Copyright © 2018 Tech Science Press CMC, vol.54, no.2, pp.197-207, 2018

Coverless Information Hiding Based on the Molecular Structure Images of Material

Yi Cao[1, 2], Zhili Zhou[1, 2, 3], Xingming Sun[1, 2] and Chongzhi Gao[4, *]

Abstract: The traditional information hiding methods embed the secret information by modifying the carrier, which will inevitably leave traces of modification on the carrier. In this way, it is hard to resist the detection of steganalysis algorithm. To address this problem, the concept of coverless information hiding was proposed. Coverless information hiding can effectively resist steganalysis algorithm, since it uses unmodified natural stego-carriers to represent and convey confidential information. However, the state-of-the-arts method has a low hidden capacity, which makes it less appealing. Because the pixel values of different regions of the molecular structure images of material (MSIM) are usually different, this paper proposes a novel coverless information hiding method based on MSIM, which utilizes the average value of sub-image's pixels to represent the secret information, according to the mapping between pixel value intervals and secret information. In addition, we employ a pseudo-random label sequence that is used to determine the position of sub-images to improve the security of the method. And the histogram of the Bag of words model (BOW) is used to determine the number of sub-images in the image that convey secret information. Moreover, to improve the retrieval efficiency, we built a multi-level inverted index structure. Furthermore, the proposed method can also be used for other natural images. Compared with the state-of-the-arts, experimental results and analysis manifest that our method has better performance in anti-steganalysis, security and capacity.

Keywords: Coverless information hiding, molecular structure images of material, pixel value, inverted index, image retrieval, bag of words model.

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Ning Liu Road, NO. 219, Nanjing, 210044, China.

[2] Jiangsu Engineering Centre of Network Monitoring, Ning Liu Road, No. 219, Nanjing, 210044, China.

[3] Department of Electrical and computer Engineering, University of Windsor, 401 Sunset Avenue, Windsor, ON, Canada N9B 3P4.

[4] School of Computer Science, Guangzhou University, Waihuanxi Road, No. 230, Guangzhou, 510006, China.

* Corresponding author: Chongzhi Gao, Email: czgao@gzhu.edu.cn.

CMC.doi:10.3970/cmc.2018.054.197 www.techscience.com/cmc

1 Introduction

Information hiding has been a crucial research area in the field of information security. According to different application scenarios, information hiding can be divided into digital watermarking [Wang, Lian and Shi (2017)] and steganography [Xiong, Xu and Shi (2017)]. With the rapid development of network and electronic technology, the number of digital files has exploded, which provides a rich carrier for information hiding. Traditional steganography embeds secret information by modifying digital carriers such as images, videos, audio, text, in accordance with certain rules [Fridrich (2009)]. For example, there are two types of information hiding methods based on images. One is Spatial Domain methods, such as Yang's adaptive LSB (least significant bit) method which uses pixel-value difference (PVD) to embed secret information [Yang, Weng and Wang (2008)]. The other is the transform domain methods which embed information by modifying the coefficients of the image frequency domain transform, such as DWT (discrete wavelet transform) [Lin, Horng and Kao (2008)], DCT (discrete cosine transform) [Pevny and Fridrich (2013)] and DFT (discrete Fourier transform) [Ruanaidh, Dowling and Boland (2008)]. However, in this way, it is unavoidable to leave traces on the stego-carrier, so these methods cannot effectively resist the detection of steganalysis algorithms.

In order to fundamentally resist the steganalysis, coverless information hiding came into being [Chen, Sun and Tobe (2015); Chen, Chen and Wu (2017); Zhou, Sun and Harit (2015)]. Coverless information hiding does not mean that the carrier is not needed. However, compared with the traditional methods, coverless information hiding method directly utilize the contents of the carrier itself to represent the secret information. The development of big data and cloud computing technology has facilitated the coverless information hiding [Li, Zhang, Chen et al. (2018); Li, Li, Huang et al. (2017); Gao, Cheng, Li et al. (2018)]. Recently, the existing coverless information hiding can be categorized into two kinds of methods: text-based methods and image-based ones, depending on the type of carrier transmitted. For text-based coverless information hiding, current methods mainly search for the texts containing the secret information according to a certain rule as the stego-texts, and determine the location of the secret information by using labels. For example, Chen's method uses Chinese mathematical expression as labels to determine the location of secret information in stego-texts, and then retrieves the eligible texts from the text big data as stego-texts [Chen, Sun and Tobe (2015)]. This method is resistant to steganalysis algorithms that rely on detecting traces of modifications as Chen's method uses unmodified natural text to convey confidential information. After that, a number of similar methods emerged. Such as Chen's another method utilizes the LSBs of the character's Unicode as labels [Chen, Chen and Wu (2017)] and in Zhou's method, a stego-text can contain more than one secret messages [Zhou, Sun and Harit (2015)]. In addition, H. Sun et al. proposed an approach that uses named entities to represent secret information [Sun, Grishman and Wang (2017)], and Zhang's method utilizes rank map to obtain the stego-texts [Zhang, Shen and Wang (2017)]. The current image-based coverless information hiding methods are similar to image retrieval and fingerprint liveness detection techniques [Zhou, Wu, Huang et al. (2017); Zhou, Wu and Sun (2017); Zhou, Yang, Chen et al. (2016); Zhou, Wang, Wu et al. (2017); Yuan (2017)]. These methods use the natural images retrieved from the image library to express the secret information. For example, the hash sequence of the original images in Zhou's method is used to represent the secret information [Zhou, Sun and Harit (2015)]. After that, Yuan's method [Yuan, Xia and Sun (2017)] hashes the SIFT features clustered by Bag of feather to get a binary string that can represent the secret information. Nowadays, the latest method is to hash the direction of the SIFT feature to obtain the same binary sequence as the secret information [Zheng, Wang and Ling (2017)]. Because the inherent characteristics of the image are used to represent the secret information and they do not modify the image, these methods can also resist the attack of the steganalysis algorithm.

However, as shown in Tab. 1, there is little hidden capacity for current coverless information hiding. The main reason is that an image can only generate a fixed-length binary string, and the selected image features are not evenly distributed. Although Zhang's approach increased capacity, it required a modified image to convey additional information.

Table 1: The capacity of current methods

Methods	capacity (bits $\cdot$ $carrier^{-1}$)
Zhou's method	8
Yuan's method	8
Zheng's method	18

In order to improve the capacity while ensuring the security and anti-steganalysis, this paper proposes a novel coverless information hiding method based on the molecular structure images of material (MSIM). As shown in Fig. 1, we divide the image into several blocks, and then the average pixel values of the sub-images are used to represent secret information fragment. Because the MSIM consists of atoms of various colors, and the average pixel values of sub-images of these model images can effectively convey the secret information.

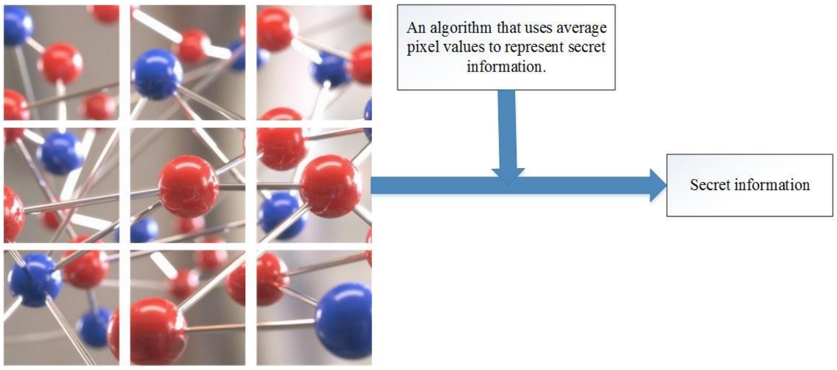

An algorithm that uses average pixel values to represent secret information.
Secret information

Figure 1: Secret information represented by the molecular structure image of material

Compared with the previous methods, the average values of MSIM pixels is more general. So that, it is easier to use multiple sub-images in one image to express the secret information fragments. This method not only improves the hidden capacity of each carrier while ensuring the security and anti-steganalysis, but also reduces the difficulty of retrieval. What's more, the proposed method can also be used for other natural images. However, if we use other natural images to deliver confidential information, we need to classify the images using machine learning [Gurusamy and Subramaniam (2017); Yang and Wu (2016); Yang and Wu (2016)] to ensure that similar images are used in communications.

The rest of this article is organized as follows. The proposed method is described in detail in the section 2. The results of the experiment and analysis are shown in section 3. The section 4 is a conclusion.

2 The proposed coverless information hiding method

The framework of proposed method is illustrated as Fig. 2.

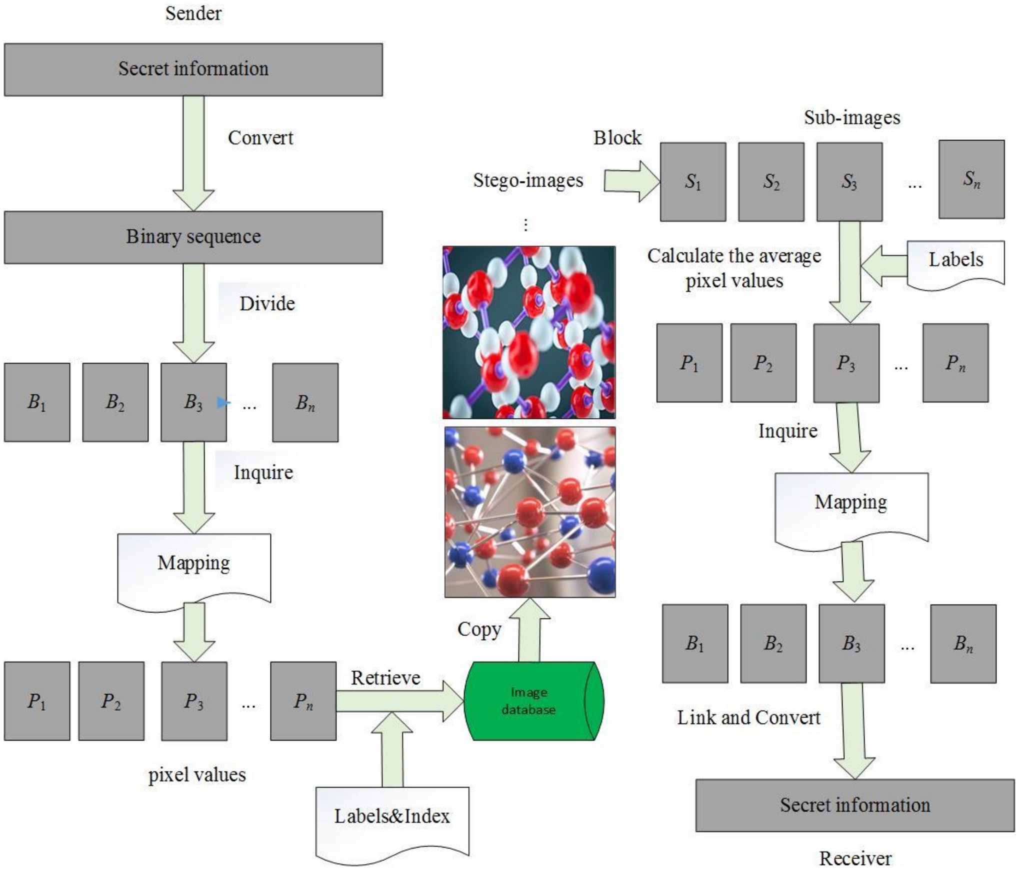


Figure 2: The framework of proposed method

Compared with the traditional information hiding methods, we do not make any modification to the stego-images. We search the appropriate images to express the secret information. The proposed method transforms secret information into a binary string at first. Then, the binary string is segmented according to the mapping relationship to obtain a binary sequence that can be represented by the average pixel value of the sub-images. In this article, we use a sub-image to represent 4-bit binary. We utilize labels to determine the location of the sub-images that represent the binary sequence. In addition, we use a multi-level inverted index structure to improve search efficiency. In the process of indexing, the bag of words model (BOW) [Li and Perona (2005); Zhou (2017)] is used to cluster the SIFT features [Lowe (2004)] of the image to get the frequency histogram of visual words. Moreover, considering that each communication may convey more than one image, we use the peak of the frequency histogram of visual words to rank the images. Finally, we use the visual word's ID corresponding to the peak of the frequency histogram to determine the number of sub-images that represent the binary sequence in an image.

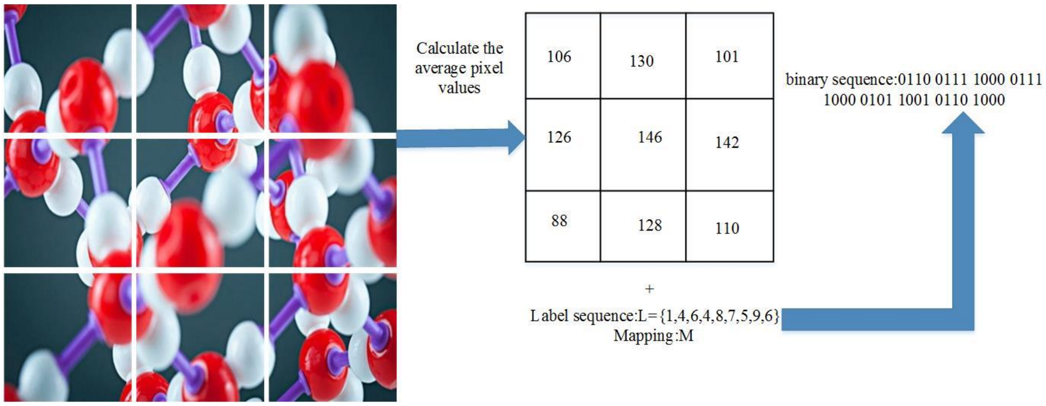
2.1 Representation of secret information

In order to represent the secret information with the natural images, we need to establish the mapping between the binary sequences and the average pixel values of the sub-images. The mapping relationship is not unique and can be set according to actual needs. For example, if the pixel values are divided into two parts, it can represent 0 and 1, respectively; If the pixel values is divided into four parts, it can represent 00, 01, 10 and 11 respectively. And so on. As shown in Tab. 2, we set up an initial mapping relationship, marked as M. In this paper, we divide the pixel values of 0-255 into 16 intervals, so each interval can correspond to a 4-bit binary sequence.

Table 2: Mapping relationship

Intervals	Binary sequence	Intervals	Binary sequence
0-15	0000	128-143	1000
16-31	0001	144-159	1001
32-47	0010	160-175	1010
48-63	0011	176-191	1011
64-79	0100	192-207	1100
80-95	0101	208-223	1101
96-111	0110	224-239	1110
112-127	0111	240-255	1111

Since we use the average pixel values of the sub-images to represent the secret information, we need to determine which sub-images represent the secret information in an image. In our framework, images are divided into $x \times y$ blocks, and these blocks are marked as $\{1, 2, 3, \dots, x \times y\}$, which is the label of this method, in the order of raster scanning. Then, we define an initial label sequence, denoted by $L = \{l_1, l_2, l_3, \cdots, l_k\}, l_k \in \{1, 2, 3, \dots, x \times y\}$. Next, we can use natural images to represent the secret information. As shown in Fig. 3, we can represent the binary sequence using the molecular structure image of material. As we can see, label sequences are pseudo-randomly selected during communication. In the process of transmission, to ensure the security of the proposed method, the mapping relationship and label sequence will be pseudo-randomized according to the user identity.


Calculate the average pixel values
binary sequence:0110 0111 1000 0111 1000 0101 1001 0110 1000
+
Label sequence:L={1,4,6,4,8,7,5,9,6}
Mapping:M

106	130	101
126	146	142
88	128	110

Figure 3: Representation of binary sequence

2.2 Multi-level inverted index structure

The core of coverless information hiding is to search the stego-images quickly. However, it would be very time-consuming if we retrieve qualified stego-images in the image database directly. In order to improve the retrieval efficiency, we establish the multi-level inverted index structure as shown in Fig. 4.

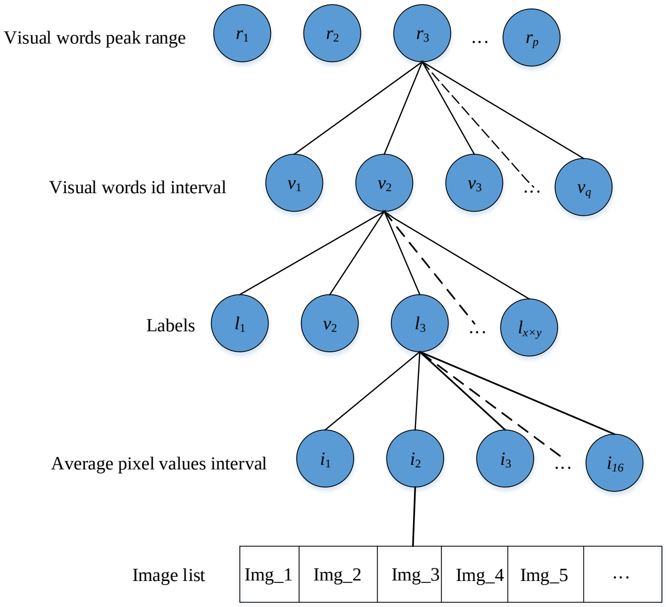


Figure 4: Multi-level inverted index structure

The first level of the index is the peak of the frequency histogram of visual words, denoted as $R = \{r_1, r_2, r_3, \cdots, r_p\}$. We first calculate the peak values of the frequency histogram of the images in the database and divide them into p ranges. The second level is the visual word's ID corresponding to the peak of the frequency histogram. In the index, we divide the visual word's ID into q segments, denoted as $V = \{v_1, v_2, v_3, \cdots, v_q\}$.The third level is labels, denoted as $L = \{l_1, l_2, l_3, \cdots, l_{x\times y}\}$. The fourth level is the average pixel values interval, denoted as $I = \{i_1, i_2, i_3, \cdots, i_{16}\}$. The fifth level is the list of images that satisfy the condition (R, V, L, I). In addition, the images have been normalized in direction and scale before indexing.

2.3 Process of information hiding

In this paper, we use the average pixel values of the sub-images to represent the binary sequence. The process of information hiding is illustrated in Fig. 5.

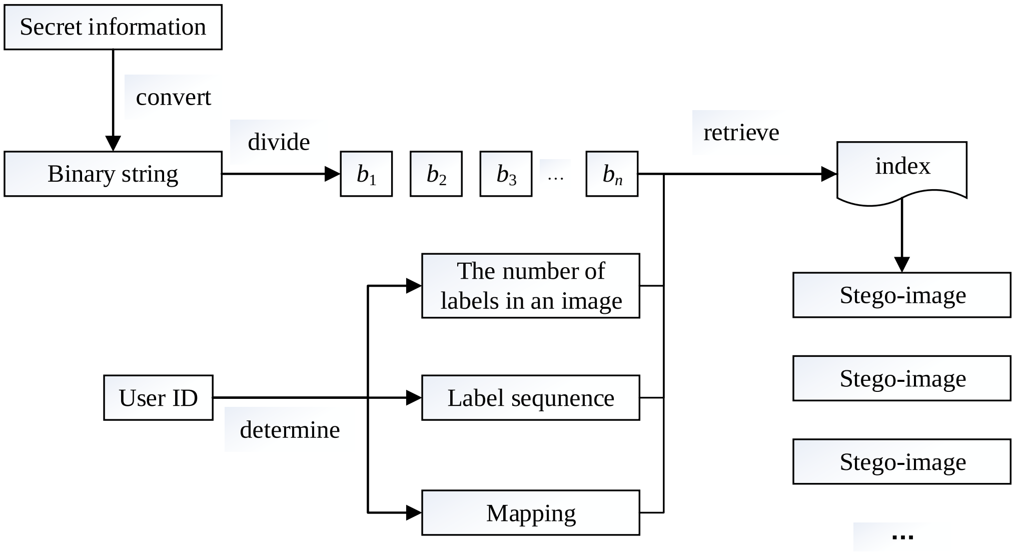


Figure 5: Process of information hiding

Step 1: We convert the secret message to a binary string at first. Since the average pixel value of each sub-image represents 4-bit binary, we divide the binary string into segments contain 4-bit binary, donated as $B = \{b_1, b_2, b_3, \cdots, b_n\}$. If the length of the binary string cannot be divisible by 4, then we add meaningless redundant information after the binary string.

Step 2: In this paper, the receiver's identity information is similar to the secret key, denoted as$U$. First, we use hash function $H_v(U)$ to determine the number of sub-images that represent confidential information in an image, denoted as $c = H_v(U)$. If n can be divisible by c, we use $(\frac{n}{c})$ stego-images to represent the secret information. If n cannot be divisible by c, we use $(\lfloor\frac{n}{c}\rfloor)$ stego-images to represent $((\lfloor\frac{n}{c}\rfloor) \times c)$ binary fragments, and use another stego-image to represent remaining binary fragments. Next, we use the hash function $H_l(U)$ to pseudo-random process the first n labels of the initial label sequence L

to obtain a label sequence $L' = \{l'_1, l'_2, l'_3, \cdots, l'_n\}$. Finally, we use the hash function $H_M(U)$ to pseudo-random process the mapping M to obtain the mapping M' for the receiver.

Step 3: Considering that n may not be divisible by c, we use V to determine the number of sub-images that represent the secret information in the last stego-image. In addition to the last image, we use the condition(R, L', I) to retrieve the index structure. We take the intersection of every c times retrieval, to get a stego-image. We use the same method, using condition (R, V, L', I) to retrieve the last image containing the secret. Obviously, the peak values of the frequency histogram of the stego-images satisfies $\{r_1 < r_2 < r_3 < \cdots < r_n, n \leq p\}$. Finally, all stego-images are sent to the receiver.

2.4 Process of information extraction

Information extraction is a hidden reverse process. The receiver first sorts the received stego-images. Next, the receiver uses hash function $H_v(U)$ to determine the number of sub-images that represent confidential information in a stego-image and recalculates the number of binary fragments represented by the last image. In this way, n can be obtained. After that, the receiver obtains the label sequence and the mapping relationship in the same way. Finally, the receiver calculates the average pixel values of the label location sub-images and obtains the secret information according to the mapping relationship.

3 Experiment and Analysis

All the experiments in this paper have been done in the Visual Studio 2013. The experiment and analysis include hiding capacity, anti-detectability, security.

3.1 Capacity

This paper uses the average pixel value of the sub-images to represent binary bit sequences. In the experiment, we used 9 sub-images in a stego-image to represent the binary sequence. At the same time, each sub-image represents 4-bit binary. The experimental results are as follows.

Table 3: The capacity of proposed methods

Methods	capacity (bits $\cdot$ $carrier^{-1}$)
Zhou's method	8
Yuan's method	8
Zheng's method	18
Our method	36

As Tab. 3 shows, the hidden capacity of this article doubles compared to the state-of-the-arts method. Moreover, the capacity of proposed method is not fixed, it can be adjusted according to actual needs. If the image database is large enough, each sub-image of the stego-images can represent more binary bits. Conversely, if the image database is relatively small, each sub-image can represent less binary for information hiding. The less the binary representation of each sub-image, the easier it is to retrieve matching images in the database.

3.2 Anti-detectability

In this paper, we convert the secret information into a binary string. Then, we use the average pixel value of the sub-images to represent the binary fragments, according to a mapping. This method, using unmodified natural images as stego-images, can fundamentally resist existing steganalysis algorithms. Moreover, stego-images of each communication are the same type, so it can resist the detection of the human eye.

3.3 Security

Prior to communication, we pseudo-randomized the mapping relationship and label sequence according to the receiver's identity. Therefore, for the same secret information, different recipients will get different stego-images. Even if an attacker suspects the image is a stego-image, it is difficult to extract it correctly. Finally, even if the attackers obtain the stego-images and the secret information at the same time, the attacker can hardly obtain the initial label sequence and the mapping relationship because of the one-way hash function. Therefore, the proposed method has high security.

4 Conclusion

This paper transforms the coverless information hiding into image retrieval through the mapping relationship between the binary fragment and the average pixel value of the sub-image. The proposed coverless information hiding method utilizes the unmodified natural molecular structure images of material to express the secret information, so it can fundamentally resist the steganalysis algorithm. Compared with the image hash value, the average pixel values distribution of the sub-images is more general. In addition, the images have been normalized in direction and scale before indexing. Furthermore, we use random label sequences and mapping relationship based on the receiver's identity. Therefore, the method in this paper has good security and robustness. Experimental results show that the hidden capacity of proposed method doubles compared to the Zheng’s method that has the highest capacity. However, compared with the traditional methods, the capacity of coverless information hiding is still very low. In future work, we will strive to increase capacity while ensuring security and robustness.

Acknowledgement: This work is supported, in part, by the National Natural Science Foundation of China under grant numbers U1536206, U1405254, 61772283, 61602253, 61672294, 61502242; in part, by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925 and BK20151530; 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.

References

Chen, X.; Chen, S.; Wu, Y. (2017): Coverless information hiding method based on the chinese character encoding. *Journal of Internet Technology*, vol. 18, no. 2, pp.133-143.

Chen, X.; Sun, H.; Tobe, Y. (2015): Coverless information hiding method based on the chinese mathematical expression. *International Conference on Cloud Computing and Security*, pp.133-143.

Fridrich, J. (2009): *Steganography in digital media: principles, algorithms, and applications*, Cambridge University Press.

Gao, C.; Cheng, Q.; Li, X.; Xia, S. (2018): Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. *Cluster Computing*, DOI: 10.1007/s10586-017-1649-y.

Gurusamy, R.; Subramaniam, V. (2017): A machine learning approach for mri brain tumor classification. *Computers, Materials & Continua*, vol. 53, no. 2, pp. 91-108.

Li, F.; Perona, P. (2005): A bayesian hierarchical model for learning natural scene categories. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, vol. 2, pp. 524-531.

Li, J.; Zhang, Y.; Chen, X.; Xiang, Y. (2018): Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, doi: 10.1016/j.cose.2017.08.007.

Li, P.; Li, J.; Huang, Z.; Gao, C.; Chen, W.; Chen, K. (2017): Privacy-preserving outsourced classification in cloud computing. *Cluster Computing*, doi: 10.1007/s10586-017-0849-9.

Lin, W.; Horng, S.; Kao, T. (2008): An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp.746-757.

Lowe, D. (2004): Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110.

Pevny, T.; Fridrich, J. (2013): Merging markov and DCT features for multi-class JPEG steganalysis. *Proceedings of SPIE-The International Society for Optical Engineering*, vol. 3, pp. 650503-650503.

Ruanaidh, J.; Dowling, W.; Boland, F. (2008): Phase watermarking of digital images. *International Conference on Image Processing. Proceedings (IEEE)*, vol. 3, pp. 239-242.

Sun, H.; Grishman, R.; Wang, Y. (2017): 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.

Wang, J.; Lian, S.; Shi, Y. (2017): Hybrid multiplicative multi-watermarking in DWT domain. *Multidimensional Systems and Signal Processing*, vol. 28, no. 2, pp. 617-636.

Xiong, L.; Xu, Z.; Shi, Y. (2017): An integer wavelet transform based scheme for reversible data hiding in encrypted images. *Multidimensional Systems and Signal Processing*, DOI: 10.1007/s11045-017-0497-5.

Yang, Y.; Wu, Q. (2016): Extreme learning machine with subnetwork hidden nodes for regression and classification. *IEEE Transactions on Cybernetics*, vol. 46, no. 12, pp. 2885-2898.

Yang, Y.; Wu, Q. (2016): Multilayer extreme learning machine with subnetwork nodes for representation learning. *IEEE Transactions on Cybernetics*, vol. 46, no. 11, pp. 2570-2583.

Yang, C.; Weng, C.; Wang, S. (2008): 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.

Yuan, C.; Li, X.; Wu, Q.; Li, J.; Sun, X. (2017): Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. *Computers, Materials & Continua*, vol. 53, no. 3, pp. 357-371.

Yuan, C.; Xia, Z.; Sun, X. (2017): Coverless image steganography based on SIFT and BOF. *Journal of Internet Technology*, vol. 18, no. 2, pp. 435-442.

Zhang, J.; Shen, J.; Wang, L. (2017): Coverless text information hiding method based on the word rank map. *Journal of Internet Technology*, vol. 18, no. 2, pp. 427-434.

Zheng, S.; Wang, L.; Ling, B. (2017): Coverless information hiding based on robust image hashing. *International Conference on Cloud Computing and Security*, pp. 536-547.

Zhou, Z.; Sun, H.; Harit, R. (2015): Coverless image steganography without embedding. *International Conference on Cloud Computing and Security*, pp. 123-132.

Zhou, Z.; Wang, Y.; Wu, Q.; Yang, C.; Sun, X. (2017): Effective and efficient global context verification for image copy detection. *IEEE Transactions on Information Forensics and Security*, vol. 12 no. 1, pp. 48-63.

Zhou, Z.; Wu, Q.; Huang, F.; Sun, X. (2017): Fast and accurate near-duplicate image elimination for visual sensor networks. *International Journal of Distributed Sensor Networks*, vol. 13, no. 2.

Zhou, Z.; Wu, Q.; Sun, X. (2017): Encoding multiple contextual clues for partial-duplicate image retrieval. *Pattern Recognition Letters, doi*: https://doi.org/10.1016/j.patrec.2017.08.01.

Zhou, Z.; Yang, C.; Chen, B.; Sun, X.; Liu, Q. et al. (2016): Effective and efficient image copy detection with resistance to arbitrary rotation. *IEICE Transactions on information and systems*, no. 6, pp. 1531-1540.