IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 20, 2019, accepted November 21, 2019, date of publication November 26, 2019,
date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2955990

Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment

ZHILI ZHOU[1], (Member, IEEE), YI CAO[1], MEIMIN WANG[1], ENMING FAN[1], AND Q. M. JONATHAN WU[2], (Senior Member, IEEE)

[1]Jiangsu Engineering Center of Network Monitoring, School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2]Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada

Corresponding author: Zhili Zhou (zhou_zhili@163.com)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1003205, in part by the National Natural Science Foundation of China under Grant 61972205, Grant 61602253, Grant U1836208, Grant U1536206, Grant U1836110, and Grant 61672294, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) Fund, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund, China, in part by the State Scholarship Fund, China, under Grant 201908320532, in part by the Post-graduate Research & Practice Innovation Program of Jiangsu Province under Grant KYCX18_1016, and in part by the College Students' Enterprise and Entreprenuership Education Program of Jiangsu Province under Grant 201910300059Z.

ABSTRACT Key distribution is the foundation for protecting users' privacy and communication security in cloud environment. Information hiding is an effective manner to hide the transmission behavior of secret information such as keys, and thus it makes the secure key distribution possible. However, the traditional information hiding systems usually embed the secret information by modifying the carrier, which inevitably leaves modification traces on the carrier. Thus, they cannot resist the detection of the steganalysis algorithm effectively. To avoid this issue, the coverless information hiding technique has been proposed accordingly, in which the original images of which features can express the secret information are directly used as stego-images. Since the existing coverless information hiding methods use the low-level handcrafted image features to express secret information, it is hard for them to realize desirable robustness against common image attacks. Moreover, their hiding capacity is limited. To conquer these problems, we design a novel robust image coverless information hiding system using Faster Region-based Convolutional Neural Networks (Faster-RCNN). We employ Faster-RCNN to detect and locate objects in images and utilize the labels of these objects to express secret information. Since the original images without any modification are used as stego-images, the proposed method can effectively resist steganalysis and will not cause attackers' suspicion. The experimental results demonstrate that the proposed system has higher performance in terms of robustness and capacity compared to the typical coverless information hiding methods.

INDEX TERMS Coverless information hiding, image steganography, object detection, faster-RCNN, key distribution.

I. INTRODUCTION

With the rapid development of network communication and information technology, information security and privacy protection have become research hotspots in cloud environment [1]–[3]. The current mainstream privacy protection approaches usually encrypt secret messages before they are transmitted. In this case, the security of communication depends on whether the key is secure. For wired connected devices, key distribution and updates can be performed on a secure communication channel constructed between these devices. However, in wireless environment, it is difficult to establish a secure channel [1]. Even if the initial key is obtained by physical means, it is difficult to securely update the key. Since secret information such as keys transmitted in wireless environment easily cause attackers' suspicions, it is easy to capture or intercept. Thus, how to implement transmission of secret messages such as keys on the public channel without causing attackers' suspicions is a challenging problem. Information hiding technique provides an alternative solution to this problem, since it can hide the behavior of secret information transmission.

The associate editor coordinating the review of this manuscript and approving it for publication was Roberto Caldelli.

In the literature, the traditional information hiding systems generally hide information by modifying the carrier slightly [5]. As an adversary of information hiding, steganalysis aims to detect the presence or absence of secret information in a suspicious carrier based on the modification traces left on the carrier. The steganalysis methods are mainly based on statistical features. For example, Fridrich et al. [6] proposed Spatial Rich Models (SRM) based on a combination of rich image models and an integrated classifier. Although it is hard to detect the secret information hidden in the carrier by human eyes, the steganalysis methods may successfully detect the existence of hidden secret information based on the modification traces.

In order to fundamentally resist the steganalysis methods, the coverless information hiding technique has been proposed accordingly. Different from the traditional information hiding systems, the concept of coverless information hiding is to use the original images of which features can express the secret information as stego-images [6]. The existing coverless information hiding systems rely on low-level handcrafted features of images to express secret information. Because the inherent features of the images are directly used to represent the secret information and the images are not modified, these methods can effectively resist the detection of the steganalysis algorithms. However, low-level handcrafted features are easily affected by various intentional or unintentional image attacks such as compression and noise addition during communication, which makes these systems less robust. In addition, it is difficult to express relatively long secret information using these features in a single stego-image, which results in very low capacity of these methods.

To address the above issues of the existing coverless information hiding systems, this paper propose a robust coverless information hiding system using Faster Region-based Convolutional Neural Networks (Faster-RCNN) [9]. We first used the Faster-RCNN algorithm to detect and locate the objects in each image, and then used high-level semantic features of the objects to represent the secret information. Compared with the low-level features, high-level semantic features, i.e., the label information of the objects are less likely to be affected by common image attacks, and thus the proposed system achieves higher robustness. Moreover, the use of high-level semantic features can also increase the hiding capacity. In addition, the system can realize the covert transmission of important information such as keys when a secure communication channel is not established in advance.

The rest of this paper is organized as follows. Related work is introduced in Section II. The proposed method is described in Section III. The experimental results and analysis are given in Section IV. Section V draws a conclusion.

II. RELATE WORK

A. FASTER RCNN

Object detection is one of basic tasks in the field of computer vision. In recent years, with the rapid development of deep learning technology, the research attention of object detection has been shifted from the traditional handcrafted feature-based algorithms to the deep neural network-based algorithms. Faster RCNN [9] employs a Region Proposal Network (RPN) which shares full-image convolutional features with the detection network, thereby achieving almost real-time detection of region proposals. It's worth noting that a Region Proposal Network is a fully convolutional network that predicts both object's bounds and scores for each position at the same time. In this paper, we use objects detected by Faster RCNN to express secret information.

B. COVERLESS INFORMATION HIDING

In the literature, many coverless information hiding systems have been proposed based on text or image files. In the text-based coverless information hiding systems, the text that contains the same characters as the secret information is used as stego-text, and the certain attributes of the characters is used to mark the position of secret information in the stego-text. In [10], the components of Chinese characters are used as labels to mark the location of the secret information in the stego-text. In [11], the authors employed the least significant bits (LSBs) of the character's Unicode as location labels. Sun et al. [12] utilized named entities to express and transmit messages, and Zhang et al. [13] adopted rank map to obtain the stego-texts. In the literature [14], Zhou et al. proposed a method that a stego-text can convey more than one character. The above text-based coverless information hiding methods have high resistance to the detection of steganalysis methods, since these methods directly employ original text to transmit secret information.

Like the text-based coverless information hiding methods, the image-based coverless information hiding methods use the inherent features of the image to express the secret information for secret communication. In general, the existing coverless information hiding methods employed image retrieval methods [14] to find the images of which features can represent or already contain the secret information as stego-images for secret communication. Fridrich et al. [18] first proposed the concept of coverless information hiding based on carrier selection, which selects specific natural images as stego-images according to certain feature mapping rules. Subsequently, Zhou et al. [19] proposed a coverless information hiding method, in which the hash sequences based on image pixel differences are extracted to represent and transmit secret information. In order to improve the hidden capacity, some other researchers [19] extracted different features to express and transmit the secret messages. In addition, Wu et al. [24] first employed the gray gradient co-occurrence matrix to encode the image, and then constructed the mapping relationship between the matrix and the random number to represent the secret information. In [25], Zhou et al. proposed a novel coverless information hiding system, which aims to hide a secret image into a set of carrier images. Specifically, the partial duplicates of the secret image in the database are retrieved and used as stego-images, each of which shares one or several visually

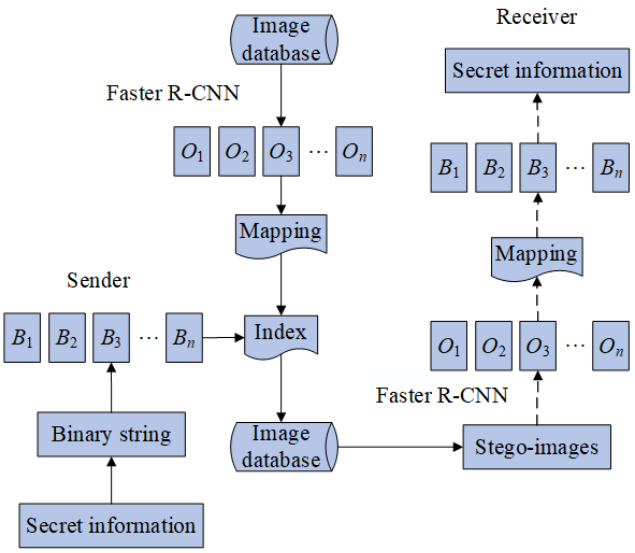


FIGURE 1. The framework of the proposed coverless information hiding system.

similar patches with the secret image for secret communication. Recently, Cao et al. [26] proposed a dynamic content selection framework for image coverless information hiding, which dynamically selects natural images to represent and transmit secret messages according to certain mapping rules constructed between secret messages and user identity. In [27], Discrete Cosine Transformation (DCT) coefficients are used to represent secret information.

All the above coverless information hiding methods employed the low-level features to represent secret information. Although they can effectively resist the steganalysis, they suffer from the robustness problem and their hiding capacity is very low. Thus, it is hard to apply them in real-world scenarios. Inspired by the above, by using object characteristics detected by Faster RCNN algorithm, we propose a novel robust coverless information hiding method that uses the original images of which features can express the secret information as stego-images to represent and transmit secret information.

III. PROPOSED METHOD

The framework of the proposed system is illustrated by Fig. 1. In the system, there is no modification trace left in the stego-images, since we directly find proper original images as stego-images to transmit secret messages. Before the image selection, we establish the mapping dictionary between binary sequences and the labels of objects. Then, we use Faster-RCNN to detect and locate the objects in images from the database, and construct a multi-level inverted index file.

To generate the stego-images, the sender first converts the secret message into a set of binary sequences. Then, by looking up the constructed index file, he finds the corresponding images of which object can represent the binary sequences according to the mapping dictionary.

TABLE 1. The established mapping dictionary.

Object label	Binary sequence
Car	00000
Bicycle Motorcycle	00001
Airplane Bus Train Truck	00010
Person	00011
…	…
Horse	11000
…	…
Dog Cat	11111

After receiving the stego-images, the receiver uses the Faster-RCNN algorithm to detect the object regions from the stego-images and obtain their labels, and then he transforms the labels to secret message according to the mapping dictionary.

A. MAPPING DICTIONARY ESTABLISHING

In order to achieve coverless information hiding, we need to establish a mapping dictionary between secret binary sequences and the features of original images. In this paper, we employ the object labels to represent the secret messages, and thus we convert the secret message to binary sequences and use the Faster-RCNN algorithm to detect the objects and their labels for establishing the mapping dictionary.

There are a set of object labels detected by the Faster-RCNN algorithm. If we divide the object labels into 2^n categories, each object can represent n-bit message. As shown in Table 1, we establish a mapping dictionary, denoted as M. In this mapping dictionary, labels are divided into 2^5 categories.

Since we use the object labels to represent the secret messages, we need to determine the order of object labels used to represent the secret information. In our system, we use the Faster-RCNN algorithm to detect objects and its labels from images. Each object is denoted as (x, y, h, w), where x and y mean the coordinates of central points of object region, and h and w represents the height and width of the object region, respectively. Then, we sort the objects according to their area values, i.e., $h \times w$ in ascending order to express the secret messages. According to Table 1, every object represents 5-bit message. Before secret communication, we convert secret message into a N-bit binary string. If N is not divisible by 5, we add several zeros at the end of the binary string to ensure the number of bits can be divisible by 5. At the same time, a 5-bit binary message indicating the number of bits is added in front of the binary sequence. For example, as shown in Fig. 2, the binary sequence represented by the image is [00011 11111 00000 00011 11000], and the actual valid message is [11111 00000 00011 11].

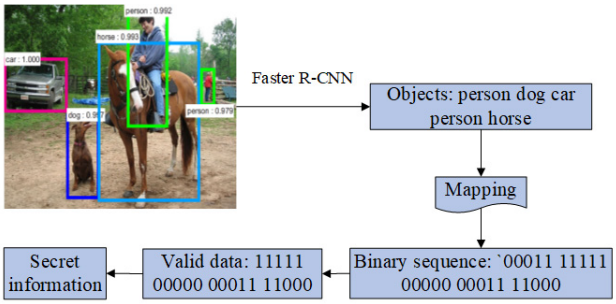


FIGURE 2. The secret information represented by object labels.

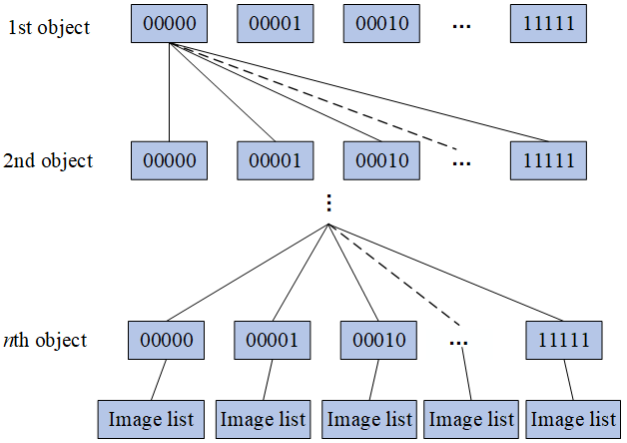


FIGURE 3. The constructed multi-level inverted index file.

B. INVERTED INDEX FILE

It is very time-consuming to directly find an image of which object labels can represent a given secret information in a large-scale image database. Therefore, in order to achieve an efficient coverless information hiding, we attempt to design a multi-level inverted index structure as shown in Fig. 3. To this end, we first employ Faster-RCNN algorithm to detect the objects and their labels in each image from database and sort these in ascending order, and then convert these labels to a binary sequence according to the mapping dictionary. Next, we store the IDs of image list in the index file according to the index values. For example, the image in Fig. 2 should be stored in the image list under the multi-level index values, i.e., 00011, 11111, 00000, 00011, 11000, 00011, and 00000.

C. INFORMATION HIDING PROCESS

The proposed method uses the object labels of the images to represent and transmit the binary sequences. As shown in Fig. 4, the process of information hiding aims to find an original image that can represent a secret message. The hiding steps are given as follows.

Step (1): In proposed method, to improve the security, different users will adopt different mapping dictionaries, and the same user will also adopt different dictionaries at different time. Before information hiding, we need to determine the mapping dictionary M' for the current secret communication,

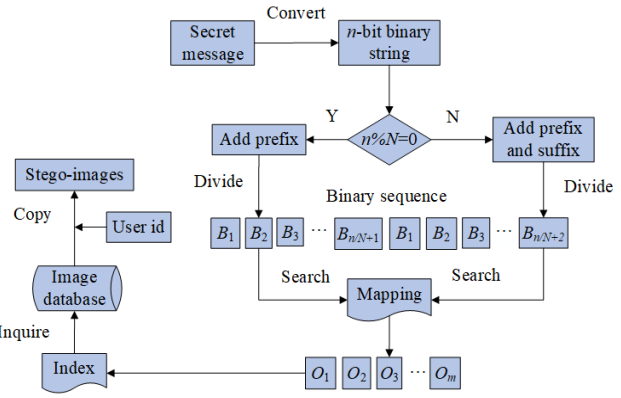


FIGURE 4. The information hiding process.

and M' is defined as follows:

$$M' = M \times f_{id}(ID) \times f_t(T) \tag{1}$$

where M is the initial mapping dictionary, $f_{id}(ID)$ and $f_t(T)$ are randomized functions, ID is the user identity, and T is the time interval, respectively.

Step (2): The secret message is converted to a binary string. Suppose that the total length of the secret information is n -bits, and every object represents n-bit binary. If N cannot be divisible by n, we add several zeros after the binary string until the length of the secret information can be divided by n. At the same time, a n-bit binary number indicating the number of bits is added in front of the binary string. Then, secret information is partitioned into m binary information segments, where the number of segments m is determined by Eq. 2. Thus, secret message can be denoted as $B = \{B_1, B_2, B_3, \ldots, B_m\}$.

$$m = \begin{cases} \dfrac{N}{n} + 1 & if\ N \bmod n = 0 \\ \left\lfloor \dfrac{N}{n} \right\rfloor + 2 & if\ N \bmod n \neq 0 \end{cases} \tag{2}$$

Step (3): The set of IDs of corresponding objects $O = \{O_1, O_2, O_3, \ldots, O_m\}$ is obtained according to the mapping M'.

Step (4): By looking up the index file, a candidate image set is obtained, and then the stego-images are selected from the candidate set according to the user's identity. That is, if there are many images in the candidate set, we randomly select an image according to the user's identity, so as to ensure different users use different stego-images to hide and transmit a same secret message.

Step (5): Finally, the stego-images are obtained and used to transmit secret image in a hidden manner.

D. INFORMATION EXTRACTION PROCESS

In our method, compared to the information hiding process of the sender, and the receiver's information extraction process is relatively simple. As shown in Fig. 5, the steps of information extraction process are given as follows.

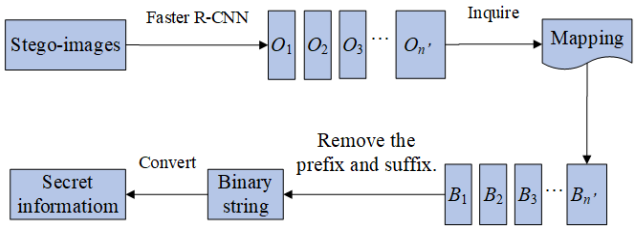


FIGURE 5. The information extraction process.

TABLE 2. The experimental result of the hiding capacity.

Methods	Capacity $(bits\ /\ carrier)$
Literature[19]	8
Literature[20]	8
Literature[21]	18
Our method, $q = 4$	20
Our method, $q = 5$	25

Step (1): The sender receives stego-images from a public channel.

Step (2): The sender uses the Faster-RCNN algorithm to detect the objects $O = \{O_1, O_2, O_3, \ldots, O_m\}$ and their labels in the stego-images and then sort them according to the area values of these object regions in ascending order.

Step (3): The sender obtains the corresponding binary sequence $B = \{B_1, B_2, B_3, \ldots, B_m\}$ according to the mapping dictionary M' determined by the step (1) of Section II-C.

Step (4): All the segments are concatenated to form the secret binary sequence, and the first n-bits in the front of the binary sequence and a number of 0 at the end of the binary sequence are removed. Then, the binary secret sequence is converted to the secret information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The environment of our experiments is given as follows. System: Ubuntu 16.04 LTS, RAM: 48GB DDR4, CPU: i5-8500 3.0GHz, GPU: NVIDIA GTX 1080Ti; Software platform: Tensorflow v1.2, python 3.6. The experiment is implemented based on the code of [9] and the database of PASCAL VOC 2007 [28] and VOC 2012 [29]. The experimental results and analysis focus on three aspects: hiding capacity, robustness and security.

A. HIDING CAPACITY

The proposed information hiding system uses the object labels of the images to transmit binary bit sequences. In the experiment, every object represents 5-bit information. Therefore, the hidden capacity of each stego-image depends on the number of objects it contains. Suppose that the average number of objects contained in the stego-images is q. In this section, we test the hiding capacity of different methods. The experimental results are as follows.

As shown in the table 2, the hiding capacity of this method increases as q increases. However, with the increase of q, the images that can represent the secret information will be more difficult to find. Moreover, since we use multiple objects in a stego-image to represent secret information, the hidden capacity of the proposed method is higher compared to the previous methods.

B. ROBUSTNESS ANALYSIS

Robustness is an important factor to evaluate the performance of coverless information hiding, which determines whether the receiver can correctly extract secret messages. Several kinds of attacks applied to the stego-images are listed below.

a. Rotation. The rotation angles are 10°, 30°, and 50°, respectively.
b. Scaling. The scaling ratios are 0.3, 0.5, 0.75, 1.5, and 3, respectively.
c. Gaussian noise. The variances σ are 0.001 and 0.005, respectively.
d. Salt and pepper noise. The variances σ are 0.001 and 0.005, respectively.
e. Speckle noise. The variances
f. σ are 0.01, 0.05, and 0.1, respectively.
g. Median filtering. The template sizes are 3×3, 5×5, and 7×7, respectively.
h. Mean filtering. The template sizes are 3×3, 5×5, and 7×7, respectively.
i. Mean filtering. The template sizes are 3×3, 5×5, and 7×7, respectively.

In this paper, Bit Error Rate (BER) is introduced to measure the robustness of the algorithm in the communication process. The BER is defined as follows:

$$BER = \frac{\sum_{i=1}^{m} p_i \oplus q_i}{m} \tag{3}$$

where $\boldsymbol{p}_i$ represents the embedded bits and $\boldsymbol{q}_i$ represents the corresponding extracted bits. As shown in Table 3, the experimental results show that, compared with the literature [20], the proposed method is more robust against both geometric attacks and noise attacks. This is mainly because we use high-level features, i.e., object labels in the image to represent secret information, and it is difficult for a general attack to affect the object labels. This also demonstrates that high-level semantic features are more robust than the low-level handcraft features.

C. SECURITY ANALYSIS

In the proposed coverless information hiding system, the objects in the original images detected by Faster RCNN algorithm are used as stego-images to convey the secret message. There is no modification in the stego-images, so the proposed system can fundamentally resist the detection by the existing steganalysis methods and human eyes. These stego-images transmitted on the public channel generally will not easily cause attackers' suspicion. Even if the attackers

TABLE 3. Bit error rate comparison between proposed method and the related method [20].

Attack		SIFT+BOF[20]	Proposed
Rotation	10°	49.34%	20.69%
	30°	47.85%	51.50%
	50°	49.75%	67.94%
Scaling	0.3	50.76%	45.12%
	0.5	50.24%	19.49%
	0.75	48.82%	12.19%
	1.5	48.75%	7.87%
	3	80.76%	7.25%
Gauss Noise	0.001	48.00%	7.23%
	0.005	47.97%	18.94%
Salt & Pepper Noise	0.001	48.70%	10.00%
	0.005	47.40%	14.37%
Speckle Noise	0.01	47.05%	13.12%
	0.05	47.87%	21.19%
	0.1	47.20%	21.38%
Median filtering	(3×3)	47.99%	15.12%
	(5×5)	49.19%	23.50%
	(7×7)	48.25%	36.62%
Mean filtering	(3×3)	49.51%	13.44%
	(5×5)	49.19%	27.83%
	(7×7)	49.25%	41.19%
Mean filtering	(3×3)	47.31%	11.81%
	(5×5)	49.53%	17.87%
	(7×7)	48.87%	24.62%

suspect that an image contains secret message, it is very hard for them to obtain the parameters of the Faster-RCNN and mapping dictionary. In summary, the proposed system has a good security, and it is very difficult for malicious attackers to crack the system.

V. CONCLUSION

This paper introduces a robust coverless information hiding system based on Faster RCNN algorithm for key distribution in cloud environment. It uses the high-level semantic features of images to express secret message and finds the images of which object labels can represent secret message as stego-images for secret communication. Compared with the existing coverless information hiding method using low-level handcraft features, the proposed method can more easily find stego-images. In addition, this system provides a solution for the covert communication with a small amount of data such as keys in cloud environment. The theoretical and experimental results show that, compared to the existing systems, the proposed coverless information hiding system has higher robustness and capacity. In future, we will focus on improving the hiding capacity of coverless information hiding.

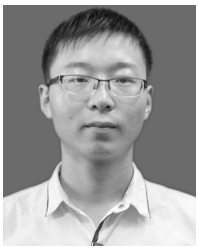
REFERENCES

[1] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Gener. Comput. Syst.*, vol. 88, pp. 636–643, Nov. 2018.
[2] Z. Zhou, C.-N. Yang, Y. Yang, and X. Sun, "Polynomial-based Google map graphical password system against shoulder-surfing attacks in cloud environment," *Complexity*, vol. 2019, Nov. 2019, Art. no. 2875676.
[3] L. Qi, S. Meng, X. Zhang, R. Wang, X. Xu, Z. Zhou, and W. Dou, "An exception handling approach for privacy-preserving service recommendation failure in a cloud environment," *Sensors*, vol. 18, no. 7, p. 2037, 2018.
[4] W. Wang, P. Xu, L. Yang, and J. Chen, "Cloud-assisted key distribution in batch for secure real-time mobile services," *IEEE Trans. Services Comput.*, vol. 11, no. 5, pp. 850–863, Sep./Oct. 2016.
[5] Y. Zhang, D. Ye, J. Gan, Z. Li, and Q. Cheng, "An image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection," *Comput. Mater. Continua*, vol. 56, no. 1, pp. 151–167, 2018.
[6] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[7] X. Duan, H. Song, C. Qin, and M. K. Khan, "Coverless steganography for digital images based on a generative model," *Comput., Mater. Continua*, vol. 55, no. 3, pp. 483–493, Jul. 2018.
[8] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Proc. Int. Conf. Cloud Comput. Secur.*, 2015, pp. 123–132.
[9] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, vol. 39, 2015, pp. 91–99.
[10] X. Chen, H. Sun, Y. Tobe, Z. Zhou, and X. Sun, "Coverless information hiding method based on the Chinese mathematical expression," in *Proc. Int. Conf. Cloud Comput. Secur.*, 2015, pp. 133–143.
[11] X. Chen, S. Chen, and Y. Wu, "Coverless information hiding method based on the Chinese character encoding," *J. Internet Technol.*, vol. 18, no. 2, pp. 133–143, 2017.
[12] H. Sun, R. Grishman, and Y. Wang, "Active learning based named entity recognition and its application in natural language coverless information hiding," *J. Internet Technol.*, vol. 18, no. 2, pp. 443–451, 2017.
[13] J. Zhang, J. Shen, L. Wang, and H. Lin, "Coverless text information hiding method based on the word rank map," *J. Internet Technol.*, vol. 18, no. 2, pp. 427–434, 2017.
[14] Z. Zhou, Y. Mu, and N. N. Zhao, "Coverless information hiding method based on multi-keywords," *Int. J. Secur. Appl.*, vol. 10, no. 9, pp. 309–320, 2016.
[15] Z. Zhou, Y. Wang, Q. M. J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 48–63, Jan. 2017.
[16] Z. Zhou, Q. Wu, F. Huang, and X. Sun, "Fast and accurate near-duplicate image elimination for visual sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 2, pp. 1–12, Feb. 2017.
[17] Z. Zhou, Q. M. J. Wu, and X. Sun, "Multiple distance-based coding: Toward scalable feature matching for large-scale Web image search," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2019.2919570.
[18] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[19] Z. Zhou, Q. M. J. Wu, C.-N. Yang, X. Sun, and Z. Pan, "Coverless image steganography using histograms of oriented gradients-based hashing algorithm," *J. Internet Technol.*, vol. 18, no. 5, pp. 1177–1184, 2017.
[20] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *J. Internet Technol.*, vol. 18, no. 2, pp. 435–442, Mar. 2017.
[21] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *Proc. Int. Conf. Intell. Comput. ICIC*, 2017, pp. 536–547.
[22] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Comput., Mater. Continua*, vol. 54, no. 2, pp. 197–207, 2018.
[23] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 7965–7980, 2019.

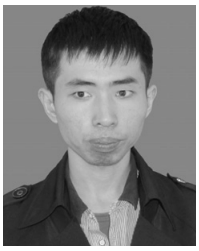
[24] J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, and Y. Jia, "A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix," *IETE Tech. Rev.*, vol. 35, pp. 23–33, Oct. 2018.
[25] Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Comput.*, vol. 23, no. 13, pp. 4927–4938, Jul. 2019.
[26] Y. Cao, Z. Zhou, C. N. Yang, and X. Sun, "Dynamic content selection framework applied to coverless information hiding," *J. Internet Technol.*, vol. 19, no. 4, pp. 1179–1186, 2018.
[27] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Trans. Multimedia*, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.
[28] (2007). *The PASCAL Visual Object Classes Challenge 2007 (VOC2007) Results*. [Online]. Available: http://host.robots.ox.ac.uk/pascal/VOC/voc2007/
[29] (2012). *The PASCAL Visual Object Classes Challenge 2007 (VOC2012) Development Kit*. [Online]. Available: http://host.robots.ox.ac.uk/pascal/VOC/voc2012/

ZHILI ZHOU received the B.S. degree in communication engineering from Hubei University, in 2007, and the M.S. and Ph.D. degrees in computer application from the School of Information Science and Engineering, Hunan University, in 2010 and 2014, respectively.

He is currently an Associate Professor with the School of Computer and Software, Nanjing University of Information Science and Technology, China. Also, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. His current research interests include near-duplicate image/video retrieval, image search, image/video copy detection, coverless information hiding, digital forensics, and image processing.



YI CAO received the B.S. degree from the Nanjing University of Information Science and Technology, China, in 2016, where he is currently pursuing the Ph.D. degree. His research interest includes networks and information security.



MEIMIN WANG received the B.S. degree from the Nanjing University of Information Science and Technology, China, in 2019, where he is currently pursuing the M.D. degree. His research interest includes blockchain and information security.

ENMING FAN is currently pursuing the B.S. degree with the School of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include image steganalysis and machine learning.

Q. M. JONATHAN WU (M'92–SM'09) received the Ph.D. degree in electrical engineering from the University of Wales, Swansea, U.K., in 1990.

From 1995 to 2005, he was with the National Research Council of Canada, where he became a Senior Research Officer and a Group Leader. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada. He has published more than 300 peer-reviewed articles in computer vision, image processing, intelligent systems, robotics, and integrated microsystems. His current research interests include 3-D computer vision, active video object tracking and extraction, interactive multimedia, sensor analysis and fusion, and visual sensor networks.

Dr. Wu is the Fellow of the Canadian Academy of Engineering. He holds the Tier 1 Canada Research Chair in Automotive Sensors and Information Systems. He is, or was, an Associate Editor of the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, *Cognitive Computation*, and the *International Journal of Robotics and Automation*. He has served on technical program committees and international advisory committees for many prestigious conferences.