 JIHPP, vol.1, no.2, pp.49-60, 2019

Coverless Image Steganography Method Based on Feature Selection

Anqi Qiu[1, 2], Xianyi Chen[1, 2], Xingming Sun[1, 2, *], Shuai Wang[3] and Guo Wei[4]

Abstract: A new information hiding technology named coverless information hiding is proposed. It uses original natural images as stego images to represent secret information. The focus of coverless image steganography method is how to represent image features and establish a map relationship between image feature and the secret information. In this paper, we use three kinds of features which are Local Binary Pattern (LBP), the mean value of pixels and the variance value of pixels. On this basis, we realize the transmission of secret information. Firstly, the hash sequence of the original cover image is obtained according to the description of the feature, and then the sequence of the secret information and the hash sequence of the original cover image are matched one by one. If the values are not the same, the image blocks of the original cover image are replaced according to the secret information to get the stego image. This paper explores the effect of three features on the visual quality of stego image. Experimental results show that the feature LBP is the best.

Keywords: Coverless-image-steganography (CIS), feature, visual quality.

1 Introduction

Recently, most of the information hiding technology embed secret information into the complex texture objects of the cover [Meng, Steven, Wang et al. (2018)] by slight modification of the content and structure of the cover (digital image, video [Nie, Xu, Feng et al. (2018)] and audio). Traditional information hiding includes spatial domain methods, such as histogram modification [Du, Yin and Zhang (2018)], least significant bit substitution [Luo, Huang and Huang (2010)], and transform domain methods, such as discrete cosine transform [Huang, Huang and Shi (2012)] and discrete wavelet transform [Kang, Liu and He (2007)]. Although these steganography techniques can implement covert communication, the information of the cover is modified. It is inevitable to leave a trace of modification on the stego cover. Therefore, the stego cover is also difficult to resist the detection of existing steganalysis algorithms. In order to resist the detection of

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China.

[2] Jiangsu Engineering Centre of Network Monitoring, Nanjing, 210044, China.

[3] Department of Radiology and BRIC, University of North Carolina at Chapel Hill, North Carolina, 27599, USA.

[4] Mathematics and Computer Science, University of North Carolina at Pembroke, North Carolina, 28372, USA.

[*] Corresponding Author: Xingming Sun. Email: sunnudt@163.com.

steganalysis algorithms, experts from China proposed a new concept of "coverless information hiding" in May 2014.

"Coverless" does not mean that no cover is needed. Rather, compared with the traditional information hiding, it emphasizes that no other cover is needed, the secret information is used to generate/acquire the stego cover directly, and the cover is not modified. The secret information is transmitted by the natural normal cover. Because it transmits a natural cover, it can resist all existing steganalysis algorithms based on anomaly detection. Existing coverless information hiding methods are mostly used for text information hiding, because information hiding is based on the text which is used most frequently and widely as information cover when the concept of coverless information hiding is proposed. Compared with text information, image information is more abundant, and pixel values, textures, edges, contours, etc. can represent certain information. If some method can be used to convert some information in the image into fixed effective information, then the secret information can be transmitted through the image without embedding. Thereby coverless image steganography can be realized and can resist the steganalysis algorithms effectively.

Although the image consists of only the pixel, the type of information contained in the image is far from the pixel. In the past research on the image, various information contained in the image has been proposed, including SIFT, SURF, HOG, etc. which indicate that the image can express more than the image itself, which is not available in the text. This is why we have to study the coverless image information hiding method.

The existing methods have used many image features to represent secret information. However, these methods have relatively low hidden capacity, and as the hidden capacity increases in each image, the number of images which we need in the image database grows exponentially, besides there may be case where we cannot find the images that meet the condition. Based on this problem, this paper proposes a high-capacity coverless information hiding technology based on image feature. In this framework, we compare three kinds of features which are the LBP value of the center pixel, the mean value of all non-center pixels and the variance value of all non-center pixels. Firstly, we divide the original image into several image blocks and obtain the hash value of the image by hash method. Secondly, the secret information is converted into a secret binary sequence. The stego image can be synthesized with image blocks according to the secret information sequence. When the receiver receives the stego image, the secret information is extracted by using the same hash method. These three kinds of feature can all describe images, but the selection of feature may affect how to choose proper image blocks which have an effect on the visual quality of stego image. The paper focuses on getting a stego image with good visual quality to transmit information by comparing different features.

The rest of the paper is organized as follows: Related work is described in Section 2. Preliminaries are introduced in Section 3. The framework of coverless information hiding is introduced in Section 4. Experimental results and analysis are provided in Section 5. Finally, conclusions are drawn in Section 6.

2 Related work

The feature used in the paper Zhou et al. [Zhou, Sun and Harit (2015)] is pixel feature. For each image in the database, its hash sequence is obtained by a robust hash algorithm which uses average intensity of each block, and then all images are inverted according to their hash sequence. The index structure retrieves the image which hash sequence is the same as the secret information sequence as a stego image. Then the images are transmitted to the receiver. The receiver obtains a hash sequence through the same hash algorithm at the receiving end. These hash sequences are secret information. The capacity of the algorithm proposed in this paper is 8 bits.

In order to improve the hidden capacity, the paper Zheng et al. [Zheng, Wang and Ling (2017)] improved the hash algorithm and increased the length of the secret information. The capacity is 18 bits. The paper Yuan et al. [Yuan, Xia and Sun (2017)] proposed the coverless information hiding based on SIFT and BOF. The transmitted secret information is text. This method converts the secret information into binary, and then segments it. For the image, the image hash sequence is obtained through SIFT feature extraction and clustering. The hash sequence of the image is matched with the sequence of secret information. The image which hash sequence is the same as the secret information sequence is transmitted as a stego image to the receiver. The paper Zhou et al. [Zhou, Mu and Wu (2017)] which denoted as CIS-PDVR uses partial-duplicate visual retrieval to realize coverless information hiding, and the transmitted secret information is image. The algorithm is inspired by the find that some parts of the two images are similar. Some image blocks which are similar with the image blocks of the secret image can be obtained. An image which is similar to the secret image visually can be formed by combining similar image blocks. However, the secret information cannot be completely extracted correctly. As shown in the Fig. 1, the extracted secret information has a clear mosaic effect. The visual quality of the recovered image is very bad. The coverless information hiding algorithm proposed in the paper Sun et al. [Sun, Grishman and Wang (2017)] was combined with natural language processing. The NER system is used to mark the location of hidden information through an algorithm based on active learning of named entities (NER). The algorithm proposed in Liu et al. [Liu, Zhang, Liu et al. (2018); Duan and Song (2018)] combined the coverless information hiding algorithm with machine learning, and used the generated model to generate images related to secret information for transmission. The paper Zhang et al. [Zhang, Peng and Long (2018)] generated the feature sequence through the relation between Direct Current coefficients in the adjacent blocks.

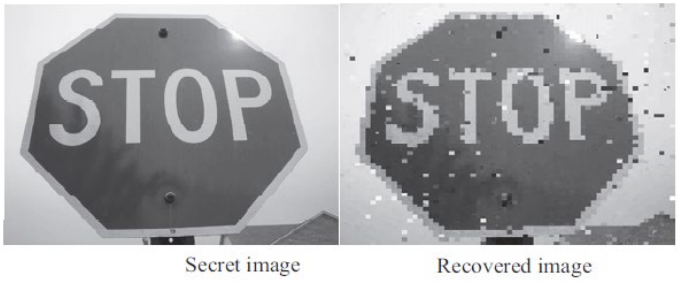

Figure 1: The original secret image and the secret image recovered by CIS-PDVR

3 Preliminaries

There are many kinds of feature descriptors used to describe images. These image features can be classified according to different criteria. For example, according to the representation of features on image data, they can be divided into point features, line features and regional features. According to the size of the area covered by the feature extraction, it can be divided into two categories: global features and local features.

LBP is an operator which used to describe the local texture features of an image. It has significant advantages such as rotation invariance and gray invariance. It was first proposed by Ojala et al. [Ojala, Pietikäinen and Harwood (1994)] for texture feature extraction. Moreover, the extracted features are local texture features of the image.

The original LBP operator is defined as a window within the 3×3 window, and the gray value of the adjacent 8 pixels is compared with the center pixel in the window. If the surrounding pixel value is greater than the central pixel value, the pixel is marked as 1, otherwise 0. In this way, 8 points in the 3×3 neighborhood can be compared to produce an 8-bit binary number (usually converted to a decimal number, i.e., LBP code, a total of 256 types), that is, the LBP value of the center pixel of the window is obtained, and this value is used to reflect the texture information for this area. As shown in Fig. 2. We get an image block with the size of 3×3. Then we compare the center pixel value with the surrounding pixel value and get the 8-bit binary number. We calculate its decimal number in this paper.

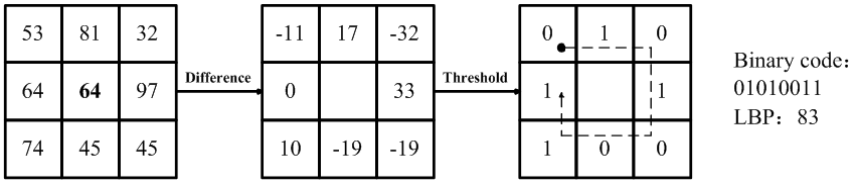

Figure 2: The generation of LBP value

4 The proposed coverless steganography framework

In this section, we will illustrate the secret information hiding and extracting procedures. Fig. 3 shows the framework of the proposed coverless information hiding.

Firstly, we select an original natural image randomly as the host image from the image database, then divide it into a number of non-overlapping blocks with same size, and obtain the binary hash value of image block with hash method based on different features.

Secondly, we convert secret information into a binary sequence. Then match it with the hash sequence of the original image one by one. If they are same, the original image block remains unchanged. If not, the similar natural image block is retrieved from the image block database for replacement, so that the binary hash value of original image block is flipped. Finally, we can synthesize the stego image.

At the receiver end, we also divide the stego image into the same number image blocks. We can obtain the binary hash value with the same hash algorithm and the secret information can be obtained by connecting the binary hash value.

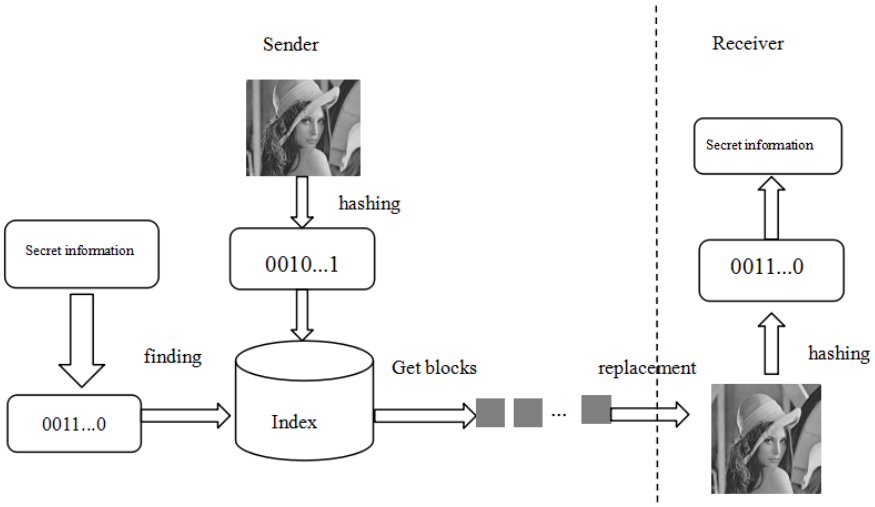

Figure 3: The framework of the proposed method

4.1 Binary hash sequence generation

In this section, we introduce the generation of binary hash value of every image block. Then we can get the hash sequence of the image, which can be mapped to secret information. Every image block can be represented by 0 or 1 according the hash algorithm. For a given image I, suppose the size of the image is $N_w \times N_h$, and then the process is described in the following.

Step1. Divide I into non-overlapping image blocks with sized$l \times l$, then the number of image blocks BN $= [(N_w \times N_h)/(l \times l)]$. For simplify, we set $l = 3$ in the paper, but the method is still reasonable under the other value. So the blocks B_i with raster scan order are$B_i = \{b_1, b_2, \dots, b_{BN}\}$, $1 \le \mathrm{i} \le \mathrm{BN}$.

Step2. We calculate three kinds of feature value which are the LBP value of the center pixel, the mean value of all non-center pixels and the variance value of all non-center pixels, each feature value can be denoted as $m_i = \{m_1, m_2, \dots, m_{BN}\}$, $1 \le \mathrm{i} \le \mathrm{BN}$ uniformly.

Step3. For i-th block, we denote the center pixel value of every image block as $P_i = \{P_1, P_2, \dots, P_{BN}\}$, $1 \le \mathrm{i} \le \mathrm{BN}$. We calculate the binary hash value of every image block by comparing P_i and m_i. Then, we can get the hash sequence h_i of the image by the following formula.

$$h_i = \begin{cases} 1, & if\ P_i > m_i \\ 0, & otherwise \end{cases}, where\ 1 \le \mathrm{i} \le \mathrm{BN} \quad (1)$$

4.2 Construction of the similarity index structure of image

The similarity index used to store the binary hash value and the image blocks corresponding to it. We collect a large number of images to construct a large-scale database and divide the images into blocks to get an image block database. Then calculate the binary hash value of every image block.

The image blocks are divided into two categories, class 0 is recorded as Block0 and class 1 is recorded as Block1. The hash value of all image blocks in class 0 is set 0 and class 1 is set 1, respectively. As shown in the following Fig. 4. We can get three kinds of different index according to different features.

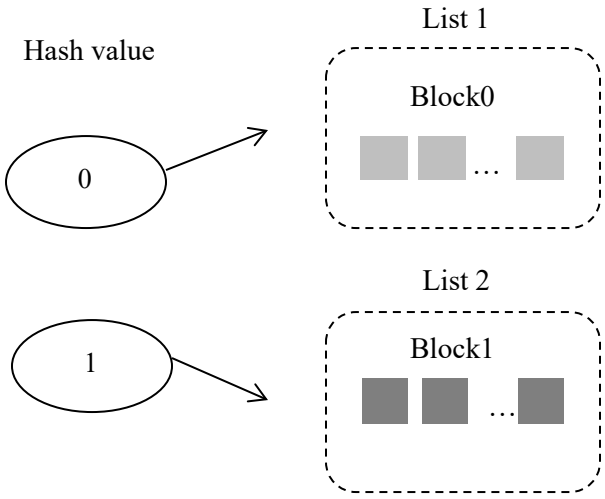

Figure 4: The similarity index

4.3 Querying images using similarity index

For the given secret information, this section introduces how to find the image blocks for matching.

To transmit the secret information, the sender matches the sequence of the secret information with the hash sequence of the original image one by one. If the corresponding locations have the same values, the image block remains unchanged. Otherwise, we should retrieve the image block from the database according to its hash value for matching, and achieve the flip of hash value of the original image block.

In order to make sure high visual quality of the stego image, we designed an efficient block matching scheme according to the MSE, the processing can be described as follows.

We determine the correct category in the index according to the value of the secret information, if the value is 0, we select the image blocks in Block 0, else we select the image blocks in Block 1, and then we calculate the mean square error MSE of all image blocks in the corresponding class and the original image block which need to be replaced according to the formula 2, and find the image block which has the smallest MSE for replacement.

$$\mathrm{MSE} = \frac{1}{l\times l}\sum_{i=1}^{l\times l}(O_i - B_i)^2, where \;\; 1 \le \mathrm{i} \le l \times l \tag{2}$$

where O_i and B_i are the pixel value of the original image block and the image block in the index, respectively.

4.4 The communication of secret data

When the image blocks that meet the requirements are found, block replacement of the original image results in a stego image. We will detail the process of information transfer.

For the sender, as shown in the following Fig. 5, we obtain the hash sequence of the original image according to the hash algorithm introduced above, and then match the secret information sequence with the hash sequence of the original image one by one. If the same location has the same value, the corresponding image block remains unchanged. If the value is not the same, then the natural image block that is most similar to the original image block is found for replacement in the similarity index. The process is as described in Section 4.3, so that the hash value at the corresponding position is flipped. Therefore, the hash sequence of the stego image is the same as the secret information sequence. Finally, the stego image is sent to the receiving end.

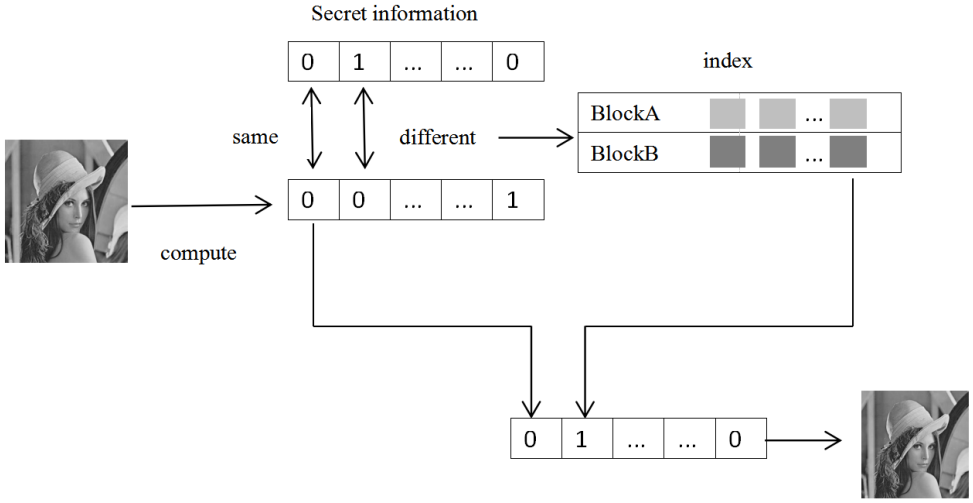

Figure 5: The process of transmission

For the receiving end, after receiving the stego image, the image is segmented according to the same rule to obtain the hash value of the image block. Since the stego image is replaced according to the secret information, the hash sequence of the stego image is the secret information sequence.

5 Experiments

We conduct our experiments on a standard computer with E5-2650 2.60 GHz CPU and 24 GB memory. We downloaded 1000 images from the web as an image database. The experiments include the capacity of our method and the visual quality of the stego image with three kinds of features.

5.1 Capacity of steganography

In our approach, the capacity is defined as the number of bits hidden in the stego image. Because every image block can embed 1 bit secret information, the number of the image

block is the capacity. Therefore, we assume that the size of original image is $I_w \times I_h$ and the size of image block is $l \times l$. For simplify, we set $l = 3$ and $I_w \times I_h = 300 \times 300$ in the paper, but the method is still reasonable under the other value. The size of the stego image is the same as original image. The capacity IC is calculated using (3).

$$\mathrm{IC} = \frac{I_w \times I_h}{l \times l} \tag{3}$$

We compare our embedding capacity with four existing coverless image steganography methods. Their approaches are coverless image steganography using partial-duplicate visual retrieval [Zhou, Mu and Wu (2017)], denoted as CIS-PDVR, coverless image steganography method based on bag-of-words [Zhou, Cao and Sun (2016)], denoted as CIS-BOW, coverless image steganography based on SIFT and BOF [Yuan, Xia and Sun (2017)], denoted as CIS-BOF and robust coverless image steganography based on DCT and LDA [Zhang, Peng and Long (2018)], denoted as CIS-DCT. So far, the largest capacity is the method proposed in CIS-PDVR. In this method, the secret information transmitted is an image. The fewer images required, the larger the hidden capacity in each image, but the worse the quality of the recovered secret information. Compared with the method in CIS-DCT, the maximum length of secret information is much higher than the length 15 in CIS-DCT. The longer the length sof the secret information, the more images are needed in CIS-DCT. This problem does not exist in our method that we just need one image to transmit information. The length of the hash sequence of the image is constant in CIS-BOW and CIS-BOF, only 16-bit and 8-bit secret information can be hidden, respectively. As shown in the Tab. 1, our hidden capacity is higher than other methods.

Table 1: The capacity comparison

Method	IC (bit)
Our proposed method	10000
CIS-PVDR	384
CIS-DCT	15
CIS-BOF	8
CIS-BOW	16

5.2 Visual quality of the stego image

We use the peak signal-to-noise ratio (PSNR) to measure the quality of stego image. In general, PSNR higher than 40 dB indicates that the image quality is excellent (it is very close to the original image), and 30-40 dB PSNR usually indicates that the image quality is good (That is, the distortion can be perceived but acceptable). The image quality is poor at 20-30 dB, and the image is unacceptable when PSNR is less than 20 dB [Huynh-Thu and Ghanbari (2008)]. We experiment with 4 classic images, namely Lena, fruits, couple and peppers. Figs. 6(a)-6(d) show the original image respectively. Figs. 6(a1)-6(d1) show the stego images with the feature LBP respectively. Figs. 6(a2)-6(d2) show the stego images with the feature mean value respectively. Figs. 6(a3)-6(d3) show the stego images with the feature variance value respectively. We embed the maximum length of secret information 10000 bits in every image. We can find from Fig. 6 that there

is no obvious mosaic effect, basically the same as the original image with the feature LBP and the mean value. The stego images have obvious mosaic effect based on the feature variance value.

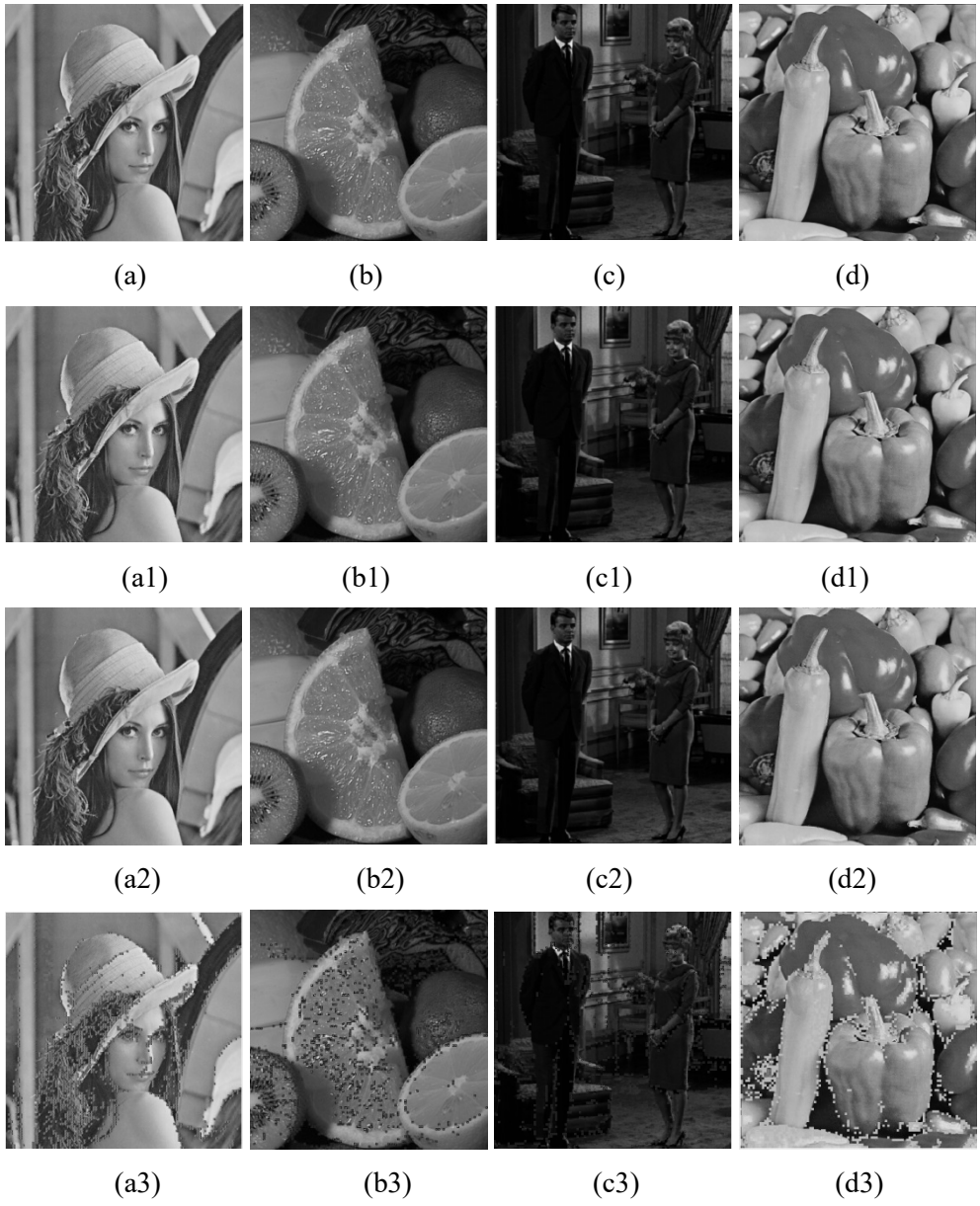

Figure 6: (a-d) The original images; (a1-d1) The stego images with the feature LBP; (a2-d2) The stego images with the feature mean value; (a3-d3) The stego images with the feature variance value

During the experiment, we found that the size of the image database affects the quality of the stego image. Fig. 7 below shows the average PSNR value of 100 images in image

database for the stego images with different features under different number of images. As can be seen, the larger the image database, the better the visual quality of the stego image. Besides, the result of LBP is better than other features.

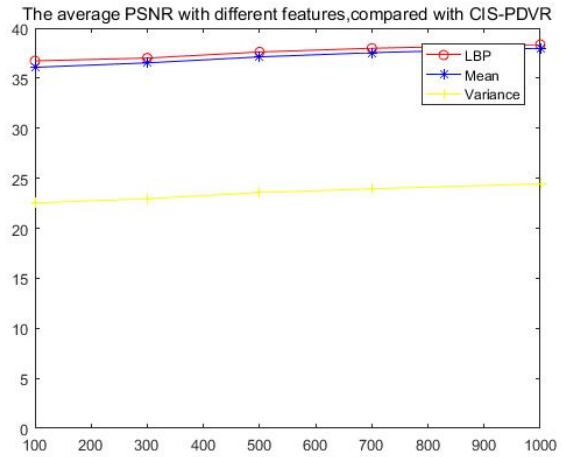

Figure 7: The average PSNR value with different features

Besides, we compare the SSIM (Structure Similarity) of images in our method with the SSIM of the method CIS-PDVR with different number of images in the image database. The SSIM is an image quality evaluation method that the evaluate result seems more consistent with the subjective sensation of people. The SSIM is in the range of [-1, 1] and when it equals to one, the two images are identical. Fig. 8 shows the average SSIM of 100 images which are selected from the database with different feature and the average SSIM of the same images in the method CIS-PDVR. We can see the SSIM of images in our method is higher than that in the CIS-PDVR. The experimental results show that the quality of the image in our method is better than the method in the CIS-PDVR. Also, the result of LBP is the best.

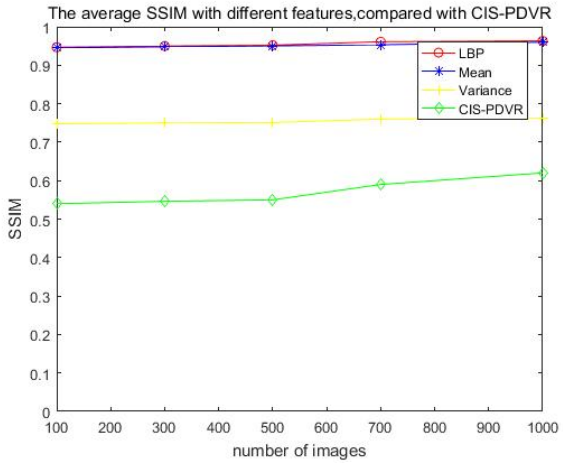

Figure 8: The average SSIM with different features, compared with CIS-PDVR

6 Conclusions

This paper proposes a high-capacity image coverless steganography method. By matching the secret information and the hash sequence of the image one by one, the similar natural image block is found in the image block database for replacement, then the hash value is inverted. Since the stego image block which obtained from the natural image is the image block most similar to the original image block, the visual quality of the stego image is still high by using proper feature. We compare three kinds of image features and find that LBP is the best. However, when we select the image block for replacement, we need to compare every image block in the index with cover image block to find the most similar image block which will cost much time. The next work will focus on establishing a new index to speed up the retrieval efficiency.

Acknowledgement: 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 U1836208, U1536206, U1836110, 61602253, 61672294; by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20181407; 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.

References

Du, Y.; Yin, Z. X.; Zhang, X. P. (2018): Improved lossless data hiding for jpeg images based on histogram modification. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 495-507.

Duan, X. T.; Song, H. X. (2018): Coverless steganography for digital images based on a generative model. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 483-493.

Huynh-Thu, Q.; Ghanbari, M. (2008): Scope of validity of PSNR in image/video quality assessment. *Electronics Letters*, vol. 44, no. 13, pp. 800-801.

Huang, F.; Huang, J.; Shi, Y. Q. (2012): New channel selection rule for jpeg steganography. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1181-1191.

Kang, Z. W.; Liu, J.; He, Y. G. (2007): Steganography based on wavelet transform and modulus function. *Journal of Systems Engineering and Electronics*, vol. 18, no. 3, pp. 628-632.

Liu, M.; Zhang, M.; Liu, J.; Zhang, Y.; Ke, Y. (2018): Coverless information hiding based on generative adversarial networks. *Journal of Applied Sciences*, vol. 36, no. 2, pp. 371-382.

Luo, W.; Huang, F.; Huang, J. (2010): Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 1448-1458.

Meng, R. H.; Steven, G. R.; Wang, J.; Sun, X. M. (2018): A fusion steganographic algorithm based on faster R-CNN**.** *Computers, Materials & Continua*, vol. 55, no. 1, pp. 1-16.

Nie, Q. K.; Xu, X. B.; Feng, B. W.; Leo, Y. Z. (2018): Defining embedding distortion for intra prediction mode-based video steganography. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 59-70.

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.

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

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

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

Zhou, Z. L.; Mu, Y.; Wu, Q. M. J. (2018): Coverless image steganography using partial-duplicate image retrieval. *Soft Computing*, pp. 1-12.

Zhang, X.; Peng, F.; Long, M. (2018): Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238.

Zhou, Z. L.; Cao, Y.; Sun, X. M. (2016): Coverless information hiding based on bag-of-words model of image. *Journal of Applied Sciences*, vol. 34, no. 5, pp. 527-536.