IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 26, 2018, accepted March 20, 2018, date of publication April 2, 2018, date of current version September 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2821690

New Secret Sharing Scheme Based on Faster R-CNNs Image Retrieval

JIANJUN LI[1], NING WANG[2], ZHI-HUI WANG[2], HAOJIE LI[2], CHIN-CHEN CHANG[3], (Fellow, IEEE), AND HONG WANG[2]

[1]School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China
[2]School of Software, Dalian University of Technology, Dalian 116023, China
[3]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan

Corresponding author: Zhi-Hui Wang (wangzhihui1017@gmail.com)

This work was supported by the Natural Science Foundation of China under Grant 61472058, Grant 61632019, and Grant 61771090.

ABSTRACT Secret image sharing has been attracting considerable research attention in recent years as images become ubiquitous on the Internet and mobile applications. In traditional (t, n) threshold secret image sharing schemes, the sender embeds the secret image into several shadow images and sends them to all participants. However, the shadow images are vulnerable during the transmission process on the Internet. In order to ensure the security of the shadow images which contain secret information, a new secret sharing scheme is proposed based on Faster region convolutional neural networks (Faster R-CNNs). This scheme uses a query image which does not have any secret information but looks similar to the original shadow image. Each participant retrieves the corresponding shadow image to search the query image in a big image database. As a result shadow images are searched by using Faster R-CNNs and stored in a database which is protected from being attacked, rather than transmitted over the network directly in the proposed scheme. The experimental results demonstrate that the proposed scheme can automatically retrieve the accurate shadow images by Faster R-CNNs and recover the secret image correctly.

INDEX TERMS Secret sharing, faster R-CNNs, steganography, image retrieval.

I. INTRODUCTION

Due to the rapid development of network technology and cloud storage technology, increasingly images are packed to cloud servers. How to utilize the aforementioned mass image data to facilitate the process of secret image sharing is quite a challenging problem.

In 1979, Shamir [1] and Blakley [2] introduced the first secret sharing scheme. In this scheme, the sender divided the secret into n shares so that each participant has one share. Among the n participants, only t or more participants can recover the secret by cooperating with each other. That is to say, less than t participants can not obtain any information about the secret. Subsequently, many advancements have been made based on this scheme. In 1995, Naor and Shamir [3] first introduced a new secret image sharing method based on a (t, n)-threshold scheme, called Visual Secret Sharing (VSS). In the VSS scheme, the secret image can be reconstructed by basically stacking t or more shadow images, which reduces computation complexity. However, when the shadow images are delivered on an insecure channel, they are more likely to attract the attention of a malicious attacker because the content is meaningless. Several works have attempted to solve the problem of distortion and authentication in secret sharing schemes. In 2004, a steganography technology was applied to generate meaningful shadow image with normal image(called a cover image) [4]. In this scheme, however, the revealed secret image is distorted slightly, which is unacceptable in some applications. In 2006, Poeprayk and Zhang [5] used a regular mapping approach for the construction of perfect secret sharings, and only the collection of participants belongs to the given access structure are able to recover the secret. In 2009, for the purpose of enhancing the quality of the shadow image and ensuring the authenticity of the shadow image simultaneously, Lin *et al.* [6] put forward a modulus operator to embed the secret data into the cover image. Nevertheless, the ability to embed secret information in their programs is lacking. In order to increase the maximum embedding capacity, a proactive secret sharing scheme without a public key system was proposed [7]. To avoid being deceived by participants and senders, each participant can authenticate the identities of all the other shares, using a structure

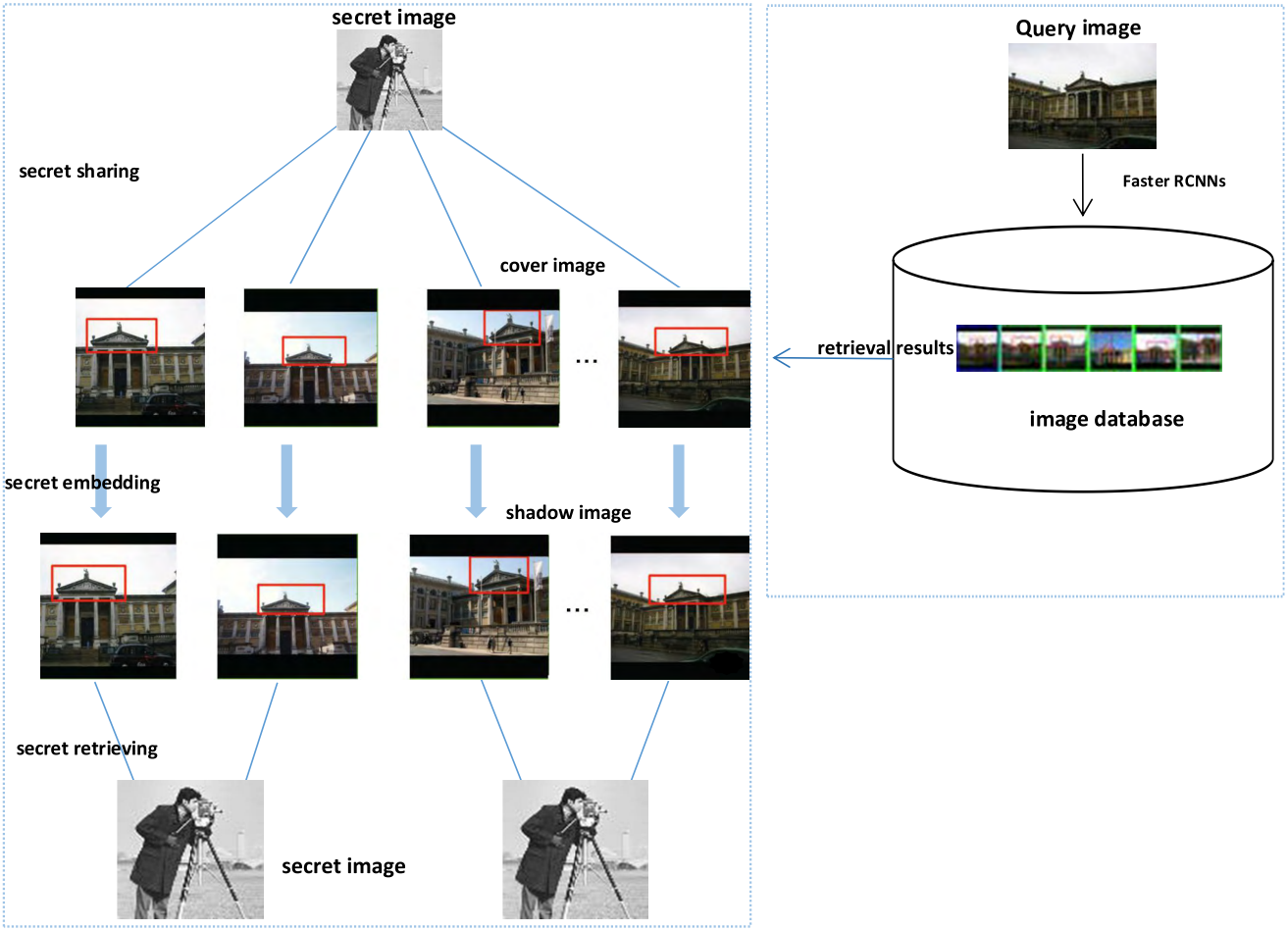

FIGURE 1. Our proposed framework consists of two parts: the first part is that the sender searches the public images database using the query image and then gets the order and the retrieval results. The second part is the normal secret retrieve process by several participants. Only t or more shadow images cooperate with each other to recover the secret image.

combined with the verifiable Liner Integer Secret Sharing (LISS) scheme. The program can achieve good performance with less time [8]. In 2011, **Khan *et al.* [9] proposed an image encryption process, called Fractional Fourier Transform (FRT), with scaling factors and random phase masks as the additional secret keys** . At the same time, a reversible secret image sharing scheme was proposed. The shadow image of this scheme had a high quality. Furthermore, this scheme losslessly recovered the secret image and cover images [10]. However, with the rapid growth of information needs, sometimes it is necessary to share more than one secret image at a time. Wang *et al.* [11] accomplished the task through an adaptable (n, n) secret image sharing mechanism based on boolean operation. **For the robustness of an image after being attacked, Horng *et al.* [12] proposed an adapticve semi-blind scheme.** In 2016, a secret image sharing method based on multi-participant authentication was proposed, and the authentication ability can be adaptively adjusted to the level of any participant authentication [13]. In 2017, in order to enhance the certification capability, a two-phase certification method has been demonstrated, which uses a combination of sub-keys and tamper-proofing methods [14].

Many steganographic methods [14], [16]–[20] have been proposed to produce meaningful shadow images that hide secret information. However, these shadow images are usually sent to the participants through the unsafe Internet and held by some specific persons without extra copies. Therefore, if shadow images are accidentally lost or intentionally attacked, the secret information will be unable to be recovered forever. Hence, putting forward a novel way to ensure the security of the shadow images is essential. We proposed a novel method that utilizes images stored in databases based on LISS. In all aforementioned secret sharing schemes, it is necessary for the sender to send a shadow to the receiver. However, in our scheme, we transport a query image which not contains secret information to all participants. A participant could retrieve the corresponding shadow image from a big database by using the query image. We divided the overall proposed framework into three parts as shown in Fig.1, the specific flow of the flow chart is described in detail as shown in the proposed framework. Our procedure

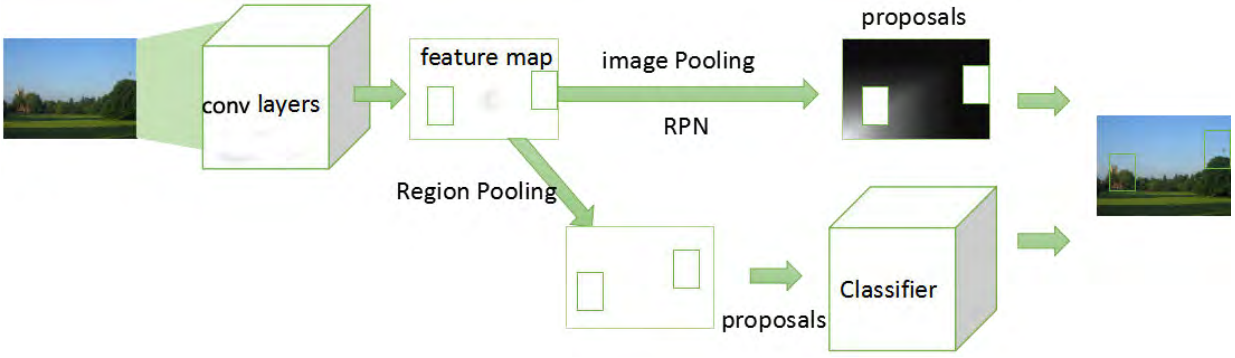

FIGURE 2. The overall schematic of the Faster R-CNNs' architecture for instance retrieval. Based on VGG16 and ZF [15], this architecture extracts whole image and instance region (green boxs) features.

can avoid exposing the shadow image on the Internet because we stored shadow images in the database.

The retrieval algorithm adopted here is Faster R-CNNs. Faster R-CNNs offer an opportunity for image retrieval and region-wise representations pooled from object detection CNN [15], [21]–[23]. Compared with other detection methods, the running time for this proposal is just 10 milliseconds while retaining a frame rate of 5 fps on a GPU.

The main contributions of this work are summarized as follows:

- We propose a novel secret sharing scheme that utilizes the representation capability of deep learning.
- We only need to send a query image rather than all shadow images to all participants, thus reducing the risk and the load on network communications.
- A novel approach is put forward to ensure security and specificity for shadow images. The sender is the owner of a database with more than ten thousand images. If any cheating events occurred, the sender could replace the shadow images in the database immediately. The security of the secret image is further improved. Since the search results may change according to the change of the database content, the sender can also use this feature to update the query image to enhance the security in real time.

The remainder of the paper is structured as follows. Section 2 introduces related works, Section 3 presents the methodology of this paper, including the overall framework of the scheme, the encryption process, image retrieval, and secret sharing procedure. Section 4 includes experiments on the database. Finally, Section 5 draws the conclusions of this work.

II. RELATED WORK

A. AN INTEGER SPAN PROGRAM FOR BUILDING A LINEAR INTEGER SECRET SHARING SCHEME

There are two definitions from an integer span program (ISP) for building a LISS scheme.

Definition 1: Given a monotone span scheme $M \in \mathbb{Z}^{h\times v}$, a complete mapping function Υ which is represented as $\{1,\ldots,h\} \rightarrow \{1,\ldots,n\}$, where h is the total rows of M, n is the number of participants, a non-zero target vector ξ expressed as $\xi = (1,0,\ldots,0)^{\mathrm{T}} \in \mathbb{Z}^{v}$. After obtaining M with respect to Υ and ξ, integer span program $\mathcal{M}$ can be created by $\mathcal{M} = (M, \Upsilon, \xi)$ [24].

Definition 2: We assume an integer span program $\mathcal{M} = (M, \Upsilon, \xi)$ and an access structure Γ. M_A is a matrix depend on Γ that retains participants who can recover confidential information. There are two situations shown below:

If the set of participants A belongs to the access structure Γ, there exists a goal vector $\lambda \in Z^h$ satisfying $M_A^{\mathrm{T}}\lambda = \xi$. Otherwise, there exists a vector $k = (k_1,\ldots,k_e)^{\mathrm{T}} \in Z^e$ such that $M_A^{\mathrm{T}}k = 0 \in Z^h$ with $k_1 = 1$.

Then the linear integer secret sharing scheme is constructed by ISP that was proposed by Damgard and Thorbek [25].

The participants set A belongs to the access structure Γ. In order to safely share the secret s, a sharing vector was constructed as $\theta = (s, \theta_2, \ldots, \theta_e)^{\mathrm{T}}$, where s represents the value of the secret, θ is a set of random numbers, $\theta \in [0 \ldots 2^{c+k}]$ where c is constant integer, k is an adjustable parameter. After obtaining θ, the secret s can be divided and embedded into cover images. $M \cdot \theta = (s_1, \ldots, s_d)$, where s_d represents the secret shared with the d-th participant.

According to **Definition 2**, $M_A^{\mathrm{T}}\lambda_A = \xi$. If A is a valid subset of an access structure Γ, then the secret can be rebuilt by ISP. The goal is to make $s_A^{\mathrm{T}}\lambda_A = s$, where $s_A^{\mathrm{T}} = (s_1,\ldots,s_d)^{\mathrm{T}}$. Subsequently, using the equation of $s_A^{\mathrm{T}}\lambda_A = (M_A \cdot \theta)^{\mathrm{T}}\lambda_A = \theta^T \cdot (M_A^{\mathrm{T}} \cdot \lambda_A) = \theta^T \cdot \varepsilon = s$ to reconstruct the secret s , where the value of $M_A \cdot \theta$ is the encrypted secret obtained by the process of secret sharing.

B. FASTER R-CNNS

This section introduces Faster R-CNNs for image retrieval. In this scheme, Faster-RNNs is used to retrieve images from a database that contains the query image. The overall architecture of the Faster R-CNNs is shown in Fig.2.

A query image is input into the Faster R-CNNs for instance retrieval at the beginning. For the sake of extracting the whole images' and the instances' features, Faster R-CNNs takes advantage of image-wise pooling of activations (IPA) of the

query image and database images, then sorts the database images by calculating the cosine distance with the query image and gets top-n images. Cosine similarity is described below:

$$sim(D_1, D_2) = cos < D_1, D_2 > = \frac{\sum_{k=1}^{n} p_k(D_1) \times p_k(D_2)}{\sqrt{(\sum_{k=1}^{n} p_k^2(D_1)) \times (\sum_{k=1}^{n} p_k^2(D_2))}} \quad (1)$$

After a simple filtering, the most important aspect is getting proposals which includes objects. Same with fully convolutional networks (FCN) [26], generating m feature maps whose size is $N \times N$ from the last convolutional layer. For each image, 300 proposals are produced with a region proposal network (RPN). Faster R-CNNs implements a region pooling layer that extracts the convolutional activations for each of the object proposals learned by RPN, which are noted as region-wise pooling of activations (RPA). In addition, for every image in the top-n images, the RPA for all RPN proposals is compared to the region descriptors of the query bounding box. Finally, after feature matching, Faster R-CNNs chooses the top-k images' descriptors on average as a new query vector, re-querying the top-n results in the database and obtaining the final images which contain the same objects.

Faster R-CNNs originated in Region-based Convolutional Networks (R-CNN) [23] and Fast Region-based Convolutional Networks (Fast R-CNNs) [22]. R-CNNs was first proposed to localize and segment objects. The highlight of R-CNNs is to deal with computer vision tasks and it applied the way of high-capacity convolutional neural networks to bottom-up region proposals. Repeated extraction proposals actually lead to repetitive calculations in the detection task. In the Fast R-CNNs, a bounding box can be extracted by mapping proposal region to the feature map in the last layer of FCNs directly. Fast R-CNNs reduces the time of proposals extraction, nonetheless the imprecision of bounding box and the redundancy of region proposal extraction increases computation complexity. Faster R-CNNs has the benefits of both the RPN and Fast R-CNNs, it can be simultaneously learned their methods as prominent object proposals and their associated class probabilities. The accuracy of the proposal and detection execution speed have been greatly improved in Faster R-CNNs [15]. Based on Faster R-CNNs, salvador using image-wise pooling of activations (IPA) with region-wise pooling of activations (RPA) construct descriptors for instance search [21]. Fig.3 shows the result of Faster R-CNNs for instance retrieval.

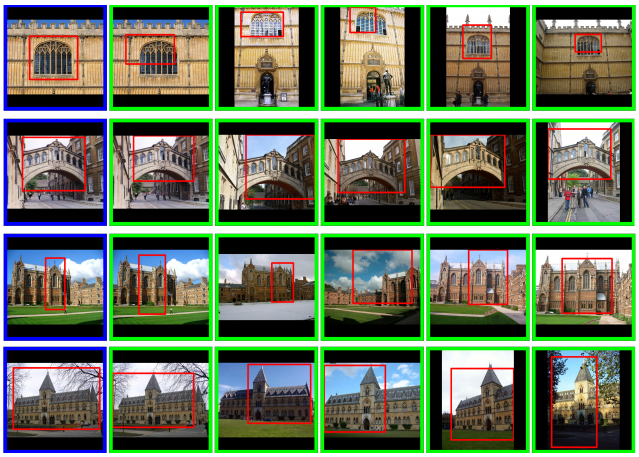

FIGURE 3. Examples of rankings and object locations obtained with Faster R-CNNs retrieval system.

III. THE PROPOSED FRAMEWORK

In subsection *A*, we describe the process of the secret image sharing method in detail. Subsection *B* shows the method of recovering original secret image by retrieving the corresponding shares with the query image. Finally, we introduce the cover images retrieval and Re-Verification for Retrieval(RVR) in subsection *C*. The entire structure of the program is shown in Fig.1, and it contains the following steps:

Step 1: The sender selects an image C from image database randomly. The selected image is taken as image which is conveyed to n participants.

Step 2: The query image is used to retrieve top-n cover images in the database through a Faster R-CNNs' retrieval network.

Step 3: Share secret s with the cover images based on LISS and eventually get n shares.

Step 4: Using RVR to verify if the order of retrieval results is consistent with the order of the shares.

Step 5: The sender records the order of shares in verification phase(RVR) $t_i = (1, \ldots, l)$, $i \epsilon n$, l is a constant determined by the sender.

Step 6: The sender encrypts the query image and order t_i with the AES encryption algorithm, then they are sent to the corresponding participant.

Step 7: Each participant feeds the query image into Faster R-CNNs, according to the homologous order to search their shares.

Step 8: t or more participants can restore the secret information.

A. SECRET IMAGE SHARING PROCEDURE

In this section, the LISS scheme with combinatorial structure is introduced, which not only reduces the time consumption, but also increases the information storage capacity. In our secret image sharing procedure, we utilize Ma's scheme to generate secret values [8] as shown in Fig.4.

At the begining, the sender selects the secret image, and an image pixel of the secret image is transformed into l-column. l is the prime selected by the sender [8].

The participants are noted as $P = \{1, \ldots, n\}$ and the sender is recorded as S. Γ demonstrates which combination of the participants can restore the original secret image.

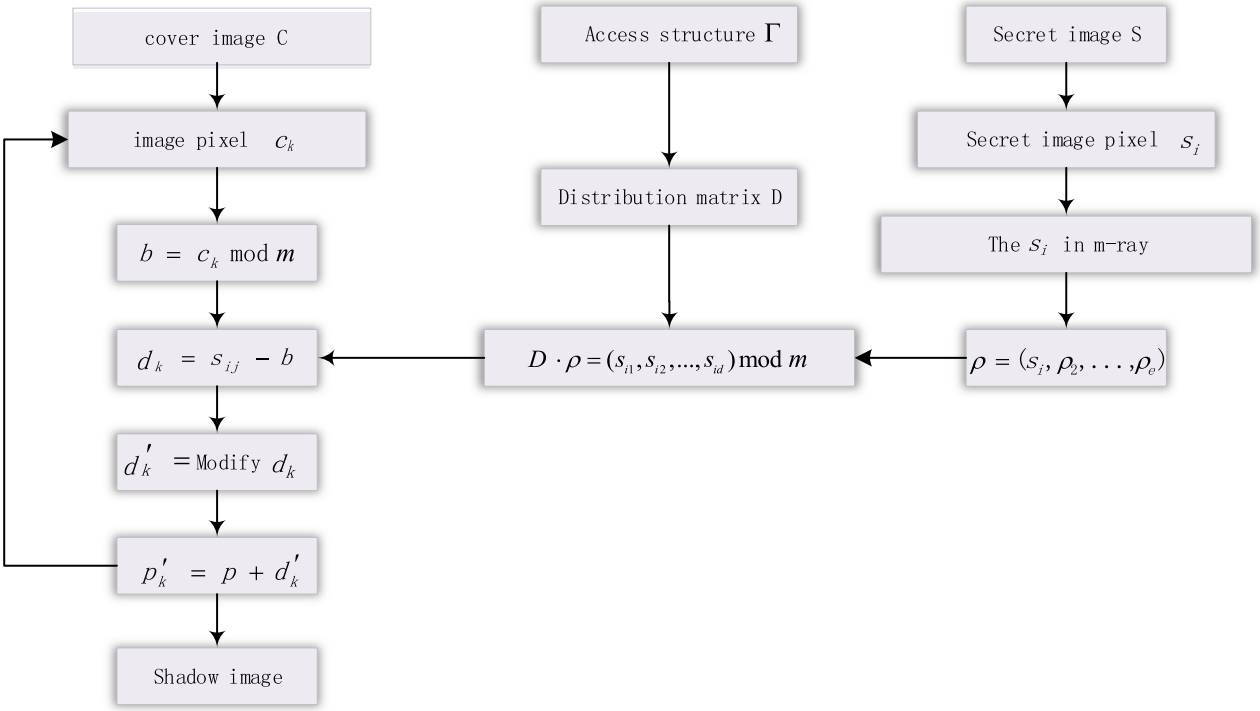

FIGURE 4. Representation of the entire secret sharing process.

The distribution matrix D and the reconstruction vector λ are determined by the sender.

In the LISS algorithm, the distribution vector $\rho = (s, \rho_2, \ldots, \rho_e)$, where ρ_i is a random integer selected from $[0, \ldots, 2^n]$, $n = (l_0 + k)$, l_0 and k are parameters chosen by sender, s is the original secret. Then, shares are calculated by $D \bullet \rho = (s_{i1}, \ldots, s_{id})$, where d is the number of participants. More details are given in the following steps:

Step 1: For every pixel c_k in the cover image $b = c_k \bmod m$, where $k = \{1, \ldots, D_c \times N_c\}$

Step 2: $d_k = s_{ij} - b$, s_{ij} is obtained by $M \cdot \rho$, where $i = \{1, \ldots, \log_m 255\}$ and $j = \{1, \ldots, d\}$.

Step 3: Modify d_k according to the relationship between m and d_k.

$$d_k' = \begin{cases} d_k & \text{if } (-\lfloor \frac{m-1}{2} \rfloor) \le d_k \le \lceil \frac{m-1}{2} \rceil; \\ d_k + m & \text{if } (-m+1) \le d_k \le -\lceil \frac{m-1}{2} \rceil; \\ d_k - m & \text{if } (-\lfloor \frac{m-1}{2} \rfloor \le d_k \le m). \end{cases} \quad (2)$$

Step 4: $p_k' = c_k + d_k$, modify the cover image pixel at the first time.

Step 5: Adjust the pixel value as Equation(3) to prevent overflow.

$$p_k' = \begin{cases} p_k' + m & \text{if } p_k' < 0; \\ p_k' - m & \text{if } p_k' > 255. \end{cases} \quad (3)$$

Step 6: Repeat above steps until all the secret values are embedded.

Example 1: For convenience, assume there is a (2, 4) threshold system in which $P = \{P_1, P_2, P_3, P_4\}$, the access structure is $\Gamma = \{P_1, P_2\}, \{P_3, P_4\}$. The distribution matrix and reconstruction vector were designed as follow:

$$D = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \lambda_A = \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \quad \lambda_b = \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix}. \quad (4)$$

Let prime $m = 11$ and the first pixel of secret image $S_1 = 189$, convert it to 11 hexadecima $s_1 = \{1, 6, 2\}_{11}$. Choose a random vector $\rho = (1, 4, 7)^{\mathrm{T}}$ for $s_1 = 1$. According to the step 2, $D \cdot \rho = (s_{i1}, \ldots, s_{id})$, s_1 can be expressed as $\{5, 4, 8, 7\}^{\mathrm{T}}$. Hide $s_{11} = 5$ in a corresponding cover image. Assume the first pixel of cover image $c_k = 168$, use $b = c_k \bmod m$ and $d_k = s_{11} - b$, then gets $b = 3$, $d_k = 2$. Update d_k to $d_k' = d_k = 2$, p_k' is the share value generated as $p_k' = c_k + d_k = 170$. In line with the similarity calculation phase above, each pixel value in the cover images is changed to a new value in the share image.

B. SECRET IMAGE RETRIEVING PHASE

This section describes the process of secret image recovery, a group of participants work together to calculate the original secret image. The process is as follows:

Step 1: Every shadow image's pixel p'_k and prime m are known, so s_{ij} is obtained by Equation (5).

$$\begin{aligned} p'_k \bmod m &= (p'_k + d'_k + mn) \bmod m \\ &= (b + s_{ij} - b + nm) \bmod m \\ &= s_{ij} \end{aligned} \tag{5}$$

Step 2: After receiving N data $(s_{i1}, \ldots, s_{ni})^T$, select a suitable subset of $s_A = s_{ij}$ to calculate s_i.

$$\begin{aligned} s_A^{\mathrm{T}} &= (M \cdot \rho)^{\mathrm{T}} \cdot \lambda_A \\ &= \rho^{\mathrm{T}} \cdot (M^{\mathrm{T}} \cdot \lambda_A) \\ &= \rho^{\mathrm{T}} \cdot \varepsilon \\ &= s_i \bmod m \end{aligned} \tag{6}$$

Example 2: According to Example 1, $p'_k = 170$, $p'_k \bmod m = s_{ij}$ so that $170 \bmod 11 = 5$, then verify that s_{ij} is correct or not.

C. COVER IMAGE AUTOMATIC RETRIEVAL AND VALIDATION

In order to achieve an automatic and quick retrieval of the shadow images, we make use of instance retrieval network Faster R-CNNs.

Common instance search systems often combine fast first filtering stages, in which all database images are ranked according to their similarity with the image query. Geometric verification and spatial analysis are common reranking strategies, which are often followed with query expansion [27]. Given a query image, the system returns a ranked list of images from database according to cosine similarity.

For every image in the top-n, Faster-RCNNs **uses** the region-wise descriptions to retrieve the location of the target in query image, region proposals are the bounding box descriptors obtained by Region Proposal Network (RPN). An image of any size is input and the output is a set of rectangular object proposals. The similarity between all proposals in an image and query is treated as the simiarity between image and query[17]. Faster-RCNNs' query expansion uses averaged top-n results as a new query for the sake of searching accurately. Inspired by Faster-RCNNs, Re-Verification for Retrieval(RVR) averages the shadow images as a new query, feed the new query into the network and retrieve the final results. Then we can get the final order which search the shadow image exactly. In RVR, in order to ensure that the shadow image still can be retrieved, RVR only uses the grayscale image to hide the secret. In addition, we record the order of the RVR results and transfer the order to the corresponding participant.

For example, the sender uses the query image K to retrieve 10 shadow images by Faster R-CNNs, then averages these images to form a new query image N, and uses N as a new query to feed into Faster R-CNNs. In the current example, we use K to retrieve and then record the location where S appears as shown in Fig.5. Assuming that a set of shadow images $S = \{1, 4, 3, 2\}$, send the key and the corresponding sequence to the participants. The participant accepted $R = \{K + 1, K + 4, K + 3, K + 2\}$, where $K + 1$ includes the key image and given order. Every participant uses the key to obtain corresponding results.

IV. EXPERMENT

A. COMPARISON WITH OTHER SECRET SHARING SCHEME

We compare various traditional secret sharing scheme with our scheme, the results are shown in Table I. **Recently, some works achieve competitive results, so we also conduct experiments to evaluate the performance of our scheme, as shown in Table II. Yang ascribes storage or transmission inefficiency to large shadows. Chen presents a multi-secret image sharing scheme to share different sized secret image.** In our scheme, searching the shadow images instead of transmitting the shadow images directly could reduce the load on network communications. The sender is the owner of the database that usually contains more than ten-thousand images. **We can retrieve a lot of images each time, therefore we can share different sized multi-secret images by transmitting in multi-order. For example, every participant gets three numbers as his order, the first numbers of all participants can retrieve a secret image.** A Big database ensures the shadow image's security by enhancing the perplexity of the shadow images for attackers. Thus, we transfer the security in transmit process to the storage process. In addition, the sender can replace the shadow images in the database immediately if the system is compromised. In our experiments, the database we selected is composed of images from Oxford Buildings which contained 5,063 images, including 55 query images of 11 different buildings [28] and another 6,412 still images of Paris landmarks, including 55 query images of 11 building in Paris Buildings [29]. **In our experiment, the database contains 11475 images, which includes Oxford Buildings and Paris landmarks. The contents in image are intricate and the**

TABLE 1. Comparison between our scheme with the traditional schemes [1], [4], [11], [14].

Scheme	Traditional Secret Sharing Scheme	our method
Find Cover Image Automatically	Manual	Automatic
The Way of Ensure Shadow's Safety	Transmission security	Storage security
Public Database	privacy	public
The size of the database	small	huge

TABLE 2. Comparison between our scheme with Chen's [30] and Yang's [31] recent works..

Scheme	Recent Secret Sharing Scheme	our method
Different sized secret images :	yes	yes
The size of shadow images:	small	arbitrary
The number of shadow images:	large	arbitrary
Public Database	privacy	public

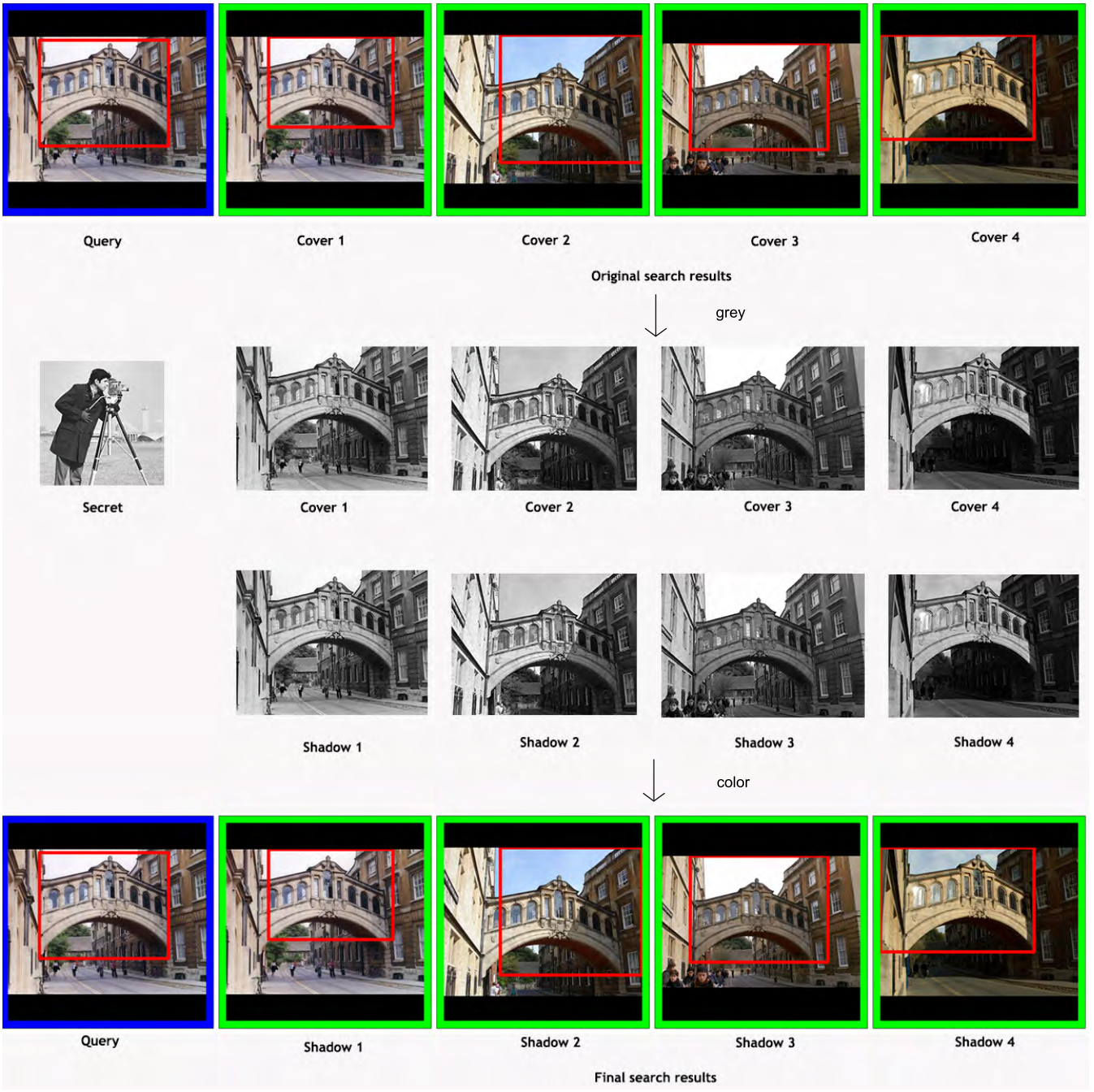

FIGURE 5. First line is original search results using Faster R-CNNs. Second line includes secret image and the greyscale cover images. Third line is shadow images containing secret. The last line is colorizing shadow images which added original color space of a and b in Lab(Lab color space). The input cameraman image is the secret that we shared. As shown: (a) Secret image size is 256 × 256 pixels. (b) The top-4 search results images and the size of all the images are different, in most cases, the size is 1024 × 768 pixels.

resolution of these images are different. Most of the image size is 1024×768**, so that different secret images can be embedded in the cover image. When the resolution of query image is very large or very small, it will undoubtedly affect the bandwidth, but it has no affect on other parts of our algorithm. Since we adopt Faster RCNNs for retrieval, we still get rightful sequences by RVR for query image in any size.**

B. EXPERIMENTAL RESULTS

In our experiments, a secret image is shared by four participants $P1, P2, P3$ and $P4$. Any two of them can reconstruct the original secret image. Let prime $l = 7$. The evaluation results of the Mean Square Error(MSE), Structural Similarity (SSIM), Peak Signal to Noise Ratio (PSNR) between shadow images and cover image are shown in Fig.7. From the visual point of view, as shown in the Fig.8. Faster R-CNNs retrieves

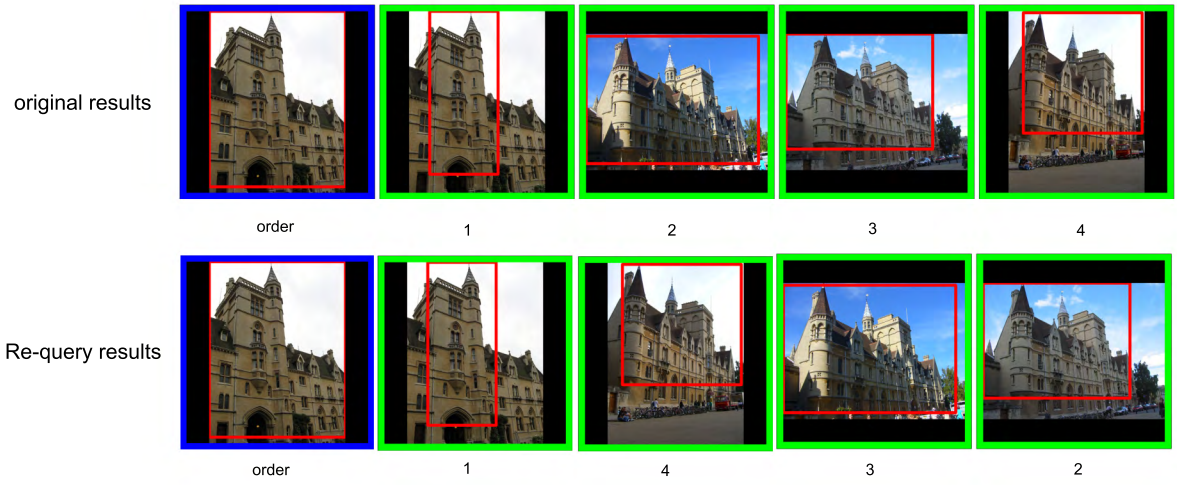

FIGURE 6. Examples of original images without secrets (top) and shadow images (bottom). The order for retrieval results have changed slightly, but the shadow image still can be retrieved correctly using the participant received sequence.

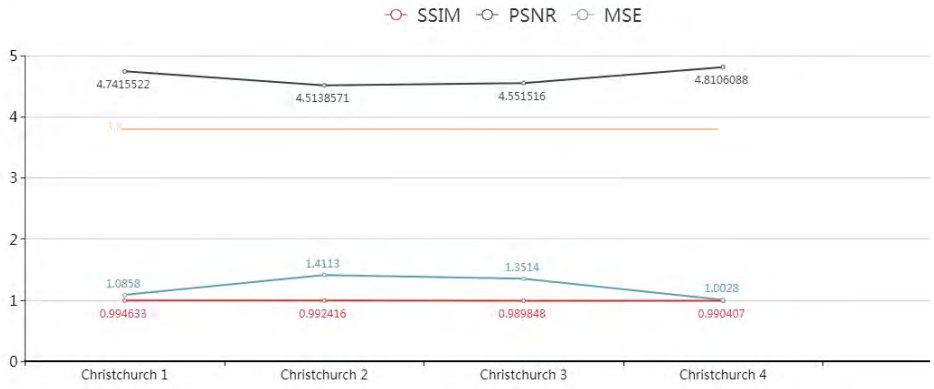

FIGURE 7. From the figure above, shadow images and cover images can not be visually distinguished.

four cover images using a query image, then we can get meaningful shadow images after embedding the secret. In terms of visual perception, four shadow images have good visual quality, since the human vision system can not tell any difference when the PSNR value is greater than 40dB. **We prove that attacker can not identify the real covers and the synthesis shadows visually. Only one share was intercepted has not important affects on robustness in our scheme, since the distribution matrix D and the reconstruction vector λ_A are determined by the sender. The distribution vector $\rho = (s, \rho_2, \ldots, \rho_e)$, and the shares calculated by $D \bullet \rho = (s_{i1}, \ldots, s_{id})$ as demonstrated in part III.**

In addition, we choose another eleven sets for experiments, each set of experiments contains four cover images and corresponding shares. The average MSE, SSIM, PSNR evaluation result for shares and cover images are shown in Fig.9. Fig.9 demonstrates that the average MSE values are around 1, the SSIM values are around 1, the PSNR values are between 45dB and 48dB, indicating that the quality of the shares generated is satisfactory.

For the purpose of evaluating system performance, we choose several different resolution secret images to check out the efficiency in secret sharing and recovery process. We divide the experiment into two sections, specially, by denoting S as the storage of our secret sharing, T as the embedding and recovery

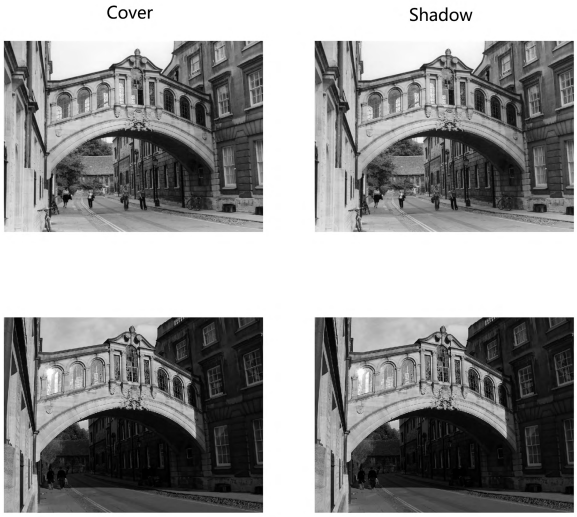

FIGURE 8. Hiding capacity evaluation in our scheme. The MSE's and the SSIM's range from 1 to 2, for the visual distinction, we add the normal visual base line in orange and set the value PSNR/10.

FIGURE 9. Three different evaluation Criterias MSE, SSIM, PSNR between a sets of cover images and corresponding shares, each set of experiment contains four cover images and corresponding shares.

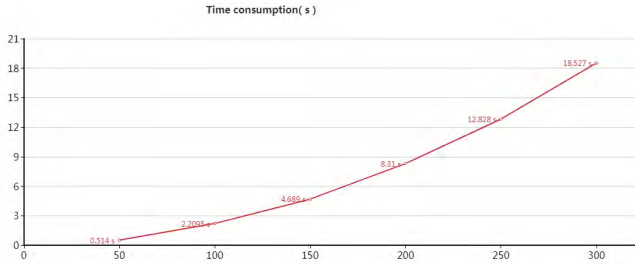

FIGURE 10. This chart lists the computation time required in different size secrets. The abscissa represents the secret image size, and the ordinate counts the time of embedding and restoring for different secrets size.

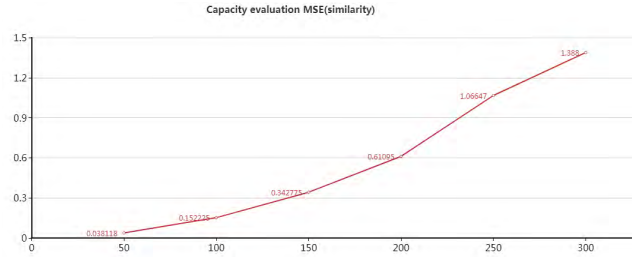

FIGURE 11. The relationship between secret image size and MSE.

time costs. We summarize that different size secrets have important influence in system performance T as shown in Fig.11. Our scheme only costs less than 2.5 seconds to share or recover a 100×100 pixels secret image with four participants. In term of storage capacity, with the secret image size increase, the embedding performance is linear declining, as shown in Fig.12. The capacity of our scheme is $M \times N / log_m 255$, where $M \times N$ is the size of cover image.

V. CONCLUSIONS

In this paper, we propose a new secret sharing scheme based on Faster R-CNNs that takes advantage of a big database. Our proposed method facilitates the security of the shadow images because the attacker does not know the shares position in the database. In addition to that, shadow images are queried by participants, if one of the shares is accidentally lost or intentionally attacked, the sender can replace the shadow images in the database immediately. Furthermore, it is only necessary to send a key image to the participants rather than all shares, as a consequence, a reduction in the network transmission overhead. However, this algorithm is still fragile because malicious invasion may cause errors in the first step of our scheme. Using a more secure method of delivering the query image and order should be investigated and is left for future research.

REFERENCES

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Comput. Conf.*, 1979, p. 313–317.

[3] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," in *Proc. Int. Workshop Secur. Protocols*, Cambridge, U.K., Apr. 1996, pp. 197–202.

[4] 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./Dec. 2004, doi: 10.1016/S0164-1212(03)00239-5.

[5] J. Pieprzyk and X. Zhang, "Ideal secret sharing schemes from permutations," *Int. J. Netw. Secur.*, vol. 2, no. 3, pp. 238–244, 2006. [Online]. Available: http://ijns.femto.com.tw/contents/ijns-v2-n3/ijns-2006-v2-n3-p238-244.pdf

[6] P. Lin, J. Lee, and C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognit.*, vol. 42, no. 5, pp. 886–895, 2009, doi: 10.1016/j.patcog.2008.09.014.

[7] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Invertible secret image sharing for gray level and dithered cover images," *J. Syst. Softw.*, vol. 86, no. 2, pp. 485–500, 2013, doi: 10.1016/j.jss.2012.09.027.

[8] C. Ma and X. Ding, "Proactive verifiable linear integer secret sharing scheme," in *Proc. 11th Int. Conf. Inf. Commun. Secur. (ICICS)*, Beijing, China, Dec. 2009, pp. 439–448, doi: 10.1007/978-3-642-11145-7_34.

[9] M. K. Khan, J. Zhang, and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification," *Future Gener. Comp. Syst.*, vol. 27, no. 4, pp. 411–418, 2011, doi: 10.1016/j.future.2010.05.019.

[10] Y.-Y. Lin and R.-Z. Wang, "Improved invertible secret image sharing with steganography," in *Proc. 7th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Dalian, China, Oct. 2011, pp. 93–96, doi: 10.1109/IIHMSP.2011.58.

[11] Z.-H. Wang, H. Jin, X. Wang, and C.-C. Chang, "An adaptable (n, n) secret image sharing mechanism based on Boolean operation," *Int. J. Netw. Secur.*, vol. 16, no. 6, pp. 487–493, 2014. [Online]. Available: http://ijns.femto.com.tw/contents/ijns-v16-n6/ijns-2014-v16-n6-p487-493.pdf

[12] S.-J. Horng, D. Rosiyadi, P. Fan, X. Wang, and M. K. Khan, "An adaptive watermarking scheme for E-government document images," *Multimedia Tools Appl.*, vol. 72, no. 3, pp. 3085–3103, 2014, doi: 10.1007/s11042-013-1579-5.

[13] J. Zarepour-Ahmadabadi, M. S. Ahmadabadi, and A. Latif, "An adaptive secret image sharing with a new bitwise steganographic property," *Inf. Sci.*, vol. 369, pp. 467–480, Nov. 2016, doi: 10.1016/j.ins.2016.07.001.

[14] L. Liu, A. Wang, C. C. Chang, and Z. Li, "A secret image sharing with deep-steganography and two-stage authentication based on matrix encoding," *Int. J. Netw. Secur.*, vol. 19, no. 3, pp. 327–334, 2017. [Online]. Available: http://ijns.femto.com.tw/contents/ijns-v19-n3/ijns-2017-v19-n3-p327-334.pdf

[15] A. Salvador, X. Giró-i-Nieto, F. Marqués, and S. Satoh, "Faster R-CNN features for instance search," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPR)*, Las Vegas, NV, USA, Jun. /Jul. 2016, pp. 9–16, doi: 10.1109/CVPRW.2016.56.

[16] J. Daemen and V. Rijmen, *The Design of Rijndael AES—The Advanced Encryption Standard* (Information Security and Cryptography). Berlin, Germany: Springer-Verlag, 2002, doi: 10.1007/978-3-662-04722-4.

[17] D. Qin and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2693–2705, Dec. 2016, doi: 10.1109/TIFS.2016.2594143.

[18] L. Pang, D. Miao, and C. Lian, "User-friendly random-grid-based visual secret sharing for general access structures," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 966–976, 2016, doi: 10.1002/sec.1392.

[19] 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, 2016, doi: 10.1002/sec.1589.

[20] V. P. Binu, D. G. Nair, and A. Sreekumar. (Feb. 2016). "Secret sharing homomorphism and secure E-voting." [Online]. Available: https://arxiv.org/abs/1602.05372

[21] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017, doi: 10.1109/TPAMI.2016.2577031.

[22] R. Girshick, "Fast R-CNN," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Santiago, Chile, Dec. 2015, pp. 1440–1448, doi: 10.1109/ICCV.2015.169.

[23] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Columbus, OH, USA, Jun. 2014, pp. 580–587, doi: 10.1109/CVPR.2014.81.

[24] Q. Chen, D. Pei, C. Tang, and G. Zhao, "Efficient integer span program for hierarchical threshold access structure," *Inf. Process. Lett.*, vol. 113, no. 17, pp. 621–627, 2013, doi: 10.1016/j.ipl.2013.05.009.

[25] M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds., *Public Key Cryptography—PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings* (Lecture Notes in Computer Science), vol. 3958. Springer, 2006, doi: 10.1007/11745853.

[26] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Boston, MA, USA, Jun. 2015, pp. 3431–3440, doi: 10.1109/CVPR.2015.7298965.

[27] R. Arandjelović and A. Zisserman, "Three things everyone should know to improve object retrieval," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Providence, RI, USA, Jun. 2012, pp. 2911–2918, doi: 10.1109/CVPR.2012.6248018.

[28] J. Philbin, O. Chum, M. Isard, J. Sivic, and A. Zisserman, "Object retrieval with large vocabularies and fast spatial matching," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Minneapolis, MN, USA, Jun. 2007, pp. 1–8, doi: 10.1109/CVPR.2007.383172.

[29] J. Philbin, O. Chum, M. Isard, J. Sivic, and A. Zisserman, "Lost in quantization: Improving particular object retrieval in large scale image databases," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Anchorage, AK, USA, Jun. 2008, pp. 1–8, doi: 10.1109/CVPR.2008.4587635.

[30] C.-C. Chen and J.-L. Chen, "A new Boolean-based multiple secret image sharing scheme to share different sized secret images," *J. Inf. Sec. Appl.*, vol. 33, pp. 45–54, Apr. 2017, doi: 10.1016/j.jisa.2017.01.006.

[31] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach," *Signal Process. Image Commun.*, vol. 31, pp. 1–9, Feb. 2015, doi: 10.1016/j.image.2014.11.003.

JIANJUN LI received the B.S. degree in information engineering from the Xi'an University of Electronic Science and Technology, Xi'an, China, and the M.S. degree in electrical and computer from The University of Western Ontario, and the Ph.D. degree in electrical and computer from the University of Windsor, Canada. He is currently a Chair Professor with Hangzhou Dianzi University. His research interests include micro-electronics, audio, video, and image processing algorithms and implementation.

NING WANG received the degree from the Hebei University of Technology. She is currently pursuing the degree with the School of Software Technology, Dalian University of Technology. Her current research interests are in image processing and object retrieval.

ZHI-HUI WANG received the B.S. degree in software engineering from North Eastern University, Shenyang, China, in 2004, and the M.S. degree in software engineering and the Ph.D. degree in software and theory of computer from the Dalian University of Technology, Dalian, China, in 2007and 2010, respectively. Since 2011, she has been a Visiting Scholar with the University of Washington. Her current research interests include information hiding and image compression.

HAOJIE LI received the B.E. degree from Nankai University, Tianjin, in 1996, and Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, in 2007. From 2007 to 2009, he was a Research Fellow of the School of Computing, National University of Singapore. He is currently a Professor with the School of Software, Dalian University of Technology. He has co-authored over 50 journal and conference papers in his research areas, including IEEE TCSVT, TMM, TIP, ACM Multimedia, and ACM ICMR. His research interests include social media computing and multimedia information retrieval. He is a member of the ACM.

CHIN-CHEN CHANG (M'88–SM'92–F'99) received the B.S. degree in applied mathematics and the M.S. degree in computer and decision sciences from National Tsing Hua University, and the Ph.D. degree in computer engineering from National Chiao Tung University. He was with National Chung Cheng University from 1989 to 2005. Since 2005, he has been a Chair Professor with the Department of Information Engineering and Computer Science, Feng Chia University. He is a fellow of the IEE, U.K. His research interests include database design, computer cryptography, image compression, and data structures.

HONG WANG received the degree in electronic and information engineering from the Dalian University of Technology in 2016, where she is currently pursuing the degree with the School of Software Technology. Her current research interests are in image processing and object retrieval.