v_{j,1} = f_j(1), v_{j,2} = f_j(2), \ldots, v_{j,n} = f_j(n), j \in [1, l]$.
4 Outputs n shadows $S_i = v_{1,i} \parallel v_{2,i} \parallel, \ldots, \parallel v_{l,i}, i = 1, 2, \ldots, n$.

Image recover phase: On input m shadows $S_1, S_2, \ldots, S_t$. $(m \ge k)$, invoke $\boldsymbol{ImageRe}^1_t$

1 Compute all k coefficients in $f_j(x)$ from $v_{1,j}, v_{2,j}, \ldots, v_{t,j}, j \in [1, l]$ using lagrange formula to recover the block B_j.
2 Outputs $O = B_1 \parallel B_2 \parallel, \ldots, \parallel B_l$

It is obvious that **Scheme 1** satisfies k-threshold property that: k or more shadows can reconstruct entire image; less than k shadows get noting on secret image. The size of each shadow in **Scheme 1** is $\frac{|O|}{k}$.

B. RELATED WORKS ON (K, N) PSIS

In this part, we first give a formal definition of progressive (k, n) threshold which is different from the traditional (k, n) threshold in secret reconstruction, and then introduce two PSIS schemes that satisfy the property of progressive (k, n) threshold.

Definition 1: An image is divided into n shadows under progressive (k, n) threshold, only if these n shadows satisfy the following features:

1 Less than k shadows get nothing in the secret image.
2 Let P_t presents the proportion of recovered image to original image from t shadows, then we have $0 < P_{t_1} < P_{t_2} \le 1$ when $k \le t_1 < t_2 \le n$.

In [30], Yang and Huang proposed two PSIS schemes for the general (k, n) case. The first scheme has the optimum shadow size $\frac{|O|}{n}$, but the image cannot be reconstructed smoothly from k to n shadows; in second scheme [30], the image can be reconstructed more smoothly, and the shadow size is expanded from $\frac{|O|}{n}$ to $\frac{|O|}{k}$. We describe the second scheme in [30] in following **Scheme 2**.

SCHEME 2: *Yang-Huang's* (k, n) *PSIS*

Shadow Generation phase:

On input secret image O:

1 The dealer divides O into C_n^{k-1} non-overlapping sub-images $o_1, o_2, \ldots, o_{C_n^{k-1}}$, each sub-image has the same size $\frac{|O|}{C_n^{k-1}}$.
2 For each sub-image $o_j, j \in [1, C_n^{k-1}]$, generates k sub-shadows $s_{1,j}, s_{2,j}, \ldots, s_{k,j}$ using $\boldsymbol{ShadowGe}^1_{(k,k)}(o_i)$.
3 Let $M_{(n,k-1)} = [b_{i,j}]$ be a $n \times C_n^{k-1}$ binary matrix, where each row vector has Hamming weight $\frac{kC_n^{k-1}}{n}$ and each column vector has Hamming weight k.
4 For each $j \in [1, C_n^{k-1}]$: For $i = 1$ to n, let $x = 2$ if $b_{i,j} = 1$, $s^*_{i,j} = s_{x,j}, x = x + 1$; else $s^*_{i,j} = s_{1,j}$.
5 The shadow $S_i, i = 1, 2, \ldots, n$ is $S_i = \sum_{j=1}^{C_n^{k-1}} s^*_{i,j}$.

Image recover phase: On input $t \ge k$ shadows, without loss of generality $S_1, S_2, \ldots, S_t$.

1 Extracting r_u different sub-shadows $s_{i_1,u}, s_{i_2,u}, \ldots, s_{i_{r_u},u}$ on the sub-image $O_u, u \in [1, C_n^{k-1}]$ from $S_1, S_2, \ldots, S_t$.
2 For each $u \in [1, C_n^k]$, if $r_u \ge k$, reconstruct the sub-image o_u using $\boldsymbol{ImageRe}^1_{r_u}$; else the sub-image o_u cannot be reconstructed.
3 Output the reconstructed partial image $O' = \bigcup_{r_u \ge k} o_u$.

In **Scheme 2**, each sub-shadow $s_{i,j}$ has size of $\frac{|O|}{kC_n^{k-1}}$, and the shadow S_i is a combination of C_n^{k-1} sub-shadows. Therefore each shadow S_i has the size of $\frac{|O|}{k}$. Any t shadows $(k \le t \le n)$ can recover $P^t_{(k,n)} = \frac{C_t^{k-1}}{C_n^{k-1}}$ percentage on the entire image. Since $P^t_{(k,n)}$ satisfies that:(1) $P^{t_1}_{(k,n)} > P^{t_2}_{(k,n)}$ for $t_1 > t_2 \ge k$; (2) $P^n_{(k,n)} = 1$, the **Scheme 2** is a (k, n) PSIS scheme.

In 2011, Yang and Chu [31] introduced a (k, n) PSIS with perfect smooth reconstruction property. In this scheme [31], any t shadows can recover a partial image of percentage $P^t_{(k,n)} = \frac{t}{n}$, thus the entire image can be smoothly reconstructed from $t = k$ to $t = n$ shadows. However, the shadow size in [31] is greatly expanded from $\frac{|O|}{n}$, which is $\frac{(1+\sum_{i=k+1}^{n} \frac{1}{i})|O|}{n}$.

III. PROPOSED SCHEME

Both the two schemes in [30] satisfy the property of progressive (k, n) threshold. The first scheme achieves the optimum shadow size $(\frac{|O|}{n})$, and the second scheme (see **Scheme 2**) achieves more smoothly progressive reconstruction with shadow size $\frac{|O|}{k}$. Yang-Chu's scheme [31] achieves the perfect smooth property, however the shadow size is greatly expanded. To balance the smooth property and shadow size, we introduce a new (k, n) PSIS scheme, where the shadow size is a little larger than $\frac{|O|}{n}$ and less the shadow size in **Scheme 2** and Yang-Chu's PSIS [31]. In addition, our scheme has almost the same smooth reconstruction property as Yang-Chu's scheme which is better than **Scheme 2**. The proposed scheme is described in following **Scheme 3**.

SCHEME 3: *Proposed* (k, n) *PSIS scheme*

Shadow Generation phase:

On input secret image O:

1 The dealer divides O into C_{n+1}^{k+1} non-overlapping sub-images $o_1, o_2, \ldots, o_{C_{n+1}^{k+1}}$, each sub-image has the same size $\frac{|O|}{C_{n+1}^{k+1}}$.

2 For each sub-image $o_j, j \in [1, C_{n+1}^{k+1}]$, generates $n+1$ sub-shadows $s_{1,j}, s_{2,j}, \ldots, s_{n+1,j}$ using $\boldsymbol{ShadowGe}_{(k,n+1)}^{1}(o_j)$.

3 Let $M_{(n+1,k+1)} = [b_{i,j}]$ be a $(n+1) \times C_{n+1}^{k+1}$ binary matrix, where each row vector has Hamming weight $\frac{(k+1)C_{n+1}^{k+1}}{n+1}$, and each column vector has Hamming weight $k+1$.

4 Generate $n+1$ shadows $S_i^*, i = 1, 2, \ldots, n, n+1$ as:

$$S_i^* = \sum_{j=1}^{C_{n+1}^{k+1}} (b_{i,j} \times s_{i,j}) \tag{1}$$

5 Randomly select n shadows in the set of $U = \{S_1^*, S_2^*, \ldots, S_n^*, S_{n+1}^*\}$ as the n shadows $S_1, S_2, \ldots, S_n$.

Image recover phase: On input t shadows ($n \geq t \geq k$), without loss of generality $S_1, S_2, \ldots, S_t$.

1 Extracting r_u sub-shadows on the sub-image $o_u, u \in [1, C_{n+1}^{k+1}]$ from $S_1, S_2, \ldots, S_t$.

2 For all $u \in [1, C_{n+1}^{k+1}]$, if $r_u \geq k$, reconstruct the sub-image O_u using $\boldsymbol{ImageRe}_{r_u}^{1}$; else the sub-image o_u cannot be reconstructed.

3 Output the reconstructed partial image $O' = \bigcup_{r_u \geq k} o_u$.

The differences between our scheme and **Scheme 2** are that: (1) the entire image O is divided into C_{n+1}^{k+1} sub-images instead of C_n^{k-1} sub-images; (2) each shadow includes $\frac{(k+1)C_{n+1}^{k+1}}{n}$ sub-shadows, since the Hamming weight of each row in $M_{(n+1,k+1)}$ is $\frac{(k+1)C_{n+1}^{k+1}}{n}$. The differences can improve the smooth property from Yang-Huang's PSIS. The properties of proposed scheme is analyzed in the following theorem.

Theorem 1: The proposed scheme is a progressive (k, n) secret image sharing scheme. Each shadow has the size of $\frac{(k+1)|O|}{k(n+1)}$.

Proof: In our scheme, the entire image O is divided into non-overlapping C_{n+1}^{k+1} sub-images $o_1, o_2, \ldots, o_{C_{n+1}^{k+1}}$, each sub-image has size of $\frac{|O|}{C_{n+1}^{k+1}}$. The sub-shadows are generated using $\boldsymbol{ShadowGe}_{(k,n)}^{1}(o_i)$, each sub-shadow $s_{i,j}$ has size of $\frac{|O|}{kC_{n+1}^{k+1}}$. In step 5 of ***Shadow Generation phase***, we have $S_i = \sum_{j=1}^{C_{n+1}^{k+1}} (b_{i,j} \times s_{i,j})$, where $b_{i,j}, j = 1, 2, \ldots, C_{n+1}^{k+1}$ is a row vector in the binary matrix $M_{(k,n)}^*$. The Hamming weight of each row in $M_{(k,n)}^*$ is $\frac{(k+1)C_{n+1}^{k+1}}{n+1}$, which means that each shadow S_i is a combination of $\frac{(k+1)C_n^{k+1}}{n+1}$ sub-shadows. Therefore the size of shadow S_i is $\frac{|O|}{kC_{n+1}^{k+1}} \times \frac{(k+1)C_{n+1}^{k+1}}{n+1} = \frac{(k+1)|O|}{k(n+1)}$.

To prove the property of (k, n) progressive threshold, first we show that any $t \leq k-1$ shadows cannot get any information on the image. In our scheme, each shadow S_i includes at most one sub-shadow of the each sub-image $O_u, u \in [1, C_{n+1}^{k+1}]$, therefore $k-1$ shadows can gather at most $k-1$ sub-shadows on each sub-image o_u. Since all the sub-shadows for on each sub-image o_u are generated using $\boldsymbol{ShadowGe}_{(k,n)}^{1}(o_u)$, $k-1$ or less sub-shadows get no information on the sub-image o_u. As a result, any $k-1$ or less shadows cannot get any information on the image. When the number of shadows satisfies $t \geq k$, we analyze the probability of reconstructing each sub-image $o_u, u \in [1, C_n^{k+1}]$ from any t shadows. For a sub-image o_u, it generates $k+1$ sub-shadows, which are distributed in $k+1$ out of the $n+1$ shadows $S_1^*, S_2^*, \ldots, S_{n+1}^*$. Without loss of generality, suppose the $k+1$ sub-shadows on o_u are distributed in the $k+1$ shadows $U_1 = \{S_1^*, S_2^*, \ldots, S_{k+1}^*\}$. The cases that t shadows can recover o_u can be divided into two categories: (1) any t shadows which include k shadows in U_1 and other $t-k$ shadows in $\{S_{k+2}^*, S_{k+3}^*, \ldots, S_{n+1}^*\}$; (2) any t shadows which include all the $k+1$ shadows in U_1 and other $t-k-1$ shadows in $\{S_{k+2}^*, S_{k+3}^*, \ldots, S_{n+1}^*\}$. The total number of cases (1) and (2) is $C_{k+1}^{k} C_{n-k}^{t-k} + C_{k+1}^{k+1} C_{n-k}^{t-k-1} = (k+1)C_{n-k}^{t-k} + C_{n-k}^{t-k-1}$. In addition, the number of all combinations for choosing t out of $n+1$ shadows is C_{n+1}^{t}, the probability of recovering each sub-image from t shadows is $\frac{(k+1)C_{n-k}^{t-k} + C_{n-k}^{t-k-1}}{C_{n+1}^{t}} = \frac{(n-t+1)C_t^k + C_t^{k+1}}{C_{n+1}^{k+1}}$. Since any t shadows in U has the same probability to recover each sub-image, the percentage of reconstructed partial image from t shadows in U is $\frac{(n-t+1)C_t^k + C_t^{k+1}}{C_{n+1}^{k+1}}$. In our scheme, the n shadows $S_1, S_2, \ldots, S_n$ are selected from U, any t shadows in $\{S_1, S_2, \ldots, S_n\}$ also satisfy that $P_{(k,n)}^t = \frac{(n-t+1)C_t^k + C_t^{k+1}}{C_{n+1}^{k+1}}$. It is easy to observe that $P_{(k,n)}^t > 0$ for $t \geq k$, and $P_{(k,n)}^{t_1} > P_{(k,n)}^{t_2}$ when $t_1 > t_2$. Especially when $t = n$, $P_{(k,n)}^n = \frac{C_n^k + C_n^{k+1}}{C_{n+1}^{k+1}} = 1$. Therefore, our proposed scheme is a (k, n) PSIS scheme. End of proof.

Here we use an example to show the proposed (k, n) PSIS scheme.

Example 1: Construction of a $(k = 2, n = 4)$ PSIS scheme. A secret image O is first divided into $C_{n+1}^{k+1} = C_5^3 = 10$ sub-images $o_1, o_2, \ldots, o_{10}$, each sub-image has size of $\frac{|O|}{10}$. Generate $n = 4$ sub-shadows $s_{i,1}, s_{i,2}, \ldots, s_{i,4}$ for each sub-image o_i using $\boldsymbol{ShadowGe}_{(2,4)}^{1}(o_i)$, each sub-shadow has size of $\frac{|O|}{20}$. Suppose the matrix $M_{(2,4)}$ is that:

$$M_{2,4} = [b_{i,j}] = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \tag{2}$$

According to Eq. (1), the 5 shadows in U are:

$$\begin{cases} S_1^* = s_{1,1} \bigcup s_{2,1} \bigcup s_{3,1} \bigcup s_{4,1} \bigcup s_{5,1} \bigcup s_{6,1} \\ S_2^* = s_{1,2} \bigcup s_{2,2} \bigcup s_{3,2} \bigcup s_{7,2} \bigcup s_{8,2} \bigcup s_{9,2} \\ S_3^* = s_{1,3} \bigcup s_{4,3} \bigcup s_{5,3} \bigcup s_{7,3} \bigcup s_{8,3} \bigcup s_{10,3} \\ S_4^* = s_{2,4} \bigcup s_{4,4} \bigcup s_{6,4} \bigcup s_{7,4} \bigcup s_{9,4} \bigcup s_{10,4} \\ S_5^* = s_{3,5} \bigcup s_{5,5} \bigcup s_{6,5} \bigcup s_{8,5} \bigcup s_{9,5} \bigcup s_{10,5} \end{cases} \tag{3}$$

FIGURE 1. 10 partial images of secret image.

We randomly secret 4 shadows in $U = \{S_1^*, S_2^*, \ldots, S_5^*\}$, without loss of generality, let $S_i = S_i^*, i = 1, 2, 3, 4$. When using $t = k = 2$ shadows to recover the image, each combination of 2 shadows can recover 3 sub-images in $o_1, o_2, \ldots, o_{10}$, and the percentage of entire image is $P^2_{(2,4)} = \frac{3}{10}$. For instance, S_1, S_2 can recover o_1, o_2, o_3 and S_2, S_4 can recover o_1, o_7, o_8. Any $t = 3$ shadows can recover 7 sub-images, $P^3_{(2,4)} = \frac{7}{10}$. For instance, S_1, S_3, S_5 can recover the 7 sub-images $o_1, o_3 - o_6, o_8, o_{10}$. When all the 4 shadows participate in image reconstruction, the entire image can be recovered, the percentage is $P^4_{(2,4)} = \frac{C_3^2 + C_3^3}{C_4^3} = 1$.

IV. DISCUSSION

A. EXPERIMENT RESULTS

In this part, a $(k = 2, n = 4)$ progressive secret image sharing scheme is experimented to evaluate the performance of our approach. The image of 510×510 Jet is used as the test secret image O, since $C_{n+1}^{k+1} = 10$, the image O is first divided into 10 sub-images $o_1, o_2, \ldots, o_{10}$ with same size as shown in Fig.1.

Using $\boldsymbol{ShadowGe}^1_{(k,n+1)}(o_i)$, each sub-image is encrypted into $n + 1 = 5$ sub-shadows $s_{i,1}, s_{i,2}, \ldots, s_{i,5}$ where each sub-shadow has size of $\frac{|O|}{20}$. The binary matrix $M_{2,4} = [b_{i,j}]$ is shown as in Eq.(2). Each shadow $S_i^*, i \in [1, 5]$ includes 6 sub-shadows which is shown in Eq.(3), and the size of each shadow is $\frac{3|O|}{10}$. We select 4 shadows $S_i = S_i^*, i = 1, 2, 3, 4$ to be the shadows in our (k, n) PSIS. The percentage of recovered partial image from any t shadows is $P^t_{(2,4)} = \frac{(5-t)C_t^2 + C_t^3}{C_5^3}$. Each combination of 2 shadows can recover 3 sub-images; Each combination of 3 shadows can recover 7 sub-images. Any 4 shadows can recover the entire image. As shwon in Fig 2, S_1, S_3 can recover o_1, o_4, o_5, S_2, S_4 can recover o_2, o_7, o_9, S_1, S_4 can recover o_2, o_4, o_6; S_1, S_2, S_3 can recover $o_1 - o_5, o_7, o_8$, S_2, S_3, S_4 can recover $o_1, o_2, o_4, o_7 - o_{10}$, and S_1, S_2, S_4 can recover $o_1 - o_4, o_6, o_7, o_9$.

B. COMPARISONS

In this part, we give the comparisons of shadow size and percentage of partial image between different (k, n) PSIS schemes. In our scheme, the size of shadow is $\frac{(k+1)|O|}{k(n+1)}$. In the first scheme of Yang-Huang's work, the size of shadow is $\frac{|O|}{n}$, the second scheme in [30] (**Scheme 2**) has shadow size of $\frac{|O|}{k}$,

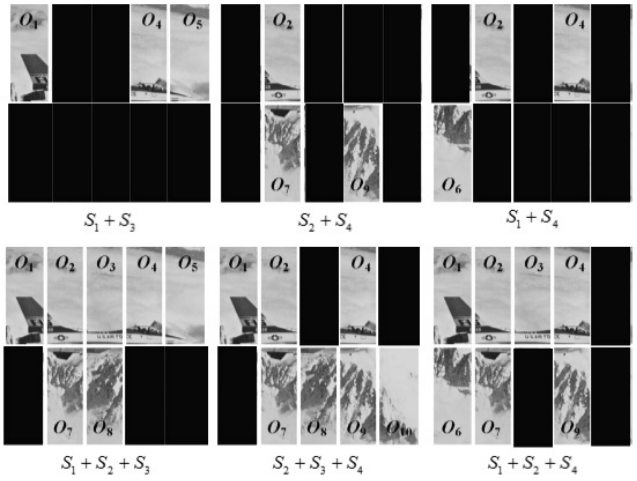

FIGURE 2. Reconstruction of partial images using 2 or 3 shadows.

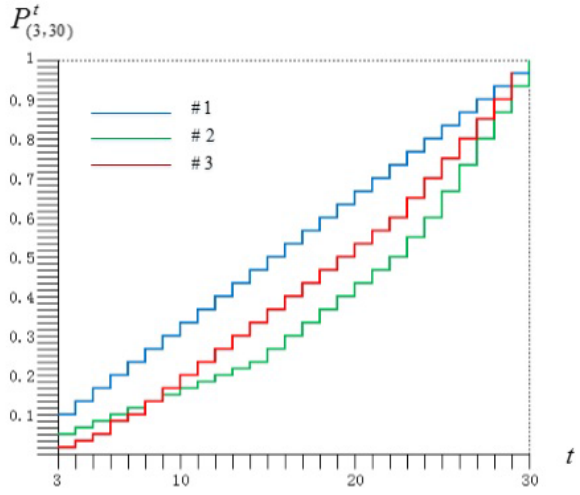

FIGURE 3. Comparison of smooth property between #1 Yang-Chu's scheme, #2 Yang-Huang's scheme, #3 proposed scheme.

Yang-Chu's scheme has the shadow size of $\frac{(1+\sum_{i=k+1}^{n}\frac{1}{i})|O|}{n}$. We use the notations $Size_{Yang\#1}$, $Size_{Yang\#2}$, $Size_{Yang-Chu}$ and $Size_{pro}$ to present the shadow sizes in first scheme in [31], **Scheme 2**, Yang-Chu's scheme [32] and our scheme respectively. The following theorem shows the comparison of shadow size between these PSIS schemes.

Theorem 2: The shadow sizes of the four (k, n) PSIS schemes satisfy that:

$$Size_{Yang\#1} < Size_{pro} < Size_{Yang-Chu} < Size_{Yang\#2}.$$

Proof: We have $Size_{Yang\#1} = \frac{|O|}{n}$, $Size_{pro} = \frac{(k+1)|O|}{k(n+1)}$, $Size_{Yang-Chu} = \frac{(1+\sum_{i=k+1}^{n}\frac{1}{i})|O|}{n}$ and $Size_{Yang\#2} = \frac{|O|}{k}$ respectively. Comparing $Size_{Yang\#1}$ with $Size_{pro}$, we have $Size_{Yang\#1} - Size_{pro} = \frac{k-n}{kn(n+1)}|O| < 0$, thus $Size_{Yang\#1} < Size_{pro}$. While $Size_{pro} - Size_{Yang-Chu} = \frac{(n-k)-k(n+1)\sum_{i=k+1}^{n}\frac{1}{i}}{kn(n+1)}|O|$. Since $\frac{k(n+1)}{i} > 1$ for each $i \in [k+1, n]$, $(n-k) - k(n+1)\sum_{i=k+1}^{n}\frac{1}{i} < 0$.

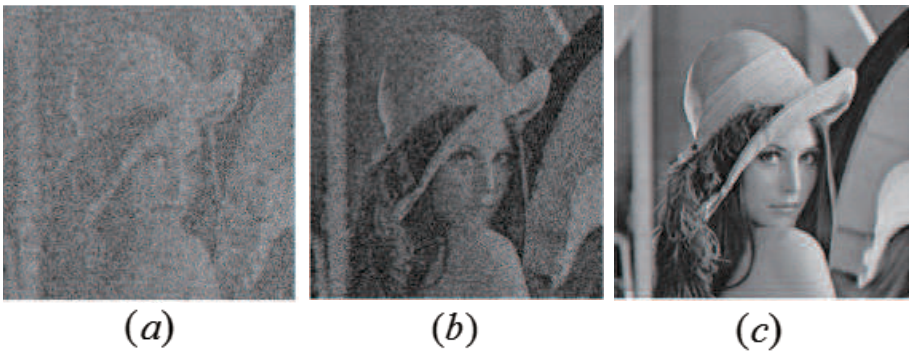

FIGURE 4. Image reconstruction in progressive model for Jet: (a) using 3 shadows (b) using 4 shadows (c) using 5 shadows.

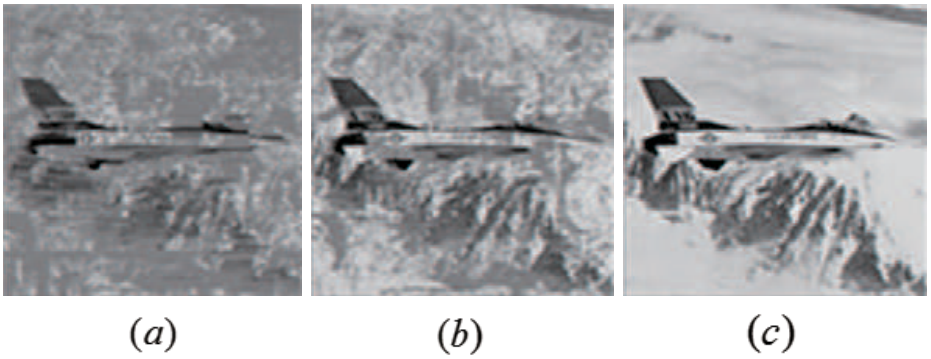

FIGURE 5. Image reconstruction in progressive model for Lena: (a) using 3 shadows (b) using 4 shadows (c) using 5 shadows.

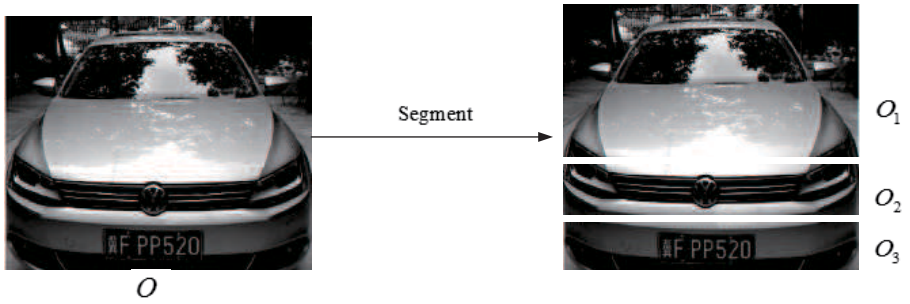

FIGURE 6. Secret image and sub-images.

Thus $Size_{pro} < Size_{Yang-Chu}$. Comparing $Size_{Yang-Chu}$ with $Size_{Yang\#2}$, we have $Size_{Yang-Chu} - Size_{Yang\#2} = \frac{\sum_{i=k+1}^{n} \frac{1}{i} - (n-k)}{kn} < 0$, therefore $Size_{Yang-Chu} < Size_{Yang\#2}$. End of proof.

The Tab.1 shows the data for comparisons of shadow size between four schemes. From the Tab.1 we can see that the shadow size in our scheme is a little larger than the shadow size in Yang-Huang's first scheme, and is much smaller than the other two PSIS schemes. For instance, when $(k, n) = (7, 13)$, the size in Yang-Chu's PSIS scheme is 150% times of our shadow size. In following Table.2, we show the different percentage $P^t_{(k,n)}$ of partial image from t shadows using three (k, n) PSIS schemes. In Fig.3, we show the different $P^t_{(k,n)}$ in a (3, 30) schemes between three schemes respectively. We can see that smooth property of our scheme is between Yang-Huang's second scheme and Yang-Chu's scheme.

TABLE 1. Comparison of shadow size between four PSIS schemes.

(k, n)	$(3, 6)$	$(4, 7)$	$(5, 9)$	$(6, 11)$	$(7, 13)$
$Size_{Yang\#1}$	$017\|O\|$	$0.14\|O\|$	$0.11\|O\|$	$0.09\|O\|$	$0.08\|O\|$
$Size_{Yang-Chu}$	$0.27\|O\|$	$0.22\|O\|$	$0.17\|O\|$	$0.15\|O\|$	$0.12\|O\|$
$Size_{Yang\#2}$	$0.33\|O\|$	$0.25\|O\|$	$0.20\|O\|$	$0.17\|O\|$	$0.14\|O\|$
$Size_{pro}$	$0.19\|O\|$	$0.15\|O\|$	$0.12\|O\|$	$0.10\|O\|$	$0.08\|O\|$

C. APPLICATIONS

Next, we show an experimental results using our scheme under a progressive reconstruction model. Progressive reconstruction model is different from the reconstruction model

TABLE 2. Comparisons between four (k, n) PSIS schemes: #1:first scheme in [24],#2second scheme in [24], #3:Yang-Chu's scheme, #4:proposed scheme.

(k,n)	t	$P^t_{(k,n)}\#1$	$P^t_{(k,n)}\#2$	$P^t_{(k,n)}\#3$	$P^t_{(k,n)}\#4$
$(3,5)$	3	$\frac{1}{10}$	$\frac{3}{10}$	$\frac{3}{5}$	$\frac{1}{5}$
	4	$\frac{4}{10}$	$\frac{6}{10}$	$\frac{4}{5}$	$\frac{3}{5}$
	5	1	1	1	1
$(4,7)$	4	$\frac{1}{35}$	$\frac{4}{35}$	$\frac{4}{7}$	$\frac{4}{56}$
	5	$\frac{5}{35}$	$\frac{10}{35}$	$\frac{5}{7}$	$\frac{16}{56}$
	6	$\frac{15}{35}$	$\frac{20}{35}$	$\frac{6}{7}$	$\frac{36}{56}$
	7	1	1	1	1
$(5,9)$	5	$\frac{1}{126}$	$\frac{5}{126}$	$\frac{5}{9}$	$\frac{5}{210}$
	6	$\frac{6}{126}$	$\frac{15}{126}$	$\frac{6}{9}$	$\frac{25}{210}$
	7	$\frac{21}{126}$	$\frac{35}{126}$	$\frac{7}{9}$	$\frac{70}{210}$
	8	$\frac{56}{126}$	$\frac{70}{126}$	$\frac{8}{9}$	$\frac{140}{210}$
	9	1	1	1	1

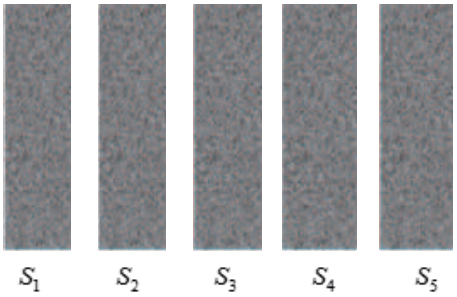

FIGURE 7. 5 shadows of secret image O.

which is shown in Fig.2. The original image is not divided into non-overlapping sub-images as shown in Fig.1. On the contrary, all secret pixels in original image are randomly divided into multi-groups of same group size, then each group of random pixels is regarded as a sub-image, and such sub-image is meaningless. When reconstructing original image, those sub-images can be recovered in scalable model. Since the pixels in sub-images are randomly selected, the original image can be reconstructed progressively with incremental shadows. The progressive reconstruction model is practical in some applications, such as the applications in medical treatment or traffic monitoring, higher authority is able to obtain more distinct image information. The following Fig.4 and Fig.5 show our $(3, 5)$ PSIS on two original images (Jet and Lena) using progressive reconstruction model, where 3 to 5 shadows can progressively reconstruct the secret images.

At last, we give an application by using our scheme. The following Fig.6 is an image O of car, which contains information with different secure levels in sub-images o_1, o_2, o_3. Using our proposed $(3, 5)$ PSIS, the image O is encrypted into 5 shadows (shown in Fig.7) with same shadow size, and any 3 shadows can recover sub-image O_1, which contains information with lowest security level; any 4 shadows can recover o_1 and o_2, where the logo can be obtained from o_2; when all 5 shadows participate in image reconstruction, the entire image can be recovered where the sub-image o_3 contains the most important information of license plate. These two applications have different reconstruction models, and each reconstruction model has important significance in applications. The progressive reconstruction model can be adopted in the application, where the meaning of image is important, but the clarity of image is less important; the sub-image reconstruction model can be used in the applications, where the image contains important information in different regions, and the clarity has great significance.

V. CONCLUSION

In this paper, we construct a new (k, n) PSIS scheme based on Thien-Lin's work, where the secret image O can be progressively reconstructed from k to n shadows. The proposed scheme achieves almost the same smooth reconstruction property as Yang-Chu's PSIS, and is better than Yang-Huang's PSIS. On the other hand, the shadow size of our scheme is much smaller than the other two PSIS schemes.

REFERENCES

[1] Z. Ma, X. Wang, R. Ma, Z. Wang, and J. Ma, "Integrating gaze tracking and head-motion prediction for mobile device authentication: A proof of concept," *Sensors*, vol. 18, no. 9, p. 2894, 2018.
[2] Z. Ma, H. R. Ge, Y. Liu, M. Zhao, and J. Ma, "A combination method for android malware detection based on control flow graphs and machine learning algorithms," *IEEE Access*, vol. 7, pp. 21235–21245, 2019.
[3] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, Dec. 2019.
[4] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *J. Ambient Intell. Humanized Comput.*, Sep. 2018. doi: 10.1007/s12652-018-1029-3.
[5] Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, "Lightweight privacy-preserving ensemble classification for face recognition," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2019.2905555.
[6] Z. Ma, Y. Liu, Z. Wang, H. Ge, and M. Zhao, "A machine learning-based scheme for the security analysis of authentication and key agreement protocols," *Neural Comput. Appl.*, Dec. 2018. doi: 10.1007/s00521-018-3929-8.
[7] Q. Sun, N. Wang, Y. Zhou, and Z. Luo, "Identification of influential online social network users based on multi-features," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 30, no. 6, 2016, Art. no. 1659015.
[8] Q. Sun, N. Wang, S. Li, and H. Zhou, "Local spatial obesity analysis and estimation using online social network sensors," *J. Biomed. Inform.*, vol. 83, no. 7, pp. 54–62, 2018.
[9] Q. Sun, Y. Qiao, J. Wang, and S. Shen, "Node importance evaluation method in wireless sensor network based on energy field model," *EURASIP J. Wireless Commun. Netw.*, vol. 1, p. 199, Aug. 2016.
[10] T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *J. Chin. Inst. Eng.*, vol. 42, no. 1, pp. 20–28, 2019. doi: 10.1080/02533839.2018.1537807.
[11] T.-Y. Wu, C.-M. Chen, K.-H. Wang, and J. M.-T. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232–49239, 2019. doi: 10.1109/ACCESS.2019.2909040.
[12] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2018.2890126.
[13] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K.-H. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," *Future Gener. Comput. Syst.*, vol. 97, pp. 453–461, Aug. 2019.
[14] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[15] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT*, vol. 950, A. De Santis, Ed. Berlin, Germany: Springer, 1995, pp. 1–12.

[16] C.-N. Yang and T.-H. Chung, "A general multi-secret visual cryptography scheme," *Opt. Commun.*, vol. 283, no. 24, pp. 4949–4962, 2010.
[17] S. J. Shyu and H.-W. Jiang, "General constructions for threshold multiple-secret visual cryptographic schemes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 733–743, May 2013.
[18] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai, and A.-Y. Tseng, "Block-based progressive visual secret sharing," *Inf. Sci.*, vol. 233, no. 1, pp. 290–304, 2013.
[19] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.
[20] R.-Z. Wang and C.-H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognit. Lett.*, vol. 27, no. 6, pp. 551–555, 2006.
[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 Appl.*, pp. 1–15, 2019.
[22] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.
[23] S. J. Shyu and H. W. Jiang, "Efficient construction for region incrementing visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 5, pp. 769–777, May 2012.
[24] C. N. Yang, H. W. Shih, C. C. Wu, and L. Harn, "k out of n region incrementing scheme in visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 5, pp. 799–810, May 2012.
[25] L. Liu, Y. Lu, X. Yan, and H. Wan, "Greyscale-images-oriented progressive secret sharing based on the linear congruence equation," *Multimedia Tools Appl.*, vol. 277, pp. 20569–20596, Aug. 2017.
[26] T.-F. Cheng, C.-C. Chang, and L. Liu, "Secret sharing: Using meaningful image shadows based on Gray code," *Multimedia Tools Appl.*, vol. 76, pp. 9337–9362, Apr. 2017.
[27] Y.-X. Liu, C.-N. Yang, Y.-S. Chou, S.-Y. Wu, and Q.-D. Sun, "Progressive (k, n) secret image sharing scheme with meaningful shadow images by GEMD and RGEMD," *J. Vis. Commun. Image Represent.*, vol. 55, pp. 766–777, Aug. 2018.
[28] Y.-X. Liu, C.-N. Yang, S.-Y. Wu, and Y.-S. Chou, "Progressive (k, n) secret image sharing schemes based on Boolean operations and covering codes," *Signal Process., Image Commun.*, vol. 66, pp. 77–86, Aug. 2018.
[29] R.-Z. Wang and S.-J. Shyu, "Scalable secret image sharing," *Signal Process., Image Commun.*, vol. 22, no. 4, pp. 363–373, 2007.
[30] C.-N. Yang and S. M. Huang, "Constructions and properties of k out of n scalable secret image sharing," *Opt. Commun.*, vol. 283, no. 9, pp. 1750–1762, 2010.
[31] C.-N. Yang and Y.-Y. Chu, "A general (k, n) scalable secret image sharing scheme with the smooth scalability," *J. Syst. Softw.*, vol. 84, no. 10, pp. 1726–1733, 2011.
[32] Y. Liu and C. Yang, "Scalable secret image sharing scheme with essential shadows," *Signal Process., Image Commun.*, vol. 58, pp. 49–55, Oct. 2017.

YONGZHEN GUO received the master's degree in control theory and control engineering from Tianjin University, Tianjin, China. He is currently pursuing the Ph.D. degree with the Beijing Institute of Technology. He is also the General Manager of the Industrial Control System Evaluation and Certification Department, China Software Testing Center.

ZHUO MA received the Ph.D. degree in computer architecture from Xidian University, Xi'an, China, in 2010, where he is currently an Associate Professor with the School of Cyber Engineering. His research interests include cryptography, machine learning in cyber security, and the Internet of Things security.

MENG ZHAO received the B.S. degree in information security from Jinan University. She is currently pursuing the master's degree with the School of Cyber Engineering, Xidian University. Her research interests include blockchain and access control.