Thresholds Based Image Extraction Schemes in Big Data Environment in Intelligent Traffic Management

Yanxiao Liu, Chingnung Yang, *Senior Member, IEEE*, and Qindong Sun

***Abstract*— Video traffic monitoring is an inexpensive and convenient source of traffic data. Traffic images processing are widely used to check traffic conditions and they can determine traffic control strategies in intelligent transportation systems (ITS). However, these traffic images always contain privacy-related data, such as vehicles registration numbers, human faces. Misuse of such data is a threat to the privacy of vehicles divers, passengers, pedestrians, etc. This paper proposes a thresholds-based images extraction solution for ITS. At first, a Faster Region Convolutional Neural Networks (RCNN) model is used to segment a traffic image into multi-regions with different importance levels; then, multi-threshold image extraction schemes are designed based on progressive secret image sharing schemes to extract images contain key traffic information, such as reg number, human faces, in which the region with higher importance level requires higher threshold for extraction. For different roles in ITS, they can extract images with different details, which can protect privacy and anonymity. The proposed methods provide a safe and intelligent way to extract images that can be used for further analysis in ITS.**

***Index Terms*— Image extraction, threshold, intelligent traffic management, big data.**

I. Introduction

With the rapid development of informatization and intelligent, information extraction and analysis in the field of intelligent traffic management [1]–[3] becomes an important research issue. At the same time, analysis on traffic related image plays an important role in modern traffic management industry. For instance, the images of real-time traffic are the basis of designing high efficiency navigation algorithms [4]–[6]; Big monitoring image data on urban traffic conditions can be used for optimization on urban traffic design [7], [8]; Driverless technology is based on the information extracted from vehicle cameras [9], [10], and the vehicle detecting and counting from all source images are also important for retail market prediction and environment monitoring [11], [12].

Normally traffic images would include sensitive information that involve security and privacy issues, it is reasonable that some sensitive traffic images can be only extracted by authorized parties. Privacy protection [13], [14] has already becomes an important topic in traffic management industry. Most existed approaches discussed prevention of information leakage from single party. However, a traffic management system usually consists of multiple authorized parties, it is also necessary to design a safe guarding sensitive image scheme among multiple authorized parties, which is more efficiency than carrying out privacy protection on each party repeatedly. In addition, a traffic image includes different information in different areas, and those information have different importance levels. It is reasonable to protect those areas with different strategies among multiple parties. Thus the motivation of our work is to construct high efficiency image protection schemes among multiple parties in traffic management industry, where the different areas in the image can be extracted with different strategies according to their importance levels.

Secret image sharing [15], [16] (SIS) is a threshold based scheme that can protect an image among multiple participants. In SIS, an image is encoded into n shadows, each shadow does not leak any information on the image. The image can be extracted only when k ($k \leq n$) or more shadows involve in, and less than k shadows can not extract the image at all. Thus the parameter k is the threshold for image extraction in SIS, such approach can be adopted in traffic management industry to construct image protection schemes among multiple parties. The technology of SIS can be mainly classified into two categories, visual cryptography (VC) based SIS and polynomial based SIS. While VC based SIS can extract image without any computation, but the extracted image is quality loss and the shadow size is expanded from image; polynomial based SIS can extracted lossless image with reduced shadow size, the computation is based on Lagrange Interpolation. Since polynomial based SIS can extract original images, which is more suitable than VC based SIS in traffic management industry. Various SIS schemes with special functions were also proposed. For instance, SIS schemes with authentication [17], [18] can verify the validity of each shadow before image extraction, threshold changeable SIS [19], [20] can adjust the threshold dynamically according to the security requirement; multi-SIS

Manuscript received January 31, 2020; revised April 17, 2020; accepted May 8, 2020. This work was supported in part by the National Natural Science Foundation under Grant 61571360, in part by the Youth Innovation Team of Shaanxi Universities, in part by the Innovation Project of Shaanxi Provincial Department of Education under Grant 17JF023, in part by the Project of Xi'an Technology Bureau under Grant GXYD14.12 and Grant GXYD14.13, in part by the Ministry of Science and Technology under Grant MOST 107-2221-E-259-007, and in part by the Ministry of Science and Technology (MOST) through Pervasive Artificial Intelligence Research (PAIR) Labs, Taiwan, under Contract 108-2634-F-259-001. The Associate Editor for this article was S. Mumtaz. *(Corresponding author: Qindong Sun.)*

Yanxiao Liu and Qindong Sun are with the Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China (e-mail: sqd@xaut.edu.cn).

Chingnung Yang is with the Department of Computer Science and Information Engineering, National Dong Hwa University, Shoufeng 974, Taiwan.

Digital Object Identifier 10.1109/TITS.2020.2994386

schemes [21], [22] can extract more than one secret image through one extraction procedure, and the SIS schemes [23] considered hiding meaningless shadow into meaningful cover images. Progressive SIS (PSIS) scheme [24]–[30] is also an important type of SIS that has a different extraction model other than the traditional (k, n) threshold. During extraction procedure in PSIS, k to n shadows can gradually reconstruct the image, more participated shadows deduce higher proportion on reconstructed information to original image. Such extraction model is called progress extraction, and it can expend application on SIS into many scenarios.

In this work, image extraction schemes are proposed using the concept of PSIS in traffic management industry, where a group of parties can safely guarding the traffic image based on different thresholds. First we use Faster RCNN model [31] as the tool for image segmentation, where the training images come from KITTI dataset and traffic big image data collection systems. The traditional image segmentation was based on artificial features, which has low efficiency and accuracy. In modern traffic management, the big image data environment makes artificial feature based image segmentation unrealistic. Therefore deep learning algorithm is used in our work for image segmentation, then the image can be divided into multiple regions with different contents and importance levels efficiently. The main contributions in this work are summarised as following:

(1) The concept of threshold based image extraction from big data environment in intelligent traffic management is first proposed.
(2) It is reasonable that parties with higher authority can extract more information in traffic image, and progressive secret image sharing based image extraction schemes are designed that can achieve this property.
(3) An image extraction scheme is designed where the parties can be divided into senior parties and junior parties, that can also expand the application in intelligent traffic management.

The secure management on traffic images would be an important issue in ITS systems. Our proposed schemes are threshold-based schemes, that enable a group of participants safely guarding traffic images together. Since threshold-based approach is a popular method for safe management, it could be also effective in ITS systems either.

The rest of this manuscript is organized as follows. In **Section** 2, we introduced some related works, which includes a brief description on polynomial based SIS, some results on PSIS schemes and an introduction on Faster RCNN model. In **Section 3**, we construct three image extraction schemes in traffic management industry. In first two schemes, all parties are equal, but the image extraction models are different; in last scheme, all parties are classified into senior parties and junior parties. The experimental results and comparisons are listed in **Section 4**, and the conclusion is made in **Section 5** at last.

II. Related Works

In this part, some related works are described in subsections respectively. Since our work is constructing image extraction scheme using polynomial based PSIS, and the image is segmented into regions using Faster RCNN model in advance, the following related work consists of polynomial based SIS, PSIS and introduction on Faster RCNN model respectively.

A. Polynomial Based SIS

Polynomial based SIS [16] was introduced d by Thien and Lin in 2002, which consists of two phases: ***Shadow Generation*** and ***Image Reconstruction***. During **Shadow Generation**, the algorithm $\boldsymbol{ShadowGe}_{(k,n)}^{Thien-Lin}(O)$ takes an image O as input, and outputs n shadows $S_1, S_2, \ldots, S_n$; during **Image Reconstruction**, an algorithm $\boldsymbol{ImageRe}_{(m)}^{Thien-Lin}$ takes a group of m shadows as inputs, and outputs the reconstructed image O. The scheme is shown below.

Thien-Lin's polynomial based (k, n) SIS

(1) ***Shadow Generation***:
$\boldsymbol{ShadowGe}_{(k,n)}^{Thien-Lin}(O) \rightarrow (S_1, S_2, \ldots, S_n)$
1 The image O is divided into non-overlapping k pixel blocks, $B_1, B_2, \ldots, B_l$.
2 For k pixels $p_{j,0}, p_{j,1}, \ldots, p_{j,k-1}$ in each block B_j, $j \in [1, l]$, generating a $k-1$ degree polynomial $f_j(x) = p_{j,0} + p_{j,1}x + p_{j,2}x^2 + \ldots, + p_{j,k-1}x^{k-1}$.
3 Using $f_j(x)$ to compute n sub-shadows $v_{j,1} = f_j(1), v_{j,2} = f_j(2), \ldots, v_{j,n} = f_j(n)$, $j \in [1, l]$.
4 The n shadows are $S_i = v_{1,i} \parallel v_{2,i} \parallel, \ldots, \parallel v_{l,i}, i = 1, 2, \ldots, n$.

(2) ***Image Reconstruction***:
$\boldsymbol{ImageRe}_{(m)}^{Thien-Lin} \rightarrow O^*$
1 Without loss of generality, suppose the m shadows are $S_1, S_2, \ldots, S_m$. Compute all k coefficients in $f_j(x)$ from the sub-shadows $v_{1,j}, v_{2,j}, \ldots, v_{m,j}$, $j \in [1, l]$ using lagrange formula

$$f_j(x) = \sum_{i=1}^{m} (v_{i,j} \times \prod_{l \neq i} \frac{x - l}{i - l}) \quad (1)$$

to recover the block B_j^*.
2 The reconstructed image is $O^* = B_1^* \parallel B_2^* \parallel, \ldots, \parallel B_l^*$.

Since each polynomial $f_j(x)$ is $k-1$ degree, only k or more sub-shadows can reconstruct $f_j(x)$, less than k sub-shadows get no information on $f_j(x)$ at all. Therefore Thien-Lin's scheme satisfies k-threshold property:

1) k or more shadows can reconstruct entire image.
2) less than k shadows get noting on secret image.

Since the computation complexity of Lagrange interpolation is about $O(n^2)$, the computation complexity of polynomial based SIS is about $O(N^2)$, where N is the number of pixels in an image. On the other hand, the computation in polynomial based SIS is the $GF(251)$, the pixels with gray value larger than 250 are all replaced to 250. There would be quality

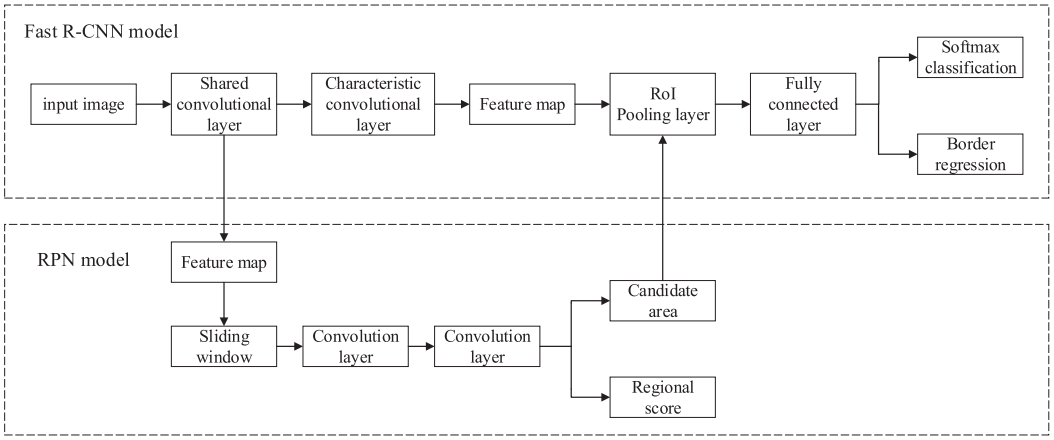

Fig. 1. Faster RCNN model.

distortion on reconstructed image, but it has little influence for obtaining image information.

B. Progressive SIS

Traditional (k, n) SIS has the property that a group of shadows can either reconstruct the entire image or nothing at all. Progressive (k, n) SIS (PSIS) provides a different reconstruction model other than traditional SIS. Suppose the symbol $Pr_{(m)}^{(O)}$ denote the proportion of reconstructed information from m shadows to original image O, then the property of reconstruction model in (k, n) PSIS can be summarized as follows.

(1) when $m < k$, $Pr_{(m)}^{(O)} = 0$; when $m = n$, $Pr_{(m)}^{(O)} = 1$.

(2) for $k \leq m_1 < m_2 < n$, $0 < Pr_{(m_1)}^{(O)} < Pr_{(m_2)}^{(O)} < 1$.

Many works discussed the approaches for PSIS. The schemes [24]–[26] were VC based PSIS schemes, while schemes [24], [25] were $(2, n)$ PSIS, where 2 to n shadows can gradually recover the image, and the scheme [26] extended $(2, n)$ PSIS to a general (k, n) PSIS. The first polynomial based PSIS [27] was proposed by Wang and Shyu, which is also a $(2, n)$ PSIS. Later, Yang and Huang [28] extended the scheme [27] to a general (k, n) PSIS. In [29] and [30], two (k, n) polynomial based PSIS schemes were constructed to satisfy the property of smooth reconstructing. The schemes [30] were interested in reducing shadow size in polynomial based PSIS schemes.

C. Faster RCNN Model

In recent years, CNN based deep learning algorithms have made significant progress in image recognition and detection. CNN has the property of weight sharing and local perception, which makes it possesses the adaptability to deformation and displacement. Region CNN (RCNN) model uses selective searching instead of traditional sliding region-based candidate region extraction to obtain the candidate region of the suspected target. Fast RCNN model is based on RCNN, which uses a special pooling layer (Region of Interest RoI) to improve the speed of target detection. Faster RCNN uses Region Proposal Networks (RPN) instead of selective searching to extract candidate region, which further improves the efficiency of candidate region extraction from Fast RCNN. In this work, Faster RCNN model is adopted to segment traffic images into regions, where the regions include different contents with different importance levels. The high speed and accuracy of Faster RCNN in target detection would improve the efficiency for image segmentation in traffic big image data environment.

The model of Faster RCNN is shown in Fig.1. In Faster RCNN model, convolution layer is used to extract the features of image. The input is the entire image, and the output is the extracted feature which is also called feature maps. The RPN network is used to recommend candidate regions. This network is used to replace the previous search selective. The input is feature maps, and the output is multiple candidate regions. RoI pooling converts different sized inputs into fixed-length outputs. The output of the classification and regression layers is the class to which the candidate region belongs, and the precise location of the candidate region in the image.

III. Proposed Schemes

In this part, we introduce the image extraction schemes in traffic management industry, where those images come from big traffic image data environment. Our schemes consists of two parts, (1) Image segmentation using Faster RCNN model; (2) Construction of image extraction schemes using polynomial based PSIS. These two parts are described in following subsections respectively.

A. Image Segmentation Using Faster RCNN

The architecture of Faster RCNN model used in our work is shown in Fig.1. This Faster RCNN model is made up of two modules: RPN candidate frame extraction module and the Fast RCNN target detection module. RPN and Fast RCNN share the same input feature maps which are extracted by the base convolutional network. The function of RPN is generating proposals from the feature maps. 512-dimensional feature maps

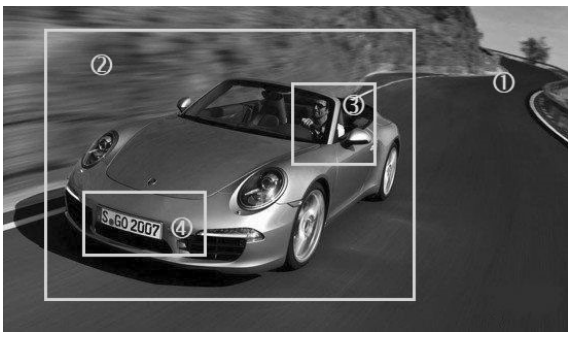

Fig. 2. Image segmentation using Faster RCNN model.

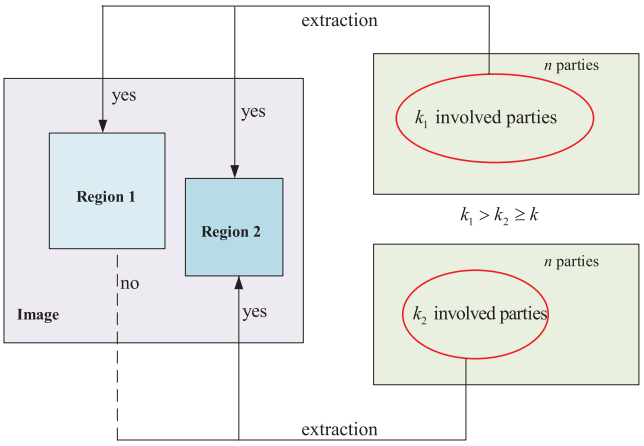

Fig. 3. Diagram of threshold based image extraction scheme.

are extracted from the entire image using base convolutional network. Fast RCNN network is used for classifying the object proposals which are detected by RPN. It takes an entire image and a set of object proposals as input, each object proposal is mapped to a region of interest from feature maps. After that, the ROI pooling layer uses max pooling to convert the features into a fixed spatial extent of 7×7. The 7×7 feature vector is fed into a sequence of fully connected layer that finally branch into two output layers-softmax results and bounding box regression results. This Faster RCNN model in our work is initialized with an ImageNet pre-trained model (VGG16). Our scheme has the capability to segment image into regions and provides different thresholds for each region according to the important levels. Normal traffic images can be obtained in our scheme, especially the traffic images that contains various information, like vehicle, human, weather conditions, etc. The following Fig.2 (http://iitlab.bit.edu.cn/mcislab/vehicledb/) shows an example of image segmentation result using Faster RCNN, where an image is segmented into 4 regions with different targets and importance levels.

B. Thresholds Based Image Extraction Schemes

In this subsection, we construct three thresholds based image extraction schemes on the traffic images, where those images have already been segmented into multiple regions. The following **Scheme 1** is based on a (k,n) PSIS, that each region has a threshold for extraction. The **Scheme 1** achieves the basis function that more parties can extracted more information with higher importance level on the original image.

Suppose the image O is segmented into u non-overlapping regions $O_i, i = 1,2,\ldots,u$, where the importance level (denoted as $Im_{(i)}$) of O_i satisfies $Im_{(u)} > Im_{(u-1)} > \ldots > Im_{(1)}$, Our **Scheme 1** is described as follows.

Scheme 1: Image extraction among multiple parties using (k,n) PSIS

(1) ***Shadow Generation Phase***:

Input: secret image O, which consists of u regions $O_1, O_2, \ldots, O_u$. Invoking an algorithm $\boldsymbol{ShadowGe}_{(k,n)}^{PSIS}(O)$ as following steps, where the parameters k and n satisfy $n-k+1=u$.

1 For each region $O_i, i = 1,2,\ldots,u$, generate n sub-shadows $v_{i,1}, v_{i,2}, \ldots, v_{i,n}$ using the algorithm $\boldsymbol{ShadowGe}_{(k+i-1,n)}^{Thien-Lin}(O_i)$.

2 The n shadows $S_i, i = 1,2,\ldots,n$ are $S_i = v_{1,i} \bigcup v_{2,i} \bigcup \ldots \bigcup v_{u,i}$.

(2) ***Image Reconstruction Phase***:

Input: m shadows (without loss of generality $S_1, S_2, \ldots, S_m$), using the algorithm $\boldsymbol{ImageRe}_{(m)}^{PSIS}$ as the following steps.

1 For each region $O_i, i = 1,2,\ldots,u$, using $\boldsymbol{ImageRe}_{(m)}^{Thien-Lin}$ from the m sub-shadows $v_{i,1}, v_{i,2}, \ldots, v_{i,m}$ to reconstruct the region O_i^*, where the sub-shadow $v_{i,j}$ is extracted from shadow S_j, $j = 1,2,\ldots,m$.

2 The reconstructed partial image is $O_{(m)}^* = \bigcup O_i^*$.

The idea of **Scheme 1** can be also described in Fig.3. The property of image extraction in **Scheme 1** is analyzed in following **Theorem 1**.

*Theorem 1: In **Scheme 1**, k to n parties can gradually extract the image, and less than k parties get no information on the image at all.*

Proof: In **Scheme 1**, each shadow S_i consists of u sub-shadows from u region $O_1, O_2, \ldots, O_u$. On the other hand, the n sub-shadows $v_{i,1}, v_{i,2}, \ldots, v_{i,n}$ from O_i are generated using $\boldsymbol{ShadowGe}_{(k+i-1,n)}^{Thien-Lin}(O_i)$, the threshold for reconstructing O_i is $k+i-1$. Therefore any $k+i-1$ or more shadows can reconstruct the regions $O_1, O_2, \ldots, O_i$, less than k shadows get no information on each region O_i at all. Since the parameters satisfy $u = n-k+1$, k to n shadows can gradually extract the image $O = O_1 \bigcup O_2 \bigcup \ldots \bigcup O_u$. Further more, since the regions have different importance levels $Im_{(u)} > Im_{(u-1)} > \ldots > Im_{(1)}$, the region with higher importance level requires higher threshold for extraction.

Theorem 1 shows that k to n parties can gradually extract the image, and the property of image extraction is that more involved parties can recover more regions. Fig.3 can even clearly display the property of **Scheme 1**, if there are not enough involved parties, no information on some regions can be extracted at all. In order to complete the application on image extraction in traffic management industry, we construct

another PSIS based image extraction in following **Scheme 2**, that has different image extraction model with **Scheme 1**.

Scheme 2: Image extraction using (k, n) PSIS with different extraction model

(1) ***Shadow Generation Phase***:

Input: secret image O, which consists of u regions $O_1, O_2, \ldots, O_u$.

1 For each region $O_i, i = 1, 2, \ldots, u$, dividing all pixels in O_i into $n - k + 1$ subsets $\mathcal{T}_{i,k}, \mathcal{T}_{i,k+1}, \ldots, \mathcal{T}_{i,n}$, that satisfies:
   a) for any $r \in [k, n]$, $\sum_{j=k}^{n} |\mathcal{T}_{r,j}| = |O_r|$.
   b) suppose O_{i_1}, O_{i_2} are two regions where $Im_{(i_1)} < Im_{(i_2)}$. For any m that $k \le m < n$, $\frac{\sum_{j=k}^{m} |\mathcal{T}_{i_1,j}|}{|O_{i_1}|} > \frac{\sum_{j=k}^{m} |\mathcal{T}_{i_2,j}|}{|O_{i_2}|}$.

2 The pixels in the subset $\mathcal{T}_{i,t}$ $(k \le t \le n)$ are generated into $s_{i,t,1}, s_{i,t,2}, \ldots, s_{i,t,n}$ using $\boldsymbol{ShadowGe}_{(t,n)}^{Thien-Lin}(\mathcal{T}_{i,t})$. Then the sub-shadows on O_i is $v_{i,j} = s_{i,k,j} || s_{i,k+1,j} || \ldots || s_{i,n,j}, j = 1, 2, \ldots, n$.

3 The shadow $S_i, i = 1, 2, \ldots, n$ on O is $S_i = v_{1,i} || v_{2,i} || \ldots || v_{u,i}$.

(2) ***Image Reconstruction Phase***:

Input: m shadows (without loss of generality $S_1, S_2, \ldots, S_m$), using the algorithm $\boldsymbol{ImageRe}_{(m)}^{PSIS}$ as the following steps.

1 For each region $O_i, i = 1, 2, \ldots, u$, using $\boldsymbol{ImageRe}_{(m)}^{Thien-Lin}$ from the m sub-shadows $v_{i,1}, v_{i,2}, \ldots, v_{i,m}$ to reconstruct the subsets $\mathcal{T}_{i,k}, \mathcal{T}_{i,k+1}, \ldots, \mathcal{T}_{i,n}$ on region O_i.

2 The reconstructed partial image is $O_{(m)}^{*}$ is made up of all reconstructed subsets in each region.

The property of image extraction in **Scheme 2** is analyzed in following **Theorem 2.**

*Theorem 2: In **Scheme 2**, k to n parties can gradually extract each region $O_i, i = 1, 2, \ldots, u$ in the original image O. For any two regions O_{i_1}, O_{i_2} where $Im_{(i_1)} < Im_{(i_2)}$, any m parties $(k \le m < n)$ extract larger proportion of information on O_{i_1} than O_{i_2}.*

Proof: As described in **Scheme 2**, all pixels in each region O_i is divided into $n - k + 1$ sunsets $\mathcal{T}_{i,k}, \mathcal{T}_{i,k+1}, \ldots, \mathcal{T}_{i,n}$, and the pixels in subset $\mathcal{T}_{i,t}$ $(k \le t \le n)$ is encoded under threshold t, any m shadows can extract the subsets $\mathcal{T}_{i,k}, \mathcal{T}_{i,k+1}, \ldots, \mathcal{T}_{i,m}$ for each region. Thus each region O_i can be gradually extracted from k to n shadows, and the entire image O can be also extracted from k to n parties.

Next, for any two region O_{i_1}, O_{i_2} where $Im_{(i_1)} < Im_{(i_2)}$, m parties can extract the subsets $\mathcal{T}_{i_1,k}, \mathcal{T}_{i_1,k+1}, \ldots, \mathcal{T}_{i_1,m}$ and $\mathcal{T}_{i_2,k}, \mathcal{T}_{i_2,k+1}, \ldots, \mathcal{T}_{i_2,m}$ on O_{i_1} and O_{i_2} respectively. The proportions of extracted information on each region is $Pr_{(O_{i_1})}^{(m)} = \frac{\sum_{j=k}^{m} |\mathcal{T}_{i_1,j}|}{|O_{i_1}|}$ and $Pr_{(O_{i_2})}^{(m)} = \frac{\sum_{j=k}^{m} |\mathcal{T}_{i_2,j}|}{|O_{i_2}|}$. Since in **Scheme 2**, we have the requirement that $\frac{\sum_{j=k}^{m} |\mathcal{T}_{i_1,j}|}{|O_{i_1}|} > \frac{\sum_{j=k}^{m} |\mathcal{T}_{i_2,j}|}{|O_{i_2}|}$, the proportion of extracted information on O_{i_1} is larger than O_{i_2}: $Pr_{(O_{i_1})}^{(m)} > Pr_{(O_{i_2})}^{(m)}$.

Scheme 1 and **Scheme 2** both can extract traffic images gradually from k to n parties, but using different extraction model. There is also a common feature in **Scheme 1** and **Scheme 2** that all the n parties have equal authority in image extraction. However, the real traffic systems usually consist of multiple parties with unequal authorities. Therefore, designing an image extracting schemes among multiple parties, where the parties have different levels is necessary. In following **Scheme 3**, all n parties in a traffic system are divided into n_s senior parties and n_j junior parties $(n_s + n_j = n)$. During image extraction, senior party has higher authority than junior party, at least k total parties which include at least t senior parties can start to extract the image, and the proportion of extracted information to original image is decided by the amount of involved senior parties. The concept of **Scheme 3** can be described in Fig.4.

Scheme 3: Image extraction among n_s senior and $n_j = n - n_s$ junior parties

(1)***Shadow Generation Phase***:

Input: segmented image $O = O_1 \bigcup O_2 \bigcup \ldots \bigcup O_u$

1 Generating $n_s + k - t$ intermediate-shadows $W_1, W_2, \ldots, W_{n_s+k-t}$ using $\boldsymbol{ShadowGe}_{(k,n_s+k-t)}^{PSIS}(O)$.

2 For the $k - t$ intermediate-shadows $W_j, j = n_s + 1, n_s + 2, \ldots, n_s + k - t$, using $\boldsymbol{ShadowGe}_{(k,n)}^{Thien-Lin}(W_j)$ to generate n sub-intermediate-shadows $w_{j,1}, w_{j,2}, \ldots, w_{j,n}$.

3 The n_s senior-shadows $S_i^{(senior)}, i = 1, 2, \ldots, n_s$ are $S_i^{(senior)} = W_i \| w_{n_s+1,i} \| w_{n_s+2,i} \|, \ldots, \| w_{n_s+k-t,i}$; the n_j junior-shadows $S_i^{(junior)}, i = n_s + 1, n_s + 2, \ldots, n$ are $S_i^{(junior)} = w_{n_s+1,i} \| w_{n_s+2,i} \|, \ldots, \| w_{n_s+k-t,i}$.

(2) ***Image Reconstruction Phase***:

Input: m shadows, which consists of r senior-shadows and $m - r$ junior-shadows.

1 Reconstructing each intermediate-shadow $W_1, W_2, \ldots, W_{s+k-t}$ using $\boldsymbol{ImageRe}_{(m)}^{Thien-Lin}$ from the m shadows.

2 Reconstructing each region O_i using $\boldsymbol{ImageRe}_{(m)}^{PSIS}$ from the reconstructed intermediate-shadows.

3 The extracted partial image is $O^m = \bigcup O_i$ where the region O_i is reconstructed.

The property of proposed **Scheme 3** is summarized in following theorems.

*Theorem 3: In **Scheme 3**, any sets include less than k total parties or any set includes less than t senior parties extract no information on the image.*

Proof: First we consider the case that less than k parties in total involved in image extraction. According to **Scheme 3**, each intermediate-shadows $W_{n_s+1}, W_{n_s+2}, \ldots, W_{n_s+k-t}$ is divided into n sub-intermediate-shadows using $\boldsymbol{ShadowGe}_{(k,n)}^{Thien-Lin}(W_j)$, the threshold for reconstructing W_j is k. Therefore less than k shadows in total can not recover any intermediate-shadow in $W_{n_s+1}, W_{n_s+2}, \ldots, W_{n_s+k-t}$.

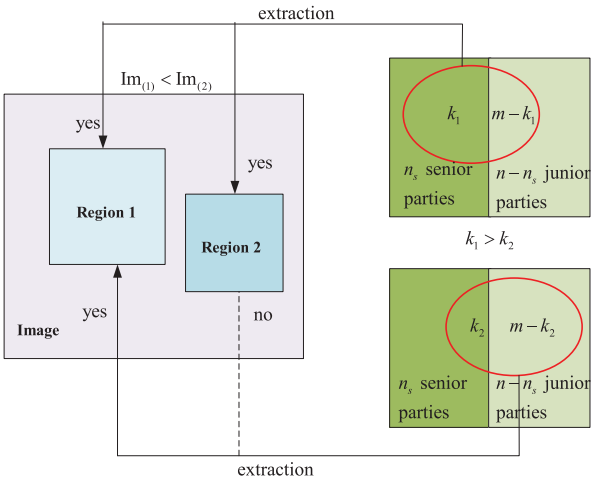

Fig. 4. Diagram of threshold based image extraction scheme among senior and junior parties.

therefore less than k shadows can get less than k intermediate-shadows in total. Since all intermediate-shadows are generated from $\boldsymbol{ShadowGe}^{PSIS}_{(k,n_s+k-t)}(O)$, at least k temporary shadows are needed to partially recover secret image, less than k shadows get noting on the secret image O.

Next we consider the case that k or more parties in total which include r senior-shadows ($r < t$) involved in image extraction. According to above analysis, these shadows can reconstruct $k-t$ intermediate-shadows $W_{n_s+1}, W_{n_s+2}, \ldots, W_{n_s+k-t}$, and each senior-shadow deduces one intermediate-shadow in $W_1, W_2, \ldots, W_{n_s}$, the total number of intermediate-shadows is $k-t+r < k$, as a result, no information can be extracted either in this case.

Theorem 4: In ***Scheme 3****, any set of k or more parties in total, which includes t to n_s senior parties can gradually extract the image.*

Proof: Suppose m parties in total, which include r senior parties involve in image extraction. ($m \geq k$, $s \geq r \geq t$). According to analysis above, $k-t+r \geq k$ intermediate-shadows can be recovered. All intermediate-shadows are generated using $\boldsymbol{ShadowGe}^{PSIS}_{(k,n_s+k-t)}(O)$, according to **Theorem 2**, k to n_s+k-t intermediate-shadows can gradually extract the image O. When the number r of senior parties changes from t to n_s, the number of intermediate-shadows changes from k to n_s+k-t correspondingly, thus the image $O = O_1 \bigcup O_2 \bigcup \ldots \bigcup O_u$ can be gradually extracted.

As a result, the proposed **Scheme 3** achieves the following properties: (1) senior party has greater authority than junior party; (2) regions with higher importance level requires higher threshold for extraction. The proposed **Scheme 3** is practical in traffic management systems. For example, three are officers with different positions in a traffic management system. The senior officer is able to recover more content of a traffic image captured by surveillance camera such as the appearance of the car, like the number shown on the plate, and the face of the driver; while junior officer can only observe less content of the traffic image. As a result, they have different authorities to deal with the traffic cases according to their levels. Using proposed **Scheme 3**, senior officer can recover the appearance of the car, the number shown on the plate, and the face of the driver to observe the behaviors of the car and the driver by a series of related traffic images; The junior officer can recover the car appearance and its plate and thus can exactly know the car trajectory.

The three schemes above are all PSIS schemes. In **Scheme 1**, k to n participants can gradually extract the image. But for some regions in this image, it is probable that no information can be extracted at all when the number of participants is larger than k. In **Scheme 2**, a certain ration information can be recovered for each region when there is any k to n participants. **Scheme 3** divides participants into senior participants and junior participants, where senior participants have stronger power than junior participants in image extraction. All the three proposed schemes are threshold based image extraction schemes. The region with higher importance level has higher threshold for extraction, when there are not enough participants, a region cannot be extracted entirely. But when the participants reach the threshold, the corresponding region can be extracted without distortion.

IV. Experimental Results and Analysis

Image extraction using proposed **Scheme 1**, **Scheme 2** and **Scheme 3** are shown in this part. According to the description above, the traffic images should be firstly segmented into regions where each region concludes different target, thus target detection is the base image segmentation. Therefore Faster RCNN model are chosen in our scheme due to its high efficiency on target detection. For the robustness and reliability, a large amount of image data is used for the training on Faster RCNN model. Thus, two sources of image data which include about 100000 traffic images are used in our experiments. One data source is the KITTI dataset which includes 7518 training images and 7481 testing images. Since the amount of images provided in KITTI dataset is not enough for training Faster RCNN model, about 85000 actual vehicle images, which are collected in the Chinese traffic environment are used as the second data source. The 7481 testing images from KITTI data set is used as testing set, and all the rest images are divided into two groups, more than 800000 images for training set and about 12000 images for validation set. The number of vehicles with different scales in each image can be up to a dozen, and various levels of occlusion and truncation. The annotation information is also very rich, including the type of target, whether it is truncated, occlusion, angle value, and related to people, cars and other categories.

This experiment is implemented under the caffe framework, based on the GPU-based high-speed computing platform. The specific hardware and software platforms are as follows:

1 Hardware platform: IntelCorei7-4710MQ, 2.5GHz Quad Core Processor, 16GB RAM, NVIDIA GeForce GTX1050Ti, 8GB DDR4.
2 Software platform: Windows10, MATLAB(R2014a), VisualCUDA7.5, CUDNN7.0, Caffe-Windows.

In order to show the advantage of target detection using Faster RCNN model, 4 different models are trained using

TABLE I
COMPARISON OF DETECTION PERFORMANCE OF DIFFERENT CNN BASED MODELS

Models	Correct detection	False detection	Miss detection	Accuracy rate	Recall rate	F1	Detection time(s)
CNN	21809	6151	8066	78.12%	72.93%	75.44	1.59
RCNN	23303	4439	6572	84.31%	77.84%	80.95	4.7
Fast RCNN	23601	3842	6274	85.74%	79.31%	82.40	2.32
Faster RCNN	25394	2511	4481	90.83%	85.43%	88.05	0.38

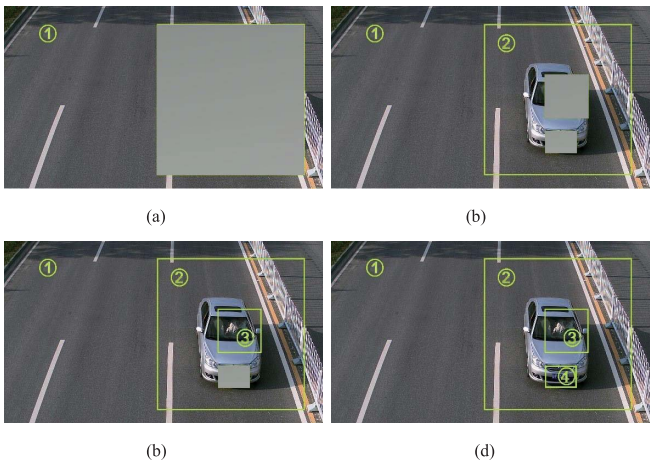

Fig. 5. Progressive image extraction on different regions.

TABLE II
THRESHOLDS FOR IMAGE RECONSTRUCTION ON PROPOSED **SCHEME 1** AND **SCHEME 3**

	Scheme 1 (k,n)		**Scheme 3** (t,n_s,k,n)	
	$(3,6)$	$(4,7)$	$(2,5,4,7)$	$(3,6,7,10)$
Fig.5(a)	$m=3$	$m=4$	$r=2, m\geq 4$	$h=3, m\geq 7$
Fig.5(b)	$m=4$	$m=5$	$r=3, m\geq 4$	$h=4, m\geq 7$
Fig.5(c)	$m=5$	$m=6$	$r=4, m\geq 4$	$h=5, m\geq 7$
Fig.5(d)	$m=6$	$m=7$	$r=5, m\geq 5$	$h=6, m\geq 7$

$\#m$: the number of involved parties in total

$\#r$: the number of involved senior parties

the data set, which are CNN, RCNN, Fast RCNN and Faster RCNN models. The statistical data of testing results on the 4 models respectively in Table I. The tests on all 4 models are based on the same testing set, which includes 7814 images, and the number of total targets from the testing set is 29875. The number of correct detection, false detection and miss detection are listed in Table I, which proves the advantage of Faster RCNN model on target detection. The accuracy rates and the average detection times for one image also explain the high efficiency of Faster RCNN model.

Fig.5(d) shows one traffic image O and is segmented into $u=4$ regions O_1, O_2, O_3, O_4. Each region includes different content, and the importance levels satisfy: $Im_{(4)} > Im_{(3)} > Im_{(2)} > Im_{(1)}$. When constructing an image extraction scheme using proposed **Scheme 1** on O, the parameter k and n should satisfy $u=n-k+1$. Here we use $k=3, n=6$, thus a $(3,6)$ SIS is constructed on O_1, a $(4,6)$ SIS is constructed on O_2, a $(5,6)$ SIS is constructed on O_3 and a $(6,6)$ SIS is constructed on O_4. The shadows S_i is $S_i = v_{1,i}||v_{2,i}||v_{3,i}||v_{4,i}$, where the sub-shadow $v_{j,i}$ is generated from O_j. When extracting the image, any 3 parties can recover O_1, any 4 parties can recover O_1 and O_2, any 5 parties can recover O_1, O_2 and O_3, all 6 parties can recover the entire image $O = O_1 \cup O_2 \cup O_3 \cup O_4$. The region with higher importance level requires more parties for extraction. The results of image extraction from 3 to 5 parties are shown in Fig.5(a), Fig.5(b) and Fig.5(c) respectively.

The image extraction scheme using **Scheme 3** is also constructed on Fig.5(d). According to **Scheme 3**, the n parties are divided into n_s senior parties and $n-n_s$ junior parties, at least k parties in total which include at least t senior parties can extract partial information on O. The parameters should satisfy $u = n_s - t + 1$. Here we set that $t=2, n_s=5, k=4, n=7$. According to **Scheme 3**, $7 = n_s + k - t$ intermediate-shadows $W_1, W_2, \ldots, W_7$ are generated from O using $\boldsymbol{ShadowGe}^{PSIS}_{(k,n_s+k-t)}(O)$. Then sub-shadows $w_{6,1}, \ldots w_{6,7}$ are generated from W_6 using $\boldsymbol{ShadowGe}^{Thien-Lin}_{(4,7)}(W_6)$, sub-shadows $w_{7,1}, \ldots w_{7,7}$ are generated from W_7 using $\boldsymbol{ShadowGe}^{Thien-Lin}_{(4,7)}(W_7)$. The $n_s=5$ senior-shadows are $S_i^{senior} = W_i||w_{6,i}||w_{7,i}, i = 1,2,\ldots,5$, and the $n-n_s=2$ junior-shadows are $S_6^{junior} = w_{6,6}||w_{7,6}, S_7^{junior} = w_{6,7}||w_{7,7}$. During image extraction, a group of at least 4 shadows in total which includes 2 senior-shadows can extract O_1 (Fig.5(a)), a group of at least 4 shadows in total which includes 3 senior-shadows can extract O_1, O_2 (Fig.5(b)), a group of shadows which includes 4 senior-shadows can extract O_1, O_2, O_3 (Fig.5(c)), and a group a group of shadows which includes 5 senior-shadows can extract the entire image $O = O_1 \cup O_2 \cup O_3 \cup O_4$ (Fig.5(d)). More thresholds for image extraction using **Scheme 1** and **Scheme 3** are shown in Table II.

Fig.6 shows the image extraction results using proposed **Scheme 2**. The original image is shown in Fig.6(a), where 4 regions are segmented using Faster RCNN model with different importance levels. As shown in Fig.6(a), the licence plate is the most important information, and the second important information is the human face, then is the car and the other sky. Two experiments are executed. Fig.6(b-1)-Fig.6(b-3) are the extracted images from 3 to 5, where there are totally 6 parties; Fig.6(c-1)-Fig.6(c-4) are the extracted images from 5 to 8, where there are totally 9 parties. The detailed information proportions on each region from different amount of parties are shown in Table III. We can see that more parties can recover

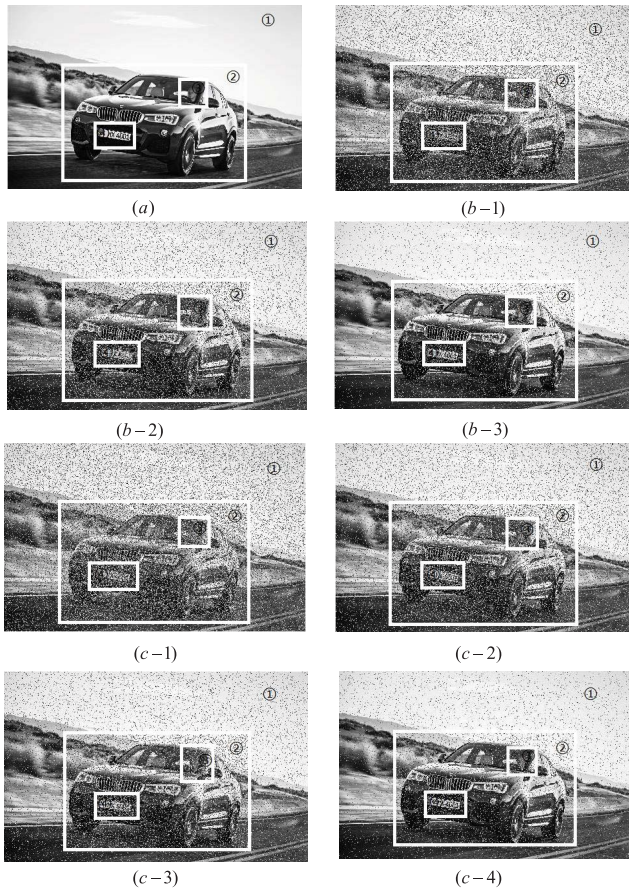

Fig. 6. Image extraction using proposed **Scheme 2**.

TABLE III
PROPORTIONS OF RECOVERED INFORMATION ON EACH REGION USING PROPOSED **SCHEME 2**

Total parties	Involved parties	Proportions on each region			
		O_1	O_2	O_3	O_4
6	3	80%	72%	60%	55%
	4	87%	79%	67%	60%
	5	95%	87%	80%	71%
9	5	75%	64%	58%	51%
	6	85%	74%	68%	61%
	7	90%	80%	72%	70%
	8	95%	90%	86%	82%

more information on each region, and same amount of parties can extract more clear information on the region with lower importance level.

V. CONCLUSION

Safely guarding sensitive images in intelligent traffic management is necessary. In this work, we construct thresholds based image extraction schemes for multiple paries in the traffic management. First the images from big data environment in intelligent management are segmented into multiple regions using Faster RCNN model, where each region has different importance level. Next three thresholds based image extraction schemes using PSIS were constructed on those segmented images, such that a group of parties with higher authorities can extract more information with higher importance level on the original image. The proposed schemes provide an effective way of protecting sensitive image among multiple parties, that can prevent the risk of information disclosure from single party in other systems. The corresponding theoretical analysis and experimental results show that Faster RCNN has high efficiency on image segmentation and the proposed image extraction schemes are also effective. The proposed methods provide a safe and intelligent way to extract images that can be used for further analysis in ITS.

REFERENCES

[1] S. Dang, M. Wen, S. Mumtaz, J. Li, and C. Li, "Enabling multi-carrier relay selection by sensing fusion and cascaded ANN for intelligent vehicular communications," *IEEE Sensors J.*, early access, Apr. 7, 2020, doi: 10.1109/JSEN.2020.2986322.

[2] B. Zhou *et al.*, "Performance limits of visible light-based positioning for Internet-of-vehicles: Time-domain localization cooperation gain," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–15, Feb. 25, 2020, doi: 10.1109/TITS.2020.2974929.

[3] K. Z. Ghafoor *et al.*, "Millimeter-wave communication for Internet of vehicles: Status, challenges and perspectives," *IEEE Internet Things J.*, early access, May 6, 2020, doi: 10.1109/JIOT.2020.2992449.

[4] F. Aghili and C.-Y. Su, "Robust relative navigation by integration of ICP and adaptive Kalman filter using laser scanner and IMU," *IEEE/ASME Trans. Mechatron*, vol. 21, no. 4, pp. 2015–2026, Aug. 2016.

[5] P.-W. Son, J. H. Rhee, and J. Seo, "Novel multichain-based loran positioning algorithm for resilient navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 666–679, Apr. 2018.

[6] W. Jiang, D. Liu, B. Cai, C. Rizos, J. Wang, and W. Shangguan, "A fault-tolerant tightly coupled GNSS/INS/OVS integration vehicle navigation system based on an FDP algorithm," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6365–6378, Jul. 2019.

[7] Y. Bi, X. Lu, Z. Sun, D. Srinivasan, and Z. Sun, "Optimal type-2 fuzzy system for arterial traffic signal control," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 9, pp. 3009–3027, Sep. 2018.

[8] Y. Han, A. Hegyi, Y. Yuan, C. Roncoli, and S. Hoogendoorn, "An extended linear quadratic model predictive control approach for multi-destination urban traffic networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3647–3660, Oct. 2019.

[9] S.-W. Kim *et al.*, "Autonomous campus mobility services using driverless taxi," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 12, pp. 3513–3526, Dec. 2017.

[10] L. Yu, D. Kong, X. Shao, and X. Yan, "A path planning and navigation control system design for driverless electric bus," *IEEE Access*, vol. 6, pp. 53960–53975, 2018.

[11] G. Zhou, V. Ambrosia, A. J. Gasiewski, and G. Bland, "Foreword to the special issue on unmanned airborne vehicle (UAV) sensing systems for Earth observations," *IEEE Trans. Geosci. Remote Sens.*, vol. 47, no. 3, pp. 687–689, Mar. 2009.

[12] X. Cao, C. Wu, J. Lan, P. Yan, and X. Li, "Vehicle detection and motion analysis in low-altitude airborne video under urban environment," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 10, pp. 1522–1533, Oct. 2011.

[13] J. Cui, J. Wen, S. Han, and H. Zhong, "Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3491–3498, Oct. 2018.

[14] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[15] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 950. Perugia, Italy: EUROCRYPT, 1995, pp. 1–12.

[16] C. C. Thien and J. C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, 2002.

[17] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 73, no. 3, pp. 405–414, Nov. 2004.

[18] C.-N. Yang, J.-F. Ouyang, and L. Harn, "Steganography and authentication in image sharing without parity bits," *Opt. Commun.*, vol. 285, no. 7, pp. 1725–1735, Apr. 2012.
[19] L. Yuan, M. Li, C. Guo, W. Hu, and X. Luo, "Secret image sharing scheme with threshold changeable capability," *Math. Problems Eng.*, vol. 2016, pp. 1–11, Jul. 2016.
[20] 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.
[21] 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.
[22] C. N. Yang and T. H. Chung, "A general multi-secret visual cryptography scheme," *Opt. Commun.*, vol. 283, no. 24, pp. 4949–4962, 2010.
[23] 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.
[24] R.-Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.
[25] 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.
[26] 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.
[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] 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, May 2010.
[29] 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, Oct. 2011.
[30] Y.-X. Liu, C.-N. Yang, and P.-H. Yeh, "Reducing shadow size in smooth scalable secret image sharing," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2237–2244, Dec. 2014.
[31] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2015, pp. 91–99.

Yanxiao Liu received the Ph.D. degree in cryptography from Xidian University, China, in 2012. He is currently working with the Department of Computer Science and Engineering, Xi'an University of Technology. His research interests include secret sharing scheme, secret image sharing, visual cryptography, and data hiding.

Chingnung Yang (Senior Member, IEEE) received the B.S. and M.S. degrees from the Department of Telecommunication Engineering, National Chiao Tung University, and the Ph.D. degree in electrical engineering from National Cheng Kung University. He has been serving with National Dong Hwa University since 1999. He has been a Visiting Professor with the University of Missouri Kansas City, University of Milan, and University of Tokyo. He is currently a Professor with the Department of Computer Science and Information Engineering. He has conducted extensive research on visual cryptography and secret image sharing, and is the Chief Scientist in both areas. He is also a fellow of IET (IEE).

Qindong Sun received the Ph.D. degree from the School of Electronic and Information Engineering, Xi'an Jiaotong University, China. He is currently a Professor with the Department of Computer Science and Engineering, Xi'an University of Technology. His research interests include network information security, online social networks, and the Internet of Things.