Dynamic Content Selection Framework Applied to Coverless Information Hiding

Yi Cao[1], Zhili Zhou[1,2], Ching-Nung Yang[3], Xingming Sun[1]

[1] Jiangsu Engineering Centre of Network Monitoring & School of Computer and Software, Nanjing University of Information Science and Technology, China

[2] Department of Electrical and computer Engineering, University of Windsor, Canada

[3] Department of Computer Science and Information Engineering National DongHwa University, Taiwan

{caoyinuist, zhou_zhili}@163.com, cnyang@gms.ndhu.edu.tw, sunnudt@163.com

Abstract

The traditional information hiding (IH) methods usually modify the carrier in accordance with certain rules to embed secret information. In this way, it is inevitable to leave some modification traces on the carrier, so that these methods are difficult to effectively resist the detection of various types of steganalysis algorithms. In order to fundamentally resist steganalysis, recently, a novel information hiding technique, called coverless information hiding (CIH), has been proposed to hide secret information into natural carrier without modification. In this paper, we propose a dynamic content selection framework (DCSF) for CIH to hide secret text information into natural images. To realize the CIH, the proposed framework dynamically selects images to represent the secret information via the mapping relationships constructed between the inherent features of the images and the secret information. More specifically, after constructing the mapping relationships by using a function of the values of local features, we choose multiple blocks from a natural image to represent the corresponding secret fragments. Moreover, to improve the security, we use a random label sequence to decide which blocks of the image will be chosen for the representation. In addition, since the required images may not be found in the image database, the approximate matching algorithm based on synonym and homonym is also proposed to find the images to approximately represent the secret information. Experimental results and analysis show that the proposed framework has good performance in anti-steganalysis and capacity.

Keywords: Dynamic content selection framework, Coverless information hiding, Bag of Words (BOW), Visual words, Approximate replacement

1 Introduction

The purpose of information hiding (IH) (or steganography) is to conceal communication and protect copyright, by hiding useful information in a host signal and extracting information when needed [1]. The popularity of personal computers and the explosive growth of multimedia data on the Internet provide a convenient condition for the implementation of information hiding, which results in the rapid development of information hiding. Digital images are often regarded as one of important carriers, which contains a large number of feature information and have been utilized widely. As is well-known, there are two ways of image steganography. One is based on Spatial Domain. Such as the method proposed in [2] that directly replace the least significant bit (LSB) of the image. In order to improve the hiding capacity and invisibility, [3] proposed an adaptive LSB hiding method based on image pixel-value difference (PVD). And methods of changing certain statistical features by modifying the data of the host image [4] and so on. The other is based on Transform domain methods, such as DFT domain concealment [5], DCT domain hiding [6] and DWT domain concealment [7], etc. These methods modify the carrier in accordance with certain rules to embed information. In the above two ways, it is inevitable to leave the traces on the secret carrier, so that these methods are also difficult to effectively resist the detection of various types of steganalysis algorithm.

In order to fundamentally resist the detection of various types of steganalysis algorithms, Zhou et al. proposed the concept of coverless information hiding (CIH) [8]. CIH does not mean that the carrier is not needed. However, compared with the traditional IH methods, it emphasizes that the information hiding does not need other carrier, but directly acquires the stego-carrier based on secret information. There are two main kinds of CIH methods depending on the carrier selected, they are text-based methods and image-based methods. For text-based coverless information hiding, Chen et al. proposed a method based on the Chinese mathematical expression [9]. Chen's method retrieves normal texts which containing

*Corresponding Author: Xingming Sun; E-mail: sunnudt@163.com
DOI: 10.3966/160792642018081904020

the secret information from text big data to convey the message. In Chen's method, Chinese mathematical expression is used as labels to determine the location of the secret information. Chen's method can effectively resist the detection of the various types of steganalysis algorithm which based on statistical analysis, due to this method don't modify the stego-text. After that, literature [10-13] proposed some similar methods. Compared with Chen's method, these methods use different labels. Such as literature [10] uses the rank map to generates the stego-vectors and literature [13] utilizes the named entities as labels. For the image, it already contains a lot of feature information, such as grayscale value, color, texture, edge, contour, and high-level semantics. Using the appropriate feature description, it is possible to make a certain mapping relationship between these feature information and secret information. If it is possible to acquire some natural images which own inherent characteristics have a certain mapping relationship with secret information. By using these images as stego-images for secret information transmission, it can effectively resist the detection of various types of image steganalysis methods. Similar to the image retrieval technique [14-18], some coverless image steganography methods have proposed. Such as [8] proposed an image steganography framework, which uses the hash sequence of the original image to represent the secret segments. After that, [19] proposed a coverless image steganography method based on Scale Invariant Feature Transform (SIFT) and Bag of Feature (BOF). Firstly, this method extracts the SIFT feature of the image; Then this method uses the BOF model to cluster the SIFT features, Finally, a hash function is used to get a hash sequence, which is the same as the secret segments. In addition, [20] uses the average of the sub-image pixels to convey secret information. [21] replaces secret image blocks with similar image blocks. What's more, as the application of deep learning continues to expand [22-23], [24] proposes a coverless information hiding method based on GAN.

However, as shown in Table 1, the capacity of these proposed methods is very low. Because the purpose of these methods is to retrieve the matching carrier, rather than modifying the carrier. And also, in these methods, a stego-carrier only represents a secret information fragment. What's more, due to the randomness of the secret message, it is difficult to retrieve the eligible carrier in the smaller carrier base.

Table 1. The capacity of proposed methods

Methods	capacity (bits · carrier $^{-1}$)
literature [8]	8
literature [19]	8
literature [9]	16
literature [20]	36

To address these problems, we propose a dynamic content selection framework (DCSF) without any modification applied for CIH. The aim of the proposed framework is to dynamically select the inherent features of the image based on the mapping between the inherent feature of the image and the secret information to express the secret information. To improve the capacity, we use an image to represent multiple secret information fragments by using image blocking method. In our framework, each sub-image can represent a secret message fragment. However, we use the random labels, that is, the position sequence of the sub-images, to dynamically select the sub-images representing the secret message fragments according to certain rules. This is mainly considered for security. At the same time, we agreed that each image represents the number of secret information fragments. Or determining the number of the secret information fragments represented by the image according to the selected features. In order to enhance the probability of retrieving stego-carriers, we have created a many-to-one mapping, that is, multiple features correspond to a secret information fragment.

In addition, if the feature corresponding to the secret information fragment cannot be found, the fragment will be replaced by synonym or homonym. As an example, we use the BOW model to extract multiple visual words in an image, and then use these visual words to represent the corresponding text information. The main contribution of this paper is to propose a dynamic content selection framework. Because there is no modification to the stego-carrier, the method can resist the detection of various steganalysis algorithms. And, in this framework, a secret carrier can represent multiple secret information fragments, so the hidden capacity can be relatively high. What's more, we use many-to-one mapping and approximate replacement, so we can effectively enhance the probability of retrieval.

The remainder of this paper is organized as follows. The Section 2 takes the Bag of Words model as an example to introduce DCSF in detail. DCSF applied to CIH is introduced in Section 3. The Section 4 shows the results of the experiment and analysis. And the Section 5 is a conclusion.

2 Proposed Method

The proposed DCSF is intended to dynamically select images that can represent multiple secret information fragments. First we create a database containing a large number of images. Next, we divide each image into $m \times n$ blocks and determine one feature which can represent the block. Then we determine a pseudo-random label sequence that represents the position of the blocks. Finally, according to the mapping relationship between the secret

information fragments and the features, we use the "label + feature" method to select the images as stego-images. As shown in Figure 1, DSCF mainly includes the following parts: mapping relationship between secret information fragments and features, label sequence, inverted index, approximate replacement method and image database.

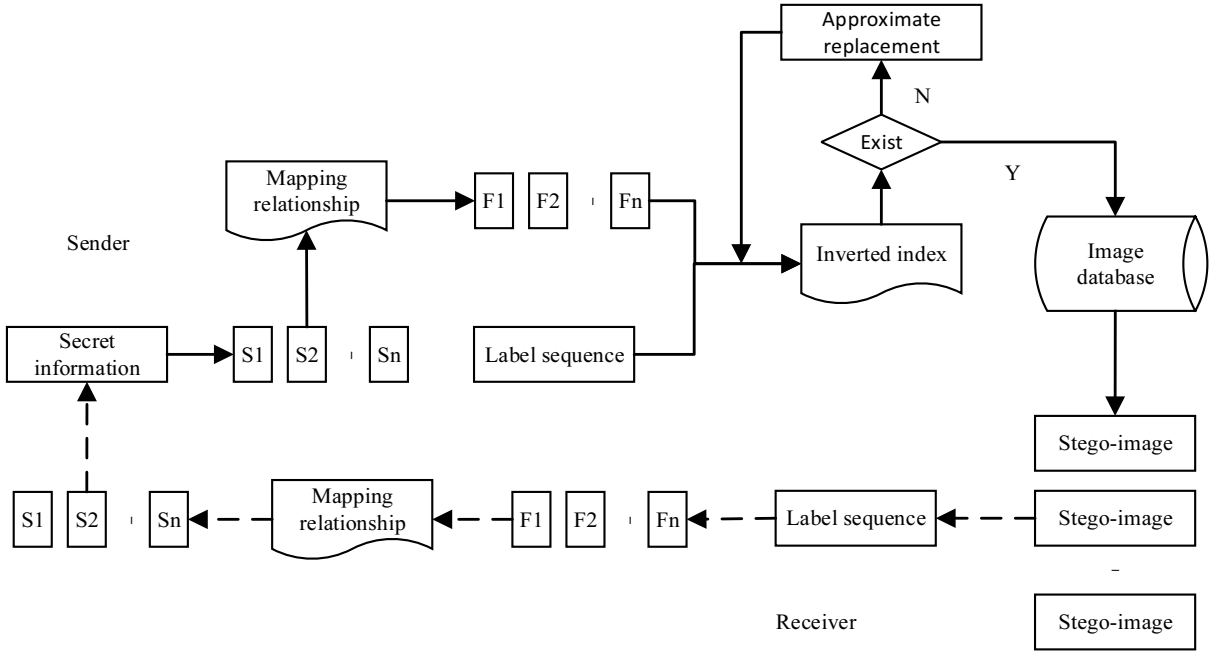


Figure 1. The framework of DSCF

2.1 Label Sequence

In order to realize dynamic selection of stego-images, and to improve the security of the DCSF, we propose a method to determine the location of the stego-blocks with the label sequence. In our framework, images are divided into $x \times y$ blocks, and these blocks are marked as $\{(1,1),(1,2),(1,3),...,(x,y)\}$, which is the label of the DCSF, in the order of raster scanning. We use the image blocks at the label location to represent the secret information fragments. First, the two sides share a collection of labels that need to be kept strictly confidential. Then the sender obtains the identity ID information I of the receiver, the current time T of the system, and the number of secret information fragments n. After that, n labels from the collection will be selected to form the original label sequence $P_0 = \{p_1, p_2, p_3, \ldots, p_n\}$. Finally, the original label sequence P_0 is randomly processed by using the hash function $H_P(I,T,P_0)$ to obtain the label sequence in current communication, namely $P = \{p'_1, p'_2, p'_3, \ldots, p'_n\}$. In this method, the identity ID information I is an integer, the system time T is divided into 12 intervals according to the hours, respectively, corresponding to the integer from 0 to 11.

2.2 The Construction of Mapping Relationships

The role of mapping relation is to convert the secret information fragments into the corresponding features sequence. If both sides use the same mapping relation, the secret information fragments and features can be reversible conversion. For example, we use the visuals words (VW) from the Bag of Words (BOW) model to express the Chinese text information. First of all, we divide and calculate a lot of texts to get the keywords and word frequency histogram. Then we construct the visual words codebook with the BOW model. The BOW model is used not only in the codebook training to be ensure to map all the keywords, but also to take into account the computational complexity and the actual number of effective visual words. The number of visual words selected in this paper is 10 000, that is, K = 10 000 when using K-means clustering [25]. We extract SIFT features, which is used to cluster, to make the codebook keep robust [26]. The specific codebook training process shown in Figure 2.

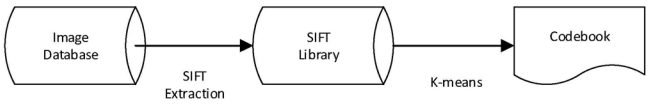
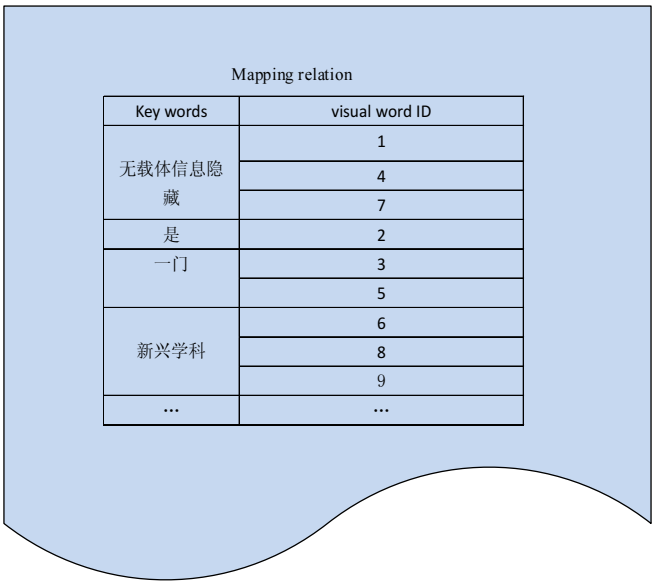


Figure 2. The process of codebook training

After generating the codebook, the position of the visual words in the codebook is its ID. And then count visual words frequency histogram which represents each sub-image. Finally, we establish the mapping relation between key words and visual words, according to the key words frequency histogram and the visual words frequency histogram. In addition, in order to ensure that the stego-image could be easily

retrieved which correspond to the keyword, multiple visual words can be used to correspond to one key word, as shown in Figure 3.


Mapping relation

Key words	visual word ID
无载体信息隐藏	1
	4
	7
是	2
一门	3
	5
新兴学科	6
	8
	9
…	…

Figure 3. Mapping relationship

According to the constructed mapping relationship, the text information can be expressed as a visual words sequence. But for each sub-image, using BOW model can still extract more than one visual word. This paper selects the visual word, whose frequency is maximum, on behalf of the sub-image area. For example, as shown in Figure 4, the image represents the secret information: "无载体信息隐藏式一门新兴学科".

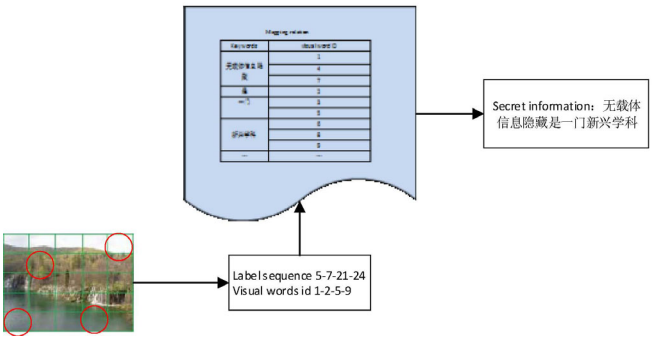


Figure 4. The examples of mapping relationship

2.3 Multi - level Inverted Index Structure

For a given secret information, it is very time-consuming to find the natural images containing this secret information exhaustively in the established large-scale image library. So we establish a multi-level inverted index containing visual words id (features), block location (label), and visual words frequency information to ensure efficient and accurate search. as shown in Figure 5.

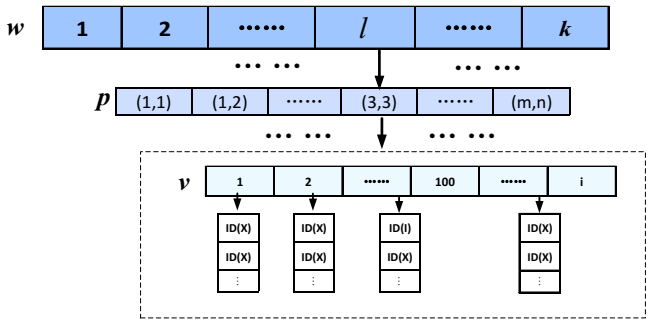


Figure 5. The inverted index structure

The first layer of the index structure is the id of the visual words. For ease of description, the id of the visual words will be marked as w. The second layer of the index structure is the label of the sub-image, denoted as p. The third layer of the index structure is the value of the visual word which can represent the image, denoted as v. The fourth layer of the index structure is a list of image IDs that meet the requirements of the previous layers, satisfying the condition (w, p, v). At the same time, the images has been normalized in direction and scale before indexing, to resist the rotation and other attacks.

2.4 Approximate Replacement Method

In order to achieve CIH in a smaller image database, we establish synonyms and homophones library based on text keywords. So, if the feature corresponding to the secret information fragment cannot be found, the fragment will be replaced by synonym or homonym.

Table 2. The example of replacement

keywords	synonym or homonym.
因为	由于 缘于
的	得 地
意志	抑制 益智 易帜 译制
…	…

3 DCSF Applied to CIH

3.1 Information Hiding Method

Secret information hiding and extracting is the core and stress of this article. The proposed DCSF achieve a goal that hiding multiple key words in an image. The method is pre-agreed that hiding q words in an image. The specific hiding steps are as follows and as shown in Figure 6 as part of the sender:

Step 1. The method of the maximum matching word segment is used to segment the secret information S into n secret information fragments, namely $S = \{s_1, s_2, s_3, \ldots, s_n\}$.. If n cannot be divisible by q, then add "的" to the end of the secret message until n can be divisible by q.

Input: receiver's ID, System time, Seceret information (I,T,S)
Output: Stego-images

Begin

(1) Segment S, get $S=\{s_1,s_2,s_3,\ldots,s_n\}$;
(2) Obtain the label sequence $P=\{p_1',p_2',p_3',\ldots,p_n'\}$;
(3) Query the mapping relationship $L=\{l_1,l_2,l_3,\ldots,l_k\}$, get visual words $W=\{w_1,w_2,w_3,\ldots,w_n\}$;
(4) Divide the W into n/q group.
(5) Search (w,p') on the basis of the index each group, calculate the intersection to select an image, and ensure $v_1<v_2<v_3<,\ldots,v_{n/q}$, if there is no one to meet, S_t will be replaced by synonym or homonym;
(6) All the selected images are the stego-images.

End.

Figure 6. Pseudocode of information hiding

Step 2. The sender obtains the identity ID information I of the receiver, the current time T of the system, and selects the first n tags from the tag sequence which shared in advance to form the original label sequence $P_0=\{p_1,p_2,p_3,\ldots,p_n\}$. Then, the original tag sequence P_0 is randomly processed by using the hash function $H_P(I,T,P_0)$ to obtain the label sequence in current communication, namely $P=\{p_1',p_2',p_3',\ldots,p_n'\}$.

Step 3. The sender queries the mapping relation $L=\{l_1,l_2,l_3,\ldots,l_k\}$ to get the visual words set $W=\{w_1,w_2,w_3,\ldots,w_n\}$, which corresponding to the secret information fragments.

Step 4. According to the search condition (w,p'), on the basis of the multi-level inverted index structure, the first layer is searched first, and the visual word corresponding to the secret information fragment are found, that is w. Second, retrieve the next level of the visual word, find the pre-determined label, that is p'. At this time, the sender will get an image set that satisfies the condition (w,p'). When the number of searches reaches q every time, seek an intersection and select one image as a stego-image in the intersection. If the image corresponding to the secret information cannot be found, the secret fragment will be replaced by homonym or synonym.

In order to facilitate the receiver to determine the order of the images, the visual words value of the stego-images $V=\{v_1,v_2,v_3,\ldots,v_{n/q}\}$ should satisfy the relationship of $v_1<v_2<v_3<,\ldots,v_{n/q}$. That is to say, we record the visual word value of the image when we get the first stego-image. In the following process, to keep the visual word value of the next stego-image is biger than the previous one. The visual word value of these images will not change. Therefore, this method can effectively resist the problem of out-of-order image, so that the receiver can extract the secret information accurately.

3.2 Information Extracting Method

Most of the work of this algorithm is carried out by the sender, and the receiver's work is relatively simple. The specific steps are as follows and as shown in Figure 7 as part of the receiver:

Input: receiver's ID, System time, Stego-images
Output: Secret information

Begin

(1) Image normalization, to keep the stego-images consistent with the index;
(2) Obtain the label sequence $P=\{p_1',p_2',p_3',\ldots,p_n'\}$;
(3) Sort the received images, to ensure $v_1<v_2<v_3<,\ldots,v_{n/q}$;
(4) Use the BOW model and the label sequence P to get the $W=\{w_1,w_2,w_3,\ldots,w_n\}$;
(5) Query the mapping relationship $L=\{l_1,l_2,l_3,\ldots,l_k\}$, get secret information fragments $\{s_1,s_2,s_3,\ldots,s_n\}$
(6) Connect all the fragments to get the secret information.

End.

Figure 7. Pseudocode of information extraction

Step 1. To resist rotation and zoom attacks, we first calculate the main direction of all received images, rotate the direction to the horizontal direction, and then scale the image to a unified size, keeping the image consistent with the index.

Step 2. First, the identity ID information I of the receiver and the number of images n/q is obtained, and the T' is the time that the time of receiving the images minus the average delay. Then selects the first n labels from the label sequence which shared in advance to form the original tag sequence $P_0=\{p_1,p_2,p_3,\ldots,p_n\}$. After that, the original tag sequence P_0 is randomly processed by using the hash function $H_P(I,T',P_0)$ to obtain the tag sequence in current communication, namely $P=\{p_1',p_2',p_3',\ldots,p_n'\}$. In this method, T and T' are in the same interval.

Step 3. Due to network latency and other intentional or unintentional scrambling attacks, the received images may in a different order from the sender's. But the sender has ensured that the visual words value of the stego-images meet the conditions $v_1<v_2<v_3<,\ldots,v_{n/q}$, so sort the received images according to the visual word value at first. And then extract the sub-images one by one according to the label $P=\{p_1',p_2',p_3',\ldots,p_n'\}$ to get the visual words collection $W=\{w_1,w_2,w_3,\ldots,w_n\}$.

Step 4. Query the mapping $L=\{l_1,l_2,l_3,\ldots,l_k\}$ to get the secret information fragment $W=\{s_1,s_2,s_3,\ldots,s_n\}$

corresponding to the collection of visual words $W=\{w_1,w_2,w_3,\ldots,w_n\}$. Finally connect all the fragments in sequence to get the text information hidden in the images.

4 Experiment and Analysis

In this paper, all experiments in Visual Studio 2013 environment, using functions provided by the OpenCV 2.4.11. The codebook used in the experiment containing 10000 visual words obtained by the Holidays data set [27]. The secret information is 100 sentences.

4.1 Hiding Capacity

In this section, we tested the hiding capacity when $q=2$ and $q=3$. At the same time, we tested the capacity of the literature [8-9, 19-20]. The capacity in this article refers to the number of bits that one image can represent. The experimental results are as Table 3.

Table 3. The experimental result of the hiding capacity

Methods	capacity (bits · carrier^{-1})
literature [8]	8
literature [19]	8
literature [9]	16
literature [20]	36
Proposed Methods q=2	44
Proposed Methods q=3	68

As shown in Table 3, the hiding capacity of this method increases as q increases. However, with the increase of q, the images that meet the conditions will be more difficult to find.

4.2 Anti-detectability

This article transforms information hiding into a search for images that meet certain conditions based on the mapping. And there is no modification to the dense image during the communication. So it can fundamentally resist the existing steganalysis algorithm and the human eye detection.

4.3 Security Analysis

In this article, we have multiple protection of the secret information. First, we use the secret key to dynamically select natural images as stego-images which without any modification. Compared with the traditional information hiding method, the proposed method can be more covert to communicate, because it is difficult to cause the attacker's suspicion. Moreover, even if the attacker has suspected that the transmitted image contains secret information, but the attacker is hard to determine the sequence of labels P_0 that was agreed in advance and kept strictly confidential. What's more, in the communication, P_0 will be converted to P through a hash function. So that the attacker cannot guess the tag's position according to stego-images. Finally, even if the attacker gets P by luck, they still cannot obtain P_0, since the hash function is unidirectional. In summary, this algorithm has a good security, it is difficult to be cracked by malicious attackers.

5 Conclusion

The essence of our proposed DCSF is to establish the mapping relations between the secret information and the features. In addition, the information hiding is converted into retrieving images that meet certain criteria. At the same time. By taking into account the security and anti-attack, the "label + keyword" is exploited to retrieve the image. We hide multiple words in an image to improve hidden capacity. The method replaced by synonyms or homonyms is utilized to improve the success rate of conceal. Experimental and theoretical analysis show that our method not only effectively improves the capacity and success rate of conceal, but also has better resistance to the existing algorithm. This is mainly due to the transmitted image is natural without any modification.

Acknowledgments

This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant U1536206, U1405254, 61772283, 61602253, 61672294, 61502242; by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925 and BK20151530; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China; by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under grant number KYCX18_1016.

References

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, *Signal Processing*, Vol. 90, No. 3, pp. 727-752, March, 2010.

[2] A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne, Electronic Watermark, *Digital Image Computing, Techniques and Applications*, Sydney, Australia, 1993, pp. 666-673.

[3] C. Yang, C. Weng, S. Wang, H. Sun, Adaptive Data Hiding

in Edge Areas of Images with Spatial LSB Domain Systems, *IEEE Transactions on Information Forensics & Security*, Vol. 3, No. 3, pp. 488-497, September, 2008.

[4] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Reversible Data Hiding, *IEEE Transactions on Circuits & Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, March, 2006.

[5] J. J. K. O. Ruanaidh, W. J. Dowling, F. M. Boland, Phase Watermarking of Digital Images, *International Conference on Image Processing*, Lausanne, Switzerland, 1996, pp. 239-242.

[6] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, December, 1997.

[7] M. S. Hsieh, D. C. Tseng, Y. H. Huang, Hiding Digital Watermarks using Multiresolution Wavelet Transform, *IEEE Transactions on Industrial Electronics*, Vol. 48, No. 5, pp. 875-882, October, 2001.

[8] Z. Zhou, Q. M. J. Wu, C. Yang, X. Sun, Z. Pan, Coverless Image Steganography Using Histograms of Oriented Gradients-based Hashing Algorithm, *Journal of Internet Technology*, Vol. 18, No. 5, pp. 1177-1184, September, 2017.

[9] X. Chen, H. Sun, Y. Tobe, Z. Zhou, X. Sun, Coverless Information Hiding Method Based on the Chinese Mathematical Expression, *International Conference on Cloud Computing and Security*, Nanjing, China, 2015, pp. 133-143.

[10] J. Zhang, L. Wang, H. Lin, Coverless Text Information Hiding Method Based on the Rank Map, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 427-434, March, 2017.

[11] X. Chen, S. Chen, Y. Wu, Coverless Information Hiding Method Based on the Chinese Character Encoding, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 313-320, March, 2017.

[12] Z. Zhou, Y. Mu, C. Yang, N. Zhao, Coverless Multi-keywords Information Hiding Method Based on Text, *International Journal of Security and Its Applications*, Vol. 10, No. 9, pp. 309-320, September, 2016.

[13] H. Sun, R. Grishman, Y. Wang, Active Learning Based Named Entity Recognition and Its Application in Natural Language Coverless Information Hiding, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 443-451, March, 2017.

[14] Z. Zhou, Y. Wang, Q. M. J. Wu, C. Yang, X. Sun, Effective and Efficient Global Context Verification for Image Copy Detection, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 1, pp. 48-63, January, 2017.

[15] Z. Zhou, C. Yang, B. Chen, X. Sun, Q. Liu, Q. M. J. Wu, Effective and Efficient Image Copy Detection with Resistance to Arbitrary Rotation, *IEICE Transactions on Information & Systems*, Vol. E99. D, No. 6, pp. 1531-1540, June, 2016.

[16] Z. Zhou, Q. M. J. Wu, F. Huang, X. Sun, Fast and Accurate Near-duplicate Image Elimination for Visual Sensor Networks, *International Journal of Distributed Sensor Networks*, Vol. 13, No. 2, pp. 1-12, February, 2017.

[17] Z. Xia, Y. Zhu, X. Sun, Z. Qin, K. Ren, Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing, *IEEE Transactions on Cloud Computing*, Vol. 6, No. 1, pp. 276-286, January-March, 2018.

[18] Z. Xia, N. Xiong, A. Vasilakos, X. Sun, EPCBIR: An Efficient and Privacy-preserving Content-based Image Retrieval Scheme in Cloud Computing, *Information Sciences*, Vol. 387, pp. 195-204, May, 2017.

[19] C. Yuan, Z. Xia, X. Sun, Coverless Image Steganography Based on SIFT and BOF, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 435-442, March, 2017.

[20] Y. Cao, Z. Zhou, X. Sun, C. Gao, Coverless Information Hiding Based on the Molecular Structure Images of Material, *Computers Materials & Continua*, Vol. 54, No. 2, pp. 197-207, January, 2018.

[21] Z. Zhou, Y. Mu, Q. M. J. Wu, Coverless Image Steganography Using Partial-Duplicate Image Retrieval, in: A. Di Nola (Ed.), *Soft Computing*, Spring, Berlin, 2018, pp. 1-12.

[22] R. Gurusamy, V. Subramaniam, A Machine Learning Approach for MRI Brain Tumor Classification, *Computers Materials & Continua*, Vol. 53, No. 2, pp. 91-108, January, 2017.

[23] C. Yuan, X. Li, Q. M. J. Wu, J. Li, X. Sun, Fingerprint Liveness Detection from Different Fingerprint Materials using Convolutional Neural Network and Principal Component Analysis, *Computers Materials & Continua*, Vol. 53, No. 4, pp. 357-371, January, 2017.

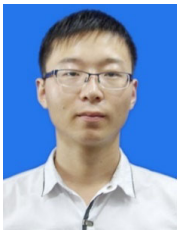
[24] M. Liu, M. Zhang, J. Liu, Y. Zhang, Y. Ke, *Coverless Information Hiding based on Generative Adversarial Networks*, arXiv:1712.06951v1, December, 2017.

[25] J. A. Hartigan, M. A. Wong, Algorithm AS 136: A K-means Clustering Algorithm, *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, Vol. 28, No. 1, pp. 100-108, January, 1979.

[26] D. G. Lowe, Distinctive Image Features from Scale-Invariant Keypoints, *International Journal of Computer Vision*, Vol. 60, No. 2, pp. 91-110, November, 2004.

[27] H. Jegou, M. Douze, C. Schmid, Hamming Embedding and Weak Geometric Consistency for Large Scale Image Search, *European Conference on Computer Vision*, Marseille, France, 2008, pp. 304-317.

Biographies



Yi Cao received the B.S. degree from Nanjing University of Information Science & Technology in 2016, China. He is currently working towards the Ph.D. degree in Nanjing University of Information Science & Technology, China. His research interest includes network and information security.

Zhili Zhou received the B.S. degree from Hubei University in 2007, and the M.S. and Ph.D. degrees from Hunan University, in 2010 and 2014, respectively. He is an Associate Professor with the School of

Computer and Software, NUIST, China. His current research interests include near-duplicate image/video retrieval, coverless information hiding.

Ching-Nung Yang received the B.S. and M.S. degrees from National Chiao Tung University, in 1983 and 1985, respectively, and the Ph.D. degree from National Cheng Kung University, in 1997. He is a Full Professor in National Dong Hwa University, Taiwan. His research interests include coding theory, information security, and cryptography.

Xingming Sun received his B.S. from Hunan Normal University, in 1984, M.S. from Dalian University of Science and Technology, China, in 1988, and Ph.D. from Computing Science from Fudan University, China, in 2001. He is a Professor in NUIST. His research interests include network and information security and digital watermarking.