Progressive Secret Image Sharing Scheme Based on Semantic Segmentation

LINA ZHANG1,2, XIANGQIN ZHENG1, AND YING LIU3
1College of Computer Science and Technology, Xi’an University of Science and Technology, Xi’an 710054, China
2School of Computer Science, Shaanxi Normal University, Xi’an 710119, China
3National Key Laboratory for Complex Systems Simulation, Beijing 100020, China

Corresponding authors: Lina Zhang (zhangln@xust.edu.cn) and Ying Liu (70998535@qq.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61873277, and in part by the Key Research and Development Program of Shaanxi under Grant 2018ZDXM-GY-036 and Grant 2019GY-056.

ABSTRACT Secret Image Sharing (SIS) plays an important role in the field of information security. At present, from the perspective of image restoration, SIS schemes are roughly divided into two categories: traditional threshold SIS schemes and Progressive SIS (PSIS) schemes. The former provides an all-or-nothing recovery mode in image reconstruction phase. If one of these shadows is damaged or lost, the reconstruction will fail. In contrast, the latter can present the original image progressively during the reconstruction phase. In this paper, a PSIS scheme based on semantic segmentation is proposed, where only specific objects or sensitive areas in the image are shared. After simple processing, the remaining background images can be publicly transmitted on insecure channels of the network. The background image will be regarded as a normal picture by people without shares. Owners who have reached the share of trapdoor numbers can recover a key target in an image. As the share increases, more key targets can be recovered. This paper is the first to propose secure secret sharing of images based on semantic targets. Through this method, it is possible to perform permission control on the target that needs to be divided and shared. Since the shared object is not the entire image, it can save storage space to a certain extent. Finally, through the analysis of the experimental results and comparison with other works, it can be concluded that the proposed scheme has a higher level of security and the amount of data that needs to be transmitted is small.

INDEX TERMS PSIS, semantic segmentation, interpolated polynomial.

I. INTRODUCTION

With the rapid development of digital devices and cloud computing, amounts of multimedia data are uploaded to cloud storage space via the Internet. Digital images are the most common information carrier in multimedia data, and security issues have become increasingly prominent in various applications based on communication networks such as social networking and copyright transactions [1]–[4]. Many kinds of image information, such as medical images, drawings of product design, and private photos, need to be protected. In addition, the security of various types of commercial image transactions need to be ensured during distribution and sale.

Deciding how to effectively protect the integrity of digital images is an urgent issue in the field of information security, which has become an important subject in academia and industry. In order to solve various image security problems, image encryption, image information hiding, and SIS have become research hotspots in recent years [5]–[7]. Generally, the existing mature cryptographic algorithm will be used for image encryption processing [8]. Since encrypted image looks very different from the general images, it is easy to attract the attention of attackers. Actually, their security depends on the security of the key. The distribution and storage of key bring some difficulties to the practicability of the algorithm. Image information hiding [9] is to hide the secret image in the image carrier for transmission. The security of this technique is based on the non-disclosure of the hiding algorithm, not the security of cryptography sense. For image encryption and information hiding, if the encrypted image or embedded image is damaged or lost, the original image cannot be recovered.

SIS schemes [10]–[12] can solve the problems mentioned above. In SIS, an image to be protected can be divided into multiple shares that are stored separately by different participants. The secret image can be reconstructed if the number of
shares reaches the threshold $k$. Even when parts of the shares are destroyed or lost, the remaining participants could still complete the work of image restoration. Furthermore, when the confidential images are stored in the carrier image by secret sharing, they can avoid the attention of attackers, which further enhances the security during storage and transmission.

There are mainly two types of SIS: Visual Cryptography (VC) [13], [14], and polynomial interpolation based SIS schemes [15], [16]. The human visual system is used in the first type of schemes and there are no complicated calculations used during the recovering phase. In fact, no complex cryptographic theories are used in these schemes. An obvious disadvantage is the large pixel expansion. Therefore, pixel values will be lost and the original image cannot be exactly recovered if SIS based on VC is used. The second type of schemes are mainly based on Shamir’s threshold secret sharing scheme [10], in which polynomial interpolation is used to share and accurately recover the secret. They have been widely used in various image sharing fields [17], [18].

The threshold-based secret sharing scheme was first proposed by Shamir [10]. When using $(k, n)$-threshold in cryptography, a secret is divided into $n$ shares. Then any $k(k < n)$ shares can recover the secret without loss, and less than $k$ shares get nothing on the secret. Thein and Lin [17] propose an SIS scheme, which is the first scheme to use secret sharing technology for images. In their work, they divide the pixels in the image into multiple sections; each section has $k$ pixels and each pixel can only belong to a specific section. Then let the pixels of each section be the coefficients of the Lagrange interpolation polynomial, respectively. Finally, $n$ shadow images are generated from the secret image. The scheme can reduce the size of each shadow image to $\frac{1}{k}$ of that of the secret image’s.

In recent years, more threshold-based SIS schemes have been proposed [19], [20]. All of these $(k, n)$ SIS schemes meet two features: (1) less than $k$ shadows reveal no image information, (2) any $k$ shadows can get the entire secret image. That is, this type of schemes provides an all-or-nothing recovery mode. However, such schemes have certain limitations. For example, there are $n-k$ shadows that will cause redundancy and will result in a waste of storage space. Besides, the greater the number of shadows, the greater the number of participants, which will increase the cost. In practice, for some images, such as medical and military images, we only care about specific objects in the image rather than the entire image. These objects must be restored according to the rights of share owners. In this case, the above SIS schemes are not applicable.

In order to meet the corresponding application requirements and improve the flexibility of the scheme, PSIS schemes have also been widely studied [21]–[25]. Compared with the traditional SIS schemes, $(k, n)$ PSIS schemes can gradually recover the secret image and meet three features: (1) Less than $k$ shadows reveal no image information. (2) Any $k$ shadows can restore part of the image. (3) After reaching $k$ shadows, each additional shadow can restore a new part of the content. Only when $n$ shadows participate in the restoration of the image, can the secret image be completely restored.

The study in [26] proposes a random-grid-based progressive visual secret sharing scheme and the priority weighting of each share can be adjusted. However, the scheme has pixel expansion, which makes the recovered image visually different from the original secret image. The approach in [27] develops a scalable SIS scheme. In their work, there are three modes for sharing secret image, and two image division methods are used: one is based on the spatial domain to divide the image into multiple non-overlapping sub-images, and the other is based on the pixel domain. The work in [28] dwells on polynomial based PSIS with a smaller shadow size that is a little larger than $\frac{[\ln n]}{n}$ and less than $\frac{[\ln n]}{k}$. The secret image can be reconstructed more smoothly from $k$ to $n$ shadows and the scheme is also based on the spatial domain when dividing secret images. The study in [29] develops two $(k, n)$ scalable SIS schemes to satisfy the dynamical security requirement, and the scheme is also based on the spatial domain to divide the image. All PSIS schemes can gradually recover the secret image.

At present, all of these schemes are based either on the spatial domain or pixel domain to divide the secret image. The shared object is the entire image, and the sub-images are not assigned priority based on their importance. For some applications, such as some images in the military, only the sensitive areas related to privacy or national interests in the image, or specific objects, are the objects that we need to protect. They are also the objects we need to share. As for the rest of the image, after certain processing, it can be transmitted publicly on the internet. Therefore, these PSIS schemes are not applicable.

In this paper, we mainly focus on the rights allocation and privacy protection of digital images when sharing. Based on instance aware semantic segmentation in computer vision problems, independent objects in images are used as research objects, and a new $(k, n)$ PSIS scheme based on semantic segmentation is proposed. This scheme has a strong purpose in protecting and restoring the original image. By segmenting the image based on semantics, the separated target objects are used as sub-images. Each sub-image is assigned priority according to its importance. The advantage of this scheme is that it can save storage space and other resources to some extent. In addition, relevant persons can gradually restore specific target objects according to their needs in specific application scenarios. Actually, it also improves some of the deficiencies in the existing PSIS schemes and improves the flexibility. Therefore, it has strong practicality.

The rest of this paper is organized as follows: In next section, we prepare some preliminaries, which include Thien-Lin secret sharing scheme [17], Guo-Ma PSIS scheme [28] and image semantic segmentation [30]. In Section 3, we propose a new $(k, n)$ PSIS scheme based on semantic segmentation. In Section 4, experimental results and analyses are used to show the performance and superiority of the proposed scheme. Comparisons with related
works are given in Section 5. The conclusion is included in Section 6.

II. PRELIMINARIES

Two representative SIS schemes, namely Thien-Lin (k, n) SIS scheme [17] and Guo-Ma PSIS scheme [28], and image semantic segmentation are introduced in this section. In reality, a lot of malleable schemes have been built. We will briefly describe Guo-Ma PSIS scheme and discuss the proposed scheme in detail.

A. THIEN-LIN’S (K, N) SIS SCHEME

In [17], Thien and Lin propose an SIS scheme, in which Lagrange-based interpolation polynomial is constructed, and the pixels of secret image are the coefficients of the polynomial. The scheme is divided into two phases: sharing phase and reveal phase. The details are shown as below.

Sharing phase:
1) Image O with size M × N is divided into several sections
   \[ \alpha_i = (p_{1i}, p_{2i}, \ldots, p_{ni}) \], where \( i = 1, 2, 3, \ldots, \frac{M \times N}{r} \) and \( M \times N \) is the total sections of the original secret image, and \( p_{ji} (j = 1, 2, 3, \ldots, r) \) is the element of section \( \alpha_i \).
2) Construct \( (r - 1) \)-degree polynomials. Let \( r \) pixels in each section \( \alpha_i \) be the \( r \) coefficients of the polynomial, respectively:
   \[ f_i(x) = p_{1i} + p_{2i}x + p_{3i}x^2 + p_{4i}x^3 + \cdots + p_{ri}x^{r-1} \] (1)
3) Then for each \( \alpha_i, f_i(1), f_i(2), \ldots, f_i(n) \) can be obtained.
4) Generate \( n \) shadow images \( P_1, P_2, \ldots, P_n \), where
   \[ P_i = \bigcup_j f_j(i), i \in [1, n], j \in [1, \frac{M \times N}{r}] \].

Recovering phase:
First, randomly select \( r \) shadow images and perform the following two steps.
1) Take the first element of each shadow image, and then construct a Lagrange interpolation polynomial to solve for the \( r \) coefficients, the corresponding \( r \) values of section \( \alpha_1 \).
2) Repeat the first step until all pixels of \( r \) shadow images are processed.
When the values of each section \( \alpha_i \) are obtained, the secret image can be recovered.

B. GUO-MA (K, N) PSIS SCHEME

The study in [28] proposes a new (k, n) PSIS scheme based on polynomial, which can reduce the shadow size. The scheme is divided into two phases: shadow generation phase and image restoration phase. The details are described in the following.

Shadow generation phase:
1) Generate sub-images. Divide the secret image \( I \) into \( C_{n+1}^{k+1} \) non-overlapping sub-images \( I_1, I_2, \ldots, I_{C_{n+1}^{k+1}} \), with the same size \( \frac{|I|}{C_{n+1}^{k+1}} \).
2) Generate sub-shadows. For each sub-image \( I_i, i \in \{1, C_{n+1}^{k+1}\} \), use Thien-Lin’s scheme to generate \( n + 1 \) sub-shadows \( B_1^i, B_2^i, \ldots, B_{n+1}^i \).
3) Generate a binary matrix. Let \( M_{n+1,k+1} = [a_{ij}] \) be a \((n + 1) \times C_{n+1}^{k+1}\) binary matrix, in which each row vector and column vector have been given Hamming weight \( \frac{(k + 1)C_{n+1}^{k+1}}{n + 1} \) and \( k + 1 \), respectively.
4) Generate \( n + 1 \) shadows \( P_i, i = 1, 2, \ldots, n + 1 \).
   \[ P_j = \sum_{i=1}^{C_{n+1}^{k+1}} (a_{ji} \times B_j^i) \] (2)

Then select \( n \) shadows from \( P_1, P_2, \ldots, P_{n+1} \) as the final \( n \) shadows \( P_1, P_2, \ldots, P_n \).
Image recover phase:
Suppose that \( i(k \leq t \leq n) \) shadows \( P_1, P_2, \ldots, P_t \) are available. The recovery process is as follows.
1) Reconstruct \( s_m (m \in \{1, C_{n+1}^{k+1}\}) \) sub-shadows from \( P_1, P_2, \ldots, P_t \).
2) For all \( m \), if \( s_m \geq k \), reconstruct sub-image \( I_m \) using Thien-Lin’s scheme.
If each sub-image \( I_i \) is recovered, then the original image \( I \) can be constructed.

C. SEMANTIC-BASED IMAGE SEGMENTATION

Semantic segmentation [30] is a very important field in computer vision. It refers to identifying images at the pixel level, that is, marking the object category to which each pixel in the image belongs. The following figure is an example of semantic segmentation, whose goal is to predict the class label of each pixel in the image, see Fig. 1.

![Figure 1. Planes. (a) is the original plane; (b) is the plane obtained by semantic segmentation.](image-url)
The focus of the research is not the semantic segmentation method, but the adoption of this idea to generate sub-images, which are the secret shared objects.

In short, we hoped that more scholars can use machine learning and deep learning to do semantic segmentation. Then, the separated objects are used as the objects of secret sharing. We also hope that increasing researchers will deeply integrate image semantic segmentation with SIS technology to enrich SIS schemes.

III. THE PROPOSED SCHEME

A. MOTIVATION

At present, since images are widely used in many fields, it has become very important to ensure that images can be safely stored and transmitted on the Internet. In addition, the traditional encryption technology and image information hiding technology cannot fully ensure the secure storage and transmission of images. In comparison, SIS is more conducive to the secure storage and transmission of images.

As the research progresses, a large number of SIS schemes have been proposed. In general, these schemes are divided into two categories: PSIS and non-progressive SIS. A common feature of these two types of schemes is that the original image is divided into multiple non-overlapping sub-images based on spatial or pixel domain of the image, and then the secret sharing technology is used to generate multiple shares and distribute them to multiple participants. One obvious disadvantage of these schemes is that the corresponding sub-images are restored randomly according to the obtained shadow images, and the recovered content has a lot of randomness. Besides, the recovered part is less readable.

Generally, in most cases, we care about only one or some target objects in an image, and the rest target objects and background are not important. For example, in telemedicine diagnostic system, for some medical images, only the location of the lesion, or the sensitive area needs to be protected. The remaining parts that do not involve patients privacy can be publicly transmitted. Besides, some pedestrian detection and target tracking focus only on specific targets; therefore, such objects are protected objects.

In this paper, a new \((k, n)\) PSIS scheme based on semantic segmentation is proposed. Since the specific objects or sensitive areas in an image are protected, this scheme has a strong purpose in protecting and restoring the original image. Therefore, it can save storage space and other resources to some extent.

B. THE PROPOSED \((k, n)\) PSIS SCHEME

The proposed scheme includes two phases: a sharing phase and a reconstruction phase. In the sharing phase, shadow generation is similar to Liu-Yang’s scheme [29], and the reconstruction of original image is the same as in Thien-Lin’s scheme [17]. The steps are shown as below.

Sharing phase:

1) First, convert the original secret image to grayscale. Then, we identify sensitive areas of the original image. Several original target sub-images are separated based on semantics from the original secret image \(O\) with size \(m \times n\), marked as \(P_1, P_2, P_3, \ldots, P_t\), where \(t\) is the number of the objects that need to be protected in \(O\). At the same time, we record the position information of each sub-image (such as the coordinate information). After that, fill the rest and represent it by \(B\). In this way, it will not be suspected when transmitting online.

2) Determine the number of pixels in \(x\)-axis and \(y\)-axis directions of all target sub-images, represented by \(M_1, M_2, \ldots, M_t\) and \(N_1, N_2, \ldots, N_t\), respectively. \(M \times N = \text{Min}(M_1 \times N_t), i \in [1, t]\), which represents the size of all of the new sub-images.

3) Resize the original target sub-image \(P_i, i \in [1, t]\) into a rectangle with size \(M \times N\). Then, we obtain a new sub-image \(PN^*_i, i \in [1, t]\). Finally, set priority for all new sub-images and number all new sub-images according to priority. Thus, we can get \(PN^*_i, i \in \{1, t\}\). The value of \(i^*\) is inversely proportional to the priority of its corresponding sub-image, i.e., the smaller the value of \(i^*\), the higher the priority of the corresponding sub-image.

4) For \(PN^*_i, i \in \{1, t\}\), use \((k + i - 1, n)\) threshold scheme to generate \(n\) shares \(s_{i,1}, s_{i,2}, \ldots, s_{i,n}\).

5) Generate \(n\) shadows \(S_j, j = 1, 2, 3, \ldots, n, S_j = \bigcup s_{q,j}, j \in [1, n], q \in [1, m]\), and then distribute them to \(n\) different participants.

Reconstruction of the secret image:

1) First, take \(l\) shadows \(S_1, S_2, \ldots, S_l\), when \(l \geq k\), and then we can restore the original image. If \(l = k\), we can recover \(PN^*_1\) with the highest priority by constructing Lagrange interpolation polynomial. If we add another shadow, then \(PN^*_2\) can be recovered. When all shadows are available, all sub-images can be reconstructed.

2) Use image processing technology to obtain \(P_i, i \in \{1, t\}\), and then reconstruct the original image based on the original position information of \(P_i\) in the image. Finally, \(O = P_l \cup B\). The secret image is reconstructed completely.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. EXPERIMENTAL RESULTS

In this section, we will give two examples to verify the performance of the proposed scheme. Next, we will analyze the first example in detail.
Example 1: The original secret image \( O \), processed background \( B \) and two target sub-images segmented from \( O \) are shown in Fig. 3. First, semantic segmentation is used to obtain the original target sub-images \( P_1, P_2 \). Then, resize \( P_1, P_2 \) to obtain the two new sub-images represented by \( PN_1, PN_2 \), which are shown in (c) and (d) in Fig. 3. Suppose that these two are sensitive areas, the objects that need to be protected in an application scenario. Here, we assume that \( PN_1 \) has a higher priority than \( PN_2 \). Let \( PN_1 = PN'_1, PN_2 = PN'_2 \). Then, fill the remaining part of the original secret image to obtain the background image \( B \). In the proposed scheme, let \( k = 5, n = 8 \). Next, \( n \) shadows need to be generated, see Fig. 4, and the specific steps are as follows.

\[
\begin{align*}
\text{(a) } & \text{Secret image } O \\
\text{(b) } & \text{Processed background } B \\
\text{(c) } & \text{Target sub-image } PN_1 \\
\text{(d) } & \text{Target sub-image } PN_2
\end{align*}
\]

\textbf{FIGURE 3.} Original secret image and sub-images after segmentation. (a) Secret image \( O \); (b) Processed background \( B \); (c) and (d) are two target sub-images segmented from (a).

\[
\begin{align*}
\text{(a) } & \text{Secret image } O \\
\text{(b) } & \text{Processed background } B \\
\text{(c) } & \text{Target sub-image } PN_1 \\
\text{(d) } & \text{Target sub-image } PN_2
\end{align*}
\]

\textbf{FIGURE 4.} Shadow images. (a) – (h) are 8 shadows that will be distributed to different participants.

Generation of shadows:
First, for \( PN'_1 \), we need to construct a \( k - 1 \) degree polynomial:
\[
f_{i}^{j}(x) = b_{i,0} + b_{i,1}x + b_{i,2}x^2 + b_{i,3}x^3 + \cdots + b_{i,k-1}x^{k-1}
\]
(3)
where \( j \) represents the sub-image subscript, and \( j = 1, 2 \); \( i \) represents the specific block in the sub-image; \((i,0), (i,1), \cdots, (i, k-1)\) represent the elements of a specific block in a sub-image. The generation of polynomial is the same as in Thien-Lin’s scheme. Here, for \( PN'_1 \), we find five polynomials:
\[
\begin{align*}
f_{1}^{1}(x) &= 67 + 69x + 71x^2 + 69x^3 + 65x^4 \\
& f_{2}^{1}(x) = 66 + 65x + 63x^2 + 66x^3 + 67x^4 \\
& f_{3}^{1}(x) = 67 + 66x + 64x^2 + 65x^3 + 64x^4 \\
& f_{4}^{1}(x) = 65 + 65x + 66x^2 + 64x^3 + 64x^4 \\
& f_{5}^{1}(x) = 67 + 68x + 65x^2 + 67x^3 + 61x^4
\end{align*}
\]
then we can obtain multiple shares:
\[
\begin{align*}
s_{1,1}^{1} &= f_{1}^{1}(9), s_{1,2}^{1} = f_{1}^{1}(10), \ldots, s_{1,8}^{1} = f_{1}^{1}(16) \\
s_{1,1}^{2} &= f_{2}^{1}(9), s_{1,2}^{2} = f_{2}^{1}(10), \ldots, s_{1,8}^{2} = f_{2}^{1}(16) \\
s_{1,1}^{3} &= f_{3}^{1}(9), s_{1,2}^{3} = f_{3}^{1}(10), \ldots, s_{1,8}^{3} = f_{3}^{1}(16) \\
s_{1,1}^{4} &= f_{4}^{1}(9), s_{1,2}^{4} = f_{4}^{1}(10), \ldots, s_{1,8}^{4} = f_{4}^{1}(16) \\
s_{1,1}^{5} &= f_{5}^{1}(9), s_{1,2}^{5} = f_{5}^{1}(10), \ldots, s_{1,8}^{5} = f_{5}^{1}(16)
\end{align*}
\]
Next, for \( PN'_2 \), a similar approach is used to generate multiple shares. The only difference is \( k = 6 \). We construct five polynomials in the same way:
\[
\begin{align*}
f_{1}^{2}(x) &= 90 + 92x + 93x^2 + 91x^3 + 89x^4 + 88x^5 \\
f_{2}^{2}(x) &= 86 + 85x + 84x^2 + 86x^3 + 86x^4 + 86x^5 \\
f_{3}^{2}(x) &= 88 + 91x + 93x^2 + 94x^3 + 91x^4 + 90x^5 \\
f_{4}^{2}(x) &= 92 + 92x + 94x^2 + 97x^3 + 98x^4 + 96x^5 \\
f_{5}^{2}(x) &= 97 + 98x + 95x^2 + 93x^3 + 89x^4 + 88x^5
\end{align*}
\]
then, we can obtain multiple shares:
\[
\begin{align*}
s_{1,1}^{1} &= f_{1}^{2}(9), s_{1,2}^{1} = f_{1}^{2}(10), \ldots, s_{1,8}^{1} = f_{2}^{2}(16) \\
s_{1,1}^{2} &= f_{2}^{2}(9), s_{1,2}^{2} = f_{2}^{2}(10), \ldots, s_{1,8}^{2} = f_{2}^{2}(16) \\
s_{1,1}^{3} &= f_{3}^{2}(9), s_{1,2}^{3} = f_{3}^{2}(10), \ldots, s_{1,8}^{3} = f_{3}^{2}(16) \\
s_{1,1}^{4} &= f_{4}^{2}(9), s_{1,2}^{4} = f_{4}^{2}(10), \ldots, s_{1,8}^{4} = f_{4}^{2}(16) \\
s_{1,1}^{5} &= f_{5}^{2}(9), s_{1,2}^{5} = f_{5}^{2}(10), \ldots, s_{1,8}^{5} = f_{5}^{2}(16)
\end{align*}
\]
Note that in order to make the obtained 8 shadow images more distinguishable, \( x = 9, 10, \ldots, 16 \), respectively. Finally, we can generate eight shadows, see Fig. 4.
\[
\begin{align*}
S_1 &= s_{1,1}^{1} \cup s_{1,1}^{2} \cup s_{1,1}^{3} \cup s_{1,1}^{4} \cup s_{1,1}^{5} \cup s_{2,1}^{1} \cup s_{2,1}^{2} \cup s_{2,1}^{3} \\
S_2 &= s_{1,2}^{1} \cup s_{1,2}^{2} \cup s_{1,2}^{3} \cup s_{1,2}^{4} \cup s_{1,2}^{5} \cup s_{2,2}^{1} \cup s_{2,2}^{2} \cup s_{2,2}^{3} \\
S_3 &= s_{1,3}^{1} \cup s_{1,3}^{2} \cup s_{1,3}^{3} \cup s_{1,3}^{4} \cup s_{1,3}^{5} \cup s_{2,3}^{1} \cup s_{2,3}^{2} \cup s_{2,3}^{3} \\
S_4 &= s_{1,4}^{1} \cup s_{1,4}^{2} \cup s_{1,4}^{3} \cup s_{1,4}^{4} \cup s_{1,4}^{5} \cup s_{2,4}^{1} \cup s_{2,4}^{2} \cup s_{2,4}^{3} \\
S_5 &= s_{1,5}^{1} \cup s_{1,5}^{2} \cup s_{1,5}^{3} \cup s_{1,5}^{4} \cup s_{1,5}^{5} \cup s_{2,5}^{1} \cup s_{2,5}^{2} \cup s_{2,5}^{3} \cup s_{2,5}^{4} \cup s_{2,5}^{5}
\end{align*}
\]
Thien-Lin’s scheme.

The secret image.

The original position in the secret image. Finally, the original sub-images

PN fails. In addition, since the number of shadows reaches the threshold, can the restoration of

PN distributed to different participants.

All shadows are shown in Fig. 4. Then, these shadows will be

distributed to different participants.

Reconstruction of the secret image:

In the image reconstruction phase, only when the number of shadows reaches the threshold, can the restoration of the original image be performed. Otherwise, the restoration fails. In addition, since $PN_1'$ has a higher priority than $PN_2'$, when we obtain five shadows, we can recover the sub-image $PN_1'$ by constructing Lagrange interpolation polynomial, see Fig. 5(a). $PN_2'$ can only be restored when there are six or more shadows. Finally, $PN_1'$ and $PN_2'$ are processed to obtain the original sub-images $P_1$ and $P_2$. Then, $P_1$ and $P_2$ are placed in the original position in the secret image. Finally, the original secret image $O'$ can be reconstructed losslessly, as shown in Fig. 5(b). Actually, the recovery of sub-images is similar to Thien-Lin’s scheme.

$S_6 = s_{1,6} \cup s_{2,6} \cup s_{1,6} \cup s_{2,6} \cup s_{1,6} \cup s_{2,6} \cup s_{1,6} \cup s_{2,6} \cup s_{1,6} \cup s_{2,6}$

$S_7 = s_{1,7} \cup s_{2,7} \cup s_{1,7} \cup s_{2,7} \cup s_{1,7} \cup s_{2,7} \cup s_{1,7} \cup s_{2,7}$

$S_8 = s_{1,8} \cup s_{2,8} \cup s_{1,8} \cup s_{2,8} \cup s_{1,8} \cup s_{2,8}$

FIGURE 5. Shadow images. (a) is image restored with 5 shadows; (b) is image restored with 6 shadows.

Example 2: Similar to the first example, the secret image needs to be segmented to generate sub-images. Then, shadow images are generated by the sub-images. Finally, the secret image is restored.

The image $I$, processed background $B$ and two target sub-images segmented from $I$ are shown in Fig. 6. First, semantic segmentation is used to obtain the original target sub-images $P_1$, $P_2$. Then, resize $P_1$, $P_2$ to obtain the two new sub-images represented by $PN_1$, $PN_2$, which are shown in (c) and (d) in Fig. 6. Suppose that these two are sensitive areas, the objects that need to be protected. Here, we assume that $PN_1$ has a higher priority than $PN_2$. Let $PN_1 = PN_1'$, $PN_2 = PN_2'$. Then, fill the remaining part of the original secret image to obtain the background image $B$. Here, let $k = 3, n = 5$. Next, $n$ shadows need to be generated, see Fig. 7, and the specific steps are as follows.

Generation of shadows:

First, for $PN_1'$, we need to construct a $k - 1$ polynomial:

$$f_i^j(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + a_{i,3}x^3 + \cdots + a_{i,k-1}x^{k-1}$$

(4)

where $j$ represents the sub-image subscript, and $j = 1, 2, \ldots$; $i$ represents the specific block in the sub-image; $(i, 0), (i, 1), \ldots, (i, k - 1)$ represent the elements of specific block in a sub-image. The generation of polynomial is the same as in Thien-Lin’s scheme. Here, for $PN_1'$, we find five polynomials:

$$f_1^1(x) = 37 + 38x + 38x^2$$

$$f_1^2(x) = 38 + 38x + 39x^2$$

$$f_1^3(x) = 39 + 39x + 40x^2$$

$$f_1^4(x) = 39 + 37x + 37x^2$$

$$f_1^5(x) = 36 + 37x + 37x^2$$

then we can obtain multiple shares:

$$s_{1,1} = f_1^1(1), s_{1,2} = f_1^1(2), \ldots, s_{1,5} = f_1^1(5)$$

$$s_{2,1} = f_2^1(1), s_{2,2} = f_2^1(2), \ldots, s_{2,5} = f_2^1(5)$$

$$s_{3,1} = f_3^1(1), s_{3,2} = f_3^1(2), \ldots, s_{3,5} = f_3^1(5)$$

$$s_{4,1} = f_4^1(1), s_{4,2} = f_4^1(2), \ldots, s_{4,5} = f_4^1(5)$$

$$s_{5,1} = f_5^1(1), s_{5,2} = f_5^1(2), \ldots, s_{5,5} = f_5^1(5)$$

Next, for $PN_2'$, a similar approach is used to generate multiple shares. The only difference is $k = 4$. We construct five polynomials in the same way:

$$f_2^1(x) = 13 + 14x + 13x^2 + 12x^3$$

$$f_2^2(x) = 13 + 14x + 13x^2 + 21x^3$$

$$f_2^3(x) = 17 + 16x + 17x^2 + 17x^3$$

$$f_2^4(x) = 15 + 13x + 15x^2 + 15x^3$$

$$f_2^5(x) = 15 + 18x + 15x^2 + 17x^3$$

FIGURE 6. Original secret image and sub-images after segmentation. (a) Secret image $I$; (b) Processed background $B$; (c) and (d) are two target sub-images segmented from (a).

FIGURE 7. Shadow images. (a) – (e) are 5 shadows that will be distributed to different participants.
then, we can obtain multiple shares:

\[ s_{2,1}^1 = f_2^1(1), s_{2,1}^2 = f_2^1(2), \cdots, s_{2,5}^1 = f_2^1(5) \]
\[ s_{2,1}^2 = f_2^2(1), s_{2,2}^2 = f_2^2(2), \cdots, s_{2,5}^2 = f_2^2(5) \]
\[ s_{2,1}^3 = f_2^3(1), s_{2,2}^3 = f_2^3(2), \cdots, s_{2,5}^3 = f_2^3(5) \]
\[ s_{2,1}^4 = f_2^4(1), s_{2,2}^4 = f_2^4(2), \cdots, s_{2,5}^4 = f_2^4(5) \]
\[ s_{2,1}^5 = f_2^5(1), s_{2,2}^5 = f_2^5(2), \cdots, s_{2,5}^5 = f_2^5(5) \]

Finally, we can generate five shadows, see Fig. 7.

\[ S_1 = s_{1,1}^1 \cup s_{1,1}^2 \cup s_{1,1}^3 \cup s_{1,1}^4 \cup s_{1,1}^5 \cup s_{1,2} \cup s_{1,2}^1 \cup s_{1,2}^2 \]
\[ S_2 = s_{1,1}^2 \cup s_{1,2}^2 \cup s_{1,2}^3 \cup s_{1,2}^4 \cup s_{1,2}^5 \cup s_{2,2} \cup s_{2,2}^1 \cup s_{2,2}^2 \]
\[ S_3 = s_{1,3}^2 \cup s_{1,3}^3 \cup s_{1,3}^4 \cup s_{1,3}^5 \cup s_{1,3} \cup s_{2,3} \cup s_{2,3}^1 \cup s_{2,3}^2 \]
\[ S_4 = s_{1,4}^2 \cup s_{1,4}^3 \cup s_{1,4}^4 \cup s_{1,4}^5 \cup s_{1,4} \cup s_{2,4} \cup s_{2,4}^1 \cup s_{2,4}^2 \]
\[ S_5 = s_{1,5}^2 \cup s_{1,5}^3 \cup s_{1,5}^4 \cup s_{1,5}^5 \cup s_{1,5} \cup s_{2,5} \cup s_{2,5}^1 \cup s_{2,5}^2 \]

All shadows are shown in Fig. 7. Then, these shadows will be distributed to different participants.

Finally, the image restoration process is similar to Example 1. The recovery results are shown in Fig. 8.

**FIGURE 8.** Shadow image. (a) is image restored with 3 shadows; (b) is image restored with 4 shadows.

B. PERFORMANCE AND SECURITY ANALYSIS

A novel \((k, n)\) PSIS scheme based on semantic segmentation is proposed in this paper. Secret image segmentation is performed based on semantics. Note that the proposed scheme is suitable for images with two or more non-overlapping sensitive areas or target objects. Only specific objects in the image participate in the generation of shadows. The rest is filled as a background image and can be publicly transmitted or restored on the network. In addition, since the background image is filled, it will not cause the attackers’ suspicion. Furthermore, this solution sets the priority for the divided objects. The higher the priority of the target object, the less shadows are required during the recovery phase.

In practice, our proposed scheme has some advantages. First, the proposed scheme is the first to use image semantic segmentation for PSIS, which provides a new research idea for other researchers in the study of SIS schemes. Second, the advantage of this image segmentation method is that it saves storage space, since the secret sharing technology does not target the entire image, but a specific area in the image. Therefore, this method reduces the shadow size. Whether it is image storage or transmission, it will greatly save resources and bring convenience to image information hiding. Finally, since the background image is publicly transmitted on the Internet, if it is lost or damaged during the transmission process, we can request the sender to send it again. Thus, the loss of the background image will not affect the recovery of the final secret image. Furthermore, if only part of the shares is lost and the number of shares available can still reach the recovery threshold, the final secret image can still be recovered.

In addition, the proposed \((k, n)\) PSIS scheme meets security requirements. On the one hand, it is determined by the characteristics of secret sharing technology; on the other hand, semantic segmentation method is used to hide important information of the image. Thus, the original secret image is presented in a completely new way, which can avoid attracting people’s attention. The secret sharing method used is similar to that of Liu-Yang’s scheme [29]. Based on that, our scheme sets the priority for the divided sub-images. In practical applications, a sub-image can be recovered based on the needs of relevant parties.

V. COMPARISON WITH RELATED WORKS

In this section, we will compare our scheme with the related works in [13], [15], [22], [24], [28], [29], [31] from several aspects to show the advantages of our proposed scheme.

First, we will discuss whether the division of sub-images has practical significance. In SIS schemes, before the shadow is generated, the secret image is often divided into multiple sub-images. In this paper, we divide the original image according to the content of the secret image. This means the secret image is divided based on image semantics. The sensitive areas or the specific objects in the image are separated, and they are the shared objects. The advantage of this technique is that relevant persons can gradually restore the secret image according to the application requirements in certain fields. At present, the existing SIS schemes such as those in [13], [15], [28], [29] have not yet segmented images based on semantics, the entire secret image is usually divided into multiple non-overlapping sub-images based on the spatial domain.

Next, this paper sets priority to the sub-images. In our solution, since the image segmentation method based on semantics is used, the separated sub-images have different practical significances. Then we assign priorities to these sub-images based on the semantic content of the sub-images. The higher the priority is, the fewer shadows are needed during the recovery phase. In contrast, there is no priority involved in these schemes such as those in [15], [24], [28], [29], [31].

Finally, we will compare the size of the shadow image. In the proposed scheme, we do not secretly share the entire image. Instead, we let one or more specific target objects
in the image be the secretly shared objects. The shadow size in the proposed scheme is \( n|M \times N| \sum_{i=0}^{t-1} \frac{1}{n+i} \), where \( |M \times N| \) and \( t \) are the size and number of the separated sub-images, respectively. Therefore, \( n|M \times N| \sum_{i=0}^{t-1} \frac{1}{n+i} < n|O| \sum_{i=0}^{t-1} \frac{1}{n+i} \), where \( |O| \) is the size of the secret image. In [15], the shadow size is \( \frac{|O|}{k(n+1)} \), which depends on the values of \( k \) and \( n \). It is easy to prove that \( \frac{(k+1)|O|}{(kn+1)} < \frac{|O|}{k} \). However, in our scheme, the shadow size depends on the values of \( k \) and \( n \) and the size and number of the separated sub-images. A novel \((n, n)\) SIS scheme in [31] is proposed. The shadow size is \( |O| \), which is larger than that in [15]. In fact, if the target sub-images are very small, the shadow size in the proposed scheme will be very small. Therefore, in our scheme, the specific shadow size depends on the characteristics of the secret image in practical applications.

Actually, in the existing SIS schemes, the shadow size and smoothness when restoring the original image are commonly used indicators to measure the performance of the schemes. The sub-images in the proposed scheme are obtained based on semantic segmentation and the shared object is not the entire secret image, but the separated sub-images. Therefore, the smoothness of the recovery depends on the number of separated sub-images. This is different from other PSIS schemes like [28].

**TABLE 1. Comparisons with related schemes.**

| Threshold property | Segmentation method | Shared object | Progressive |
|--------------------|---------------------|---------------|-------------|
| [15] \( k' < k < k'' < n \) | Space-based | O | no |
| [22] \( k < n \) | no | O | yes |
| [28] \( k < n \) | Space-based | O | yes |
| [29] \( k < n \) | Space-based | O | yes |
| [31] \( k = n \) | no | O | no |
| Our scheme \( k < n \) | Semantic-based | Prat | yes |

Besides, the five differences including the threshold property, segmentation method, shared object and progressive between the proposed scheme and related schemes are given in Table 1. In Table 1, the schemes in [15], [22], [28], [29] and [31] are different; \( k, k', k'' \) are different thresholds. In this paper, the threshold is not limited by the scheme itself, and it just satisfies the condition of \( k < n \). In addition, the unique feature of the proposed scheme is to segment the original secret image based on semantics and let the divided sub-images which are just a part of the secret image as the shared objects.

VI. CONCLUSION

At present, image semantic segmentation technology is widely used in many fields, e.g., automatic driving of cars, diagnosis of medical images etc. When these divided images are stored and transmitted on the network, it is important to ensure their security.

In this paper, a new \((k, n)\) PSIS scheme based on semantic segmentation is proposed. First, according to the characteristics of the secret image and the needs of relevant users or specific application scenarios, the confidential image is segmented based on semantics. Only particular objects or sensitive areas in the image will be used for secret sharing, and the remaining part can be publicly transmitted or stored after being processed. In addition, the segmented target sub-images are assigned different priorities. The higher the priority, the less shadows are needed to restore it, and by analogy, the sub-image with the lowest priority will be the last one to be restored. This solution not only reduces the shadow size, saves storage space, but also provides convenience for hiding image information. In fact, the background image in the proposed scheme is processed by filling, and the resulting image is still insufficient. Therefore, our future work is to find the optimal image processing method including selecting a more appropriate image semantic segmentation method. It aims to make the processed image look natural, thus, it will not be suspected by the attackers. We can also apply the proposed scheme to social networks [32], multi-agent systems [33], automated manufacturing systems [34] and cyber physical systems [35].

**REFERENCES**

[1] A. Al-Haj and H. Abdel-Nabi, "Digital image security based on data hiding and cryptography," in Proc. 3rd Int. Conf. Inf. Manage. (ICIM), Chengdu, China, Apr. 2017, pp. 437–440.

[2] G. Madhgu, G. Holfi, and S. Murthy, "An overview of image security techniques," Int. J. Comput. Appl., vol. 154, no. 6, pp. 37–46, Nov. 2016.

[3] Y. Tan, J. Qin, L. Tan, H. Tang, and X. Xiang, "A survey on the new development of medical image security algorithms," in Proc. Int. Conf. Cloud Comput. Secur., Hainan, China, 2018, pp. 458–467.

[4] M. S. Ramya, P. S. Somn, and L. R. Deeptha, "A novel approach for image sharing using reversible watermarking," in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Udupi, India, Sep. 2017, pp. 338–343.

[5] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," Opt. Lasers Eng., vol. 90, pp. 146–154, Mar. 2017.

[6] S. Zhang, X. Li, Q. Li, and Q. Zhou, "Image information hiding method for JPEG data flow," in Proc. 8th Int. Conf. Infell. Syst., Modelling Simulation (IMSIS), Kuala Lumpur, Malaysia, May 2018, pp. 67–71.

[7] X. Yan, Y. Lu, and L. Liu, "A general progressive secret image sharing construction method," Signal Process., Image Commun., vol. 71, pp. 66–75, Feb. 2019.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vis. Comput., vol. 24, no. 9, pp. 926–934, Sep. 2006.

[9] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image information hiding algorithm that employs edge detection and data coding," Comput. Methods Programs Biomed., vol. 127, pp. 24–43, Apr. 2016.

[10] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[11] R.-Z. Wang and C.-H. Su, "Secret image sharing with smaller shadow images," Pattern Recognit. Lett., vol. 27, no. 6, pp. 551–555, Apr. 2006.

[12] T.-H. Chen and C.-S. Wu, "Efficient multi-secret image sharing based on Boolean operations," Signal Process., vol. 91, no. 1, pp. 90–97, Jan. 2011.

[13] K. Shankar and P. Eswaran, "A new k out of n secret image sharing scheme in visual cryptography," in Proc. 10th Int. Conf. Intell. Syst. Control (ISCO), Coimbatore, India, Jan. 2016, pp. 1–6.

[14] K. Brindha and N. Jayanthi, "Secret image enhanced sharing using visual cryptography," Cybern. Inf. Technol., vol. 17, no. 3, pp. 128–139, Sep. 2017.

[15] 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., vol. 78, no. 13, pp. 18653–18667, Jul. 2019.
[16] X. Wu and C.-N. Yang, “A combination of color-black-and-white visual cryptography and polynomial based secret image sharing,” J. Vis. Commun. Image Represent., vol. 61, pp. 74–84, May 2019.

[17] C.-C. Thien and J.-C. Lin, “Secret image sharing,” Comput. Graph., vol. 26, no. 5, pp. 765–770, Oct. 2002.

[18] Y. Liu and C. Yang, “Scalable secret image sharing scheme with essential shadows,” Signal Process., Image Commun., vol. 58, pp. 49–55, Oct. 2017.

[19] K. M. Faroum, “A novel fast and provably secure (t, n)-threshold secret sharing construction for digital images,” J. Inf. Secur. Appl., vol. 19, no. 6, pp. 331–340, 2014.

[20] A. Kanso and M. Ghebleh, “An efficient (t, n)-threshold secret image sharing scheme,” Multimedia Tools Appl., vol. 76, no. 15, pp. 16369–16388, 2017.

[21] H. Prasetyo and C.-H. Hsia, “Improved progressive secret sharing with priority weight,” in Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW), Yilan, Taiwan, May 2019, pp. 1–2.

[22] L. Liu, Y. Lu, X. Yan, and S. Wan, “A progressive threshold secret image sharing with meaningful shares for gray-scale image,” in Proc. 12th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN), Hefei, China, Dec. 2016, pp. 380–385.

[23] 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.

[24] Z.-H. Wang, Y.-F. Di, J. Li, C.-C. Chang, and H. Liu, “Progressive secret image sharing scheme using meaningful shadows,” Secur. Commun. Netw., vol. 9, no. 17, pp. 4075–4088, Nov. 2016.

[25] Y.-C. Hou and Z.-Y. Quan, “Progressive visual cryptography with unexpanded shares,” IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1760–1764, Nov. 2011.

[26] H.-C. Chao and T.-Y. Fan, “Random-grid based progressive visual secret sharing scheme with adaptive priority,” Digit. Signal Process., vol. 68, pp. 69–80, Sep. 2017.

[27] R.-Z. Wang and S.-J. Shyu, “Scalable secret image sharing,” Signal Process., Image Commun., vol. 22, no. 4, pp. 363–373, Apr. 2007.

[28] Y. Guo, Z. Ma, and M. Zhao, “Polynomial based progressive secret image sharing scheme with smaller shadow size,” IEEE Access, vol. 7, pp. 73782–73789, 2019.

[29] Y.-X. Liu, C.-N. Yang, Q.-D. Sun, and Y.-C. Chen, “(k, n) scalable secret image sharing with multiple decoding options,” J. Intell. Fuzzy Syst., vol. 38, no. 1, pp. 219–228, Jan. 2020.

[30] Y. Li, H. Qi, J. Dai, X. Ji, and Y. Wei, “Fully convolutional instance-aware semantic segmentation,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Honolulu, HI, USA, Jul. 2017, pp. 2359–2367.

[31] L. Dong and M. Ku, “Novel (n, n) secret image sharing scheme based on addition,” in Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., Darmstadt, Germany, 2010, pp. 583–586.

[32] L. Yang, Z. Yu, M. A. El-Meligy, A. M. El-Sherbini, and N. Wu, “On multiplicity-aware influence spread in social networks,” IEEE Access, vol. 8, pp. 106705–106713, 2020.

[33] X. Li, Z. Yu, Z. Li, and N. Wu, “Group consensus via pinning control for a class of heterogeneous multi-agent systems with input constraints,” Inf. Sci., vol. 542, pp. 247–262, Jan. 2021, doi: 10.1016/j.ins.2020.05.085.

[34] X. Zan, Z. Wu, C. Guo, and Z. Yu, “A Pareto-based genetic algorithm for multi-objective scheduling of automated manufacturing systems,” Adv. Mech. Eng., vol. 12, no. 1, pp. 1–15, 2020.

[35] S. Zhou, Z. Yu, E. S. A. Nasr, H. A. Mahmoud, E. M. Awwad, and N. Wu, “Homomorphic encryption of supervisory control systems using automata,” IEEE Access, vol. 8, pp. 147185–147198, 2020, doi: 10.1109/ACCESS.2020.3014217.

LINA ZHANG received the Ph.D. degree in applied mathematics from Wuhan University, in 2008. She is currently an Associate Professor with the College of Computer Science and Technology, Xi’an University of Science and Technology. Her research interests include cryptography and information security.

XIANGQIN ZHENG received the B.S. degree in the Internet of Things from Suzhou University. She is currently pursuing the master’s degree with the College of Computer Science and Technology, Xi’an University of Science and Technology. Her research interests include cryptography and information security.

YING LIU is currently a Senior Engineer with the National Key Laboratory for Complex Systems Simulation, Beijing, China. Her research interests include information security, artificial intelligence, and intelligent system security and control.

VOLUME 8, 2020