Multimedia Tools and Applications
https://doi.org/10.1007/s11042-018-6444-0

A novel coverless information hiding method based on the average pixel value of the sub-images

Liming Zou[1] · Jiande Sun[1] · Min Gao[1] · Wenbo Wan[1] · Brij Bhooshan Gupta[2]

Received: 21 May 2018 / Revised: 16 July 2018 / Accepted: 20 July 2018
Published online: 24 July 2018

Abstract
In traditional information hiding methods, the secret information is embedded into the carriers, which will inevitably leave traces of modification on the carriers. In those methods, the modified images can be easily detected by some steganalysis algorithm and thus the security can not be guaranteed. To address this problem, the concept of coverless information hiding is proposed. However, general coverless information hiding method has a lower information hiding capacity. In this paper, we propose a novel coverless information hiding method based on the average pixel values of sub-images. We generate hash sequences by a hashing algorithm and realize the secret information hiding through mapping relationship. In the first place, we build a dictionary and a hash array. Then we map the dictionary and the hash array through mapping relationship. Furthermore, we build a multi-level index structure for retrieving the stego-images efficiently. The experimental results and analysis show that our method has a good performance in the capacity of information hiding, the security, the robustness to image attacks and the hiding success rate based on different image databases.

Keywords Coverless information hiding · Sub-images · Average pixel value · Multi-level index structure

1 Introduction

With the development of media and information technology, digital multimedia is popular in network transmission [32, 35]. However, it also brings more and more information security

✉ Jiande Sun
jiandesun@hotmail.com

✉ Wenbo Wan
wanwenbo@sdnu.edu.cn

[1] School of Information Science and Engineering, Shandong Normal University, Jinan, China

[2] Department of Computer Engineering, National Institute of Technology Kurukshetra Haryana INDIA, Thanesar, India

problems, such as information integrity, copyright protection and the authenticity of information [22, 23]. In order to improve information security, there are two existing technologies cryptography and information hiding [29]. In cryptography, the third party can not read the information after the secret information is encrypted. But the third party can easily determine whether the carrier carries the secret information, which leads to the interception of secret information. In order to solve this problem, the concept of information hiding is proposed. Compared with traditional encryption technology, information hiding technology has the characteristics of transparency, robustness and security, and it becomes a new information security discipline [30]. In traditional information hiding methods, the secret information is embedded into the carrier by changing the carrier itself [16, 18].

According to [3], the existing image-based information hiding methods can be roughly divided into three categories: spatial domain, frequency domain and adaptive domain. Typical spatial domain methods include the LSB (least significant bit) replacement [25], LSB matching [19], color palette [8] and histogram-based methods [13]. Although the modification of cover image caused by the spatial domain embedding mechanism is not easily detected by human eyes, the embedded information is sensitive to image attacks. To address this issue, many frequency domain steganography methods have been proposed, such as quantization Table (QT) [12], discrete Fourier transform (DFT) [17], and discrete wavelet transform (DWT) based embedding [4, 24]. Adaptive steganography is a special case of the spatial domain and frequency domain methods. In the literature, there are many typical adaptive steganography methods, such as the locally adaptive coding-based [2], edge based [15] and Bit Plane Complexity Segmentation (BPCS) based data embedding [7, 9]. Although the existing methods employ different technologies for image information hiding, all of the methods implement the information hiding by embedding the secret information into a designated cover image. Since the embedding process modifies the cover image, modification traces will be left in the cover image. Consequently, it is possible to be detected by various existing steganalysis tools such as [10, 11, 26, 27], all of which are based on the modification traces.

To avoid leaving traces on the carriers, the concept of coverless information hiding is proposed [14, 28]. Coverless information hiding is proposed to resist all of the existing steganalysis tools [20]. The main idea of coverless information hiding is to find the natural digital images which already contain the secret information. In the coverless information hiding method, there is a mapping relationship between the secret information and the carrier. Compared with the traditional information hiding methods, coverless information hiding methods do not change the carrier. Therefore, coverless information hiding methods have higher security than traditionary information hiding methods. At present, the choice of carrier can be text, image, audio, video, etc. [5]. As widespread in social media, images become the ideal carrier for information hiding with many features [21, 31]. In this paper, images are adopted to hide secret information. As a matter of fact, another problem in coverless information hiding method is to improve the hiding capacity [6]. In this paper, we propose a novel coverless information hiding method based on the average pixel values of the sub-images. We divide the image into several sub-images and compute the average pixel values of sub-images [1] at first, and then generate the hash sequence to express the secret information.

The main contributions of this paper are concluded as follows. We build a Chinese dictionary and a hash array. We propose a novel mapping relationship to link the secret information with the carriers. And we build a multi-level index structure for retrieving the stego-images efficiently.

The rest of this paper is organized as follows. Section 2 is our proposed coverless information hiding method. And the experiment and analysis will be discussed in Section 3. Finally, Section 4 concludes the paper and put forward the future work with brief words.

2 The proposed coverless information hiding method

In this paper, we propose a novel coverless information hiding method based on the average pixel value of sub-images to generate binary sequences and realize secret information hiding. We use the binary sequence to represent the secret information. The framework of our coverless information hiding method is illustrated in Fig. 1.

In this paper, we achieve the goal of information hiding based on the Chinese sentences. A Chinese sentence generally include subject, predicate, object, preposition and so on. In the framework of our coverless information hiding method, the secret information is segmented according to the structure of a Chinese sentence. The segments of the secret information is marked as $\{I_1, I_2, \ldots, I_n\}$, where n is the segments number of the Chinese sentence. And then the position of each segment could be got according to the dictionary, which is marked as $\{P_1, P_2, \ldots, P_n\}$. According to the position of each secret information segment, we can get the label information of the hash sequence in each part of the hash array of images, which is marked as $\{L_1, L_2, \ldots, L_n\}$. The corresponding images can be indexed according to the label information. Then the stego-image that randomly selected from the corresponding images is sent to the receiver. After receiving the image, the receiver blocks the image and gets the sub-images at first, where the sub-images is marked as $\{S_1, S_2, \ldots, S_m\}$, with m as the number of sub-images. And we can generate hash sequence by the average pixel values of sub-images. Then the receiver partitions the hash sequence. The number of segments of hash sequence should be consistent with the number of the secret information segments. The segments of hash sequence are marked as $\{B_1, B_2, \ldots, B_n\}$. The receiver can get the label information according to each segment of the hash sequence and the hash array. And then the receiver can get corresponding

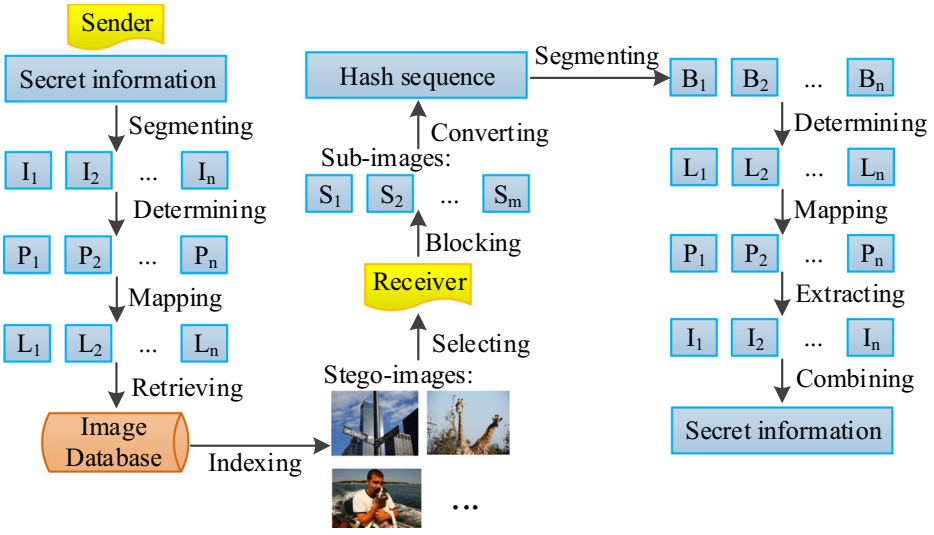

Fig. 1 The framework of proposed method

position information of each segment of secret information. Finally, each segment of secret information can be extracted according to the position information and combined to the secret information.

2.1 Building data sets

We build a Chinese dictionary and a 50968×80 hash array. In this paper, our Chinese dictionary are composed of four parts, including the subjects, the predicates, the objects and the prepositions, where $n = 4$. Each part contains 8 different Chinese words. The Chinese dictionary is marked as W, and the four parts of the dictionary are marked as $\{W_1, W_2, W_3, W_4\}$ respectively. The Chinese dictionary is shown in Table 1.

When extracting hash sequence from the image, the image is partitioned into the sub-images as needed. Then we calculate the average pixel value of each sub-image respectively, which is marked as $Ave-pixel$. And the connective order of sub-images is illustrated in Fig. 2, where the image is divided into 9 sub-images.

We can get a hash sequence according to the connective order by a hashing algorithm. The hashing algorithm is illustrated as Eq. (1) when $1 \le i \le m-1$, and Eq. (2) when $i = m$.

$$\begin{cases} h_i = 0, Ave-pixel(i+1) \ge Ave-pixel(i) \\ h_i = 1, Ave-pixel(i+1) < Ave-pixel(i) \end{cases} \tag{1}$$

$$\begin{cases} h_i = 0, Ave-pixel(1) \ge Ave-pixel(i) \\ h_i = 1, Ave-pixel(1) < Ave-pixel(i) \end{cases} \tag{2}$$

$Ave-pixel(i)$ is the average pixel value for ith sub-image. In this paper, we divide each image into 8 rows and 10 columns with a total of 80 sub-images ($m = 80$) and get a hash sequence of 80 bits. According to the dictionary, we divide the 80-bit hash sequence into four segments and each segment contains 20 bits. There are 50,968 images downloaded from the Internet used in this paper. After extracting hash sequences from images, we get a 50968×80 hash array, which is marked as M. To correspond with the dictionary, the 50968×80 hash array is divided into four 50968×20 hash arrays, which are marked as $\{M_1, M_2, M_3, M_4\}$ respectively.

2.2 Mapping the secret information

In the Chinese dictionary, every word will have a position information ($1 \le P \le 8$) in the corresponding section. These four 50968×20 hash arrays are independent with each other. Corresponding to the Chinese dictionary, every 20-bit hash sequence in the four 50968×20 hash arrays is labeled according to its decimal of 20-bit hash. The maximum value of the decimal for 20-bit hash is $(2^{20}-1)$. Let $U = (2^{20}-1)/8$. Then the relationship between each label and the decimal of 20-bit hash is shown in Table 2.

Table 1 The composition of the Chinese dictionary

Subjects:					军	师	谋长	队
Predicates:	来	去	走	回	住	吃	是	在
Objects:	家	学校	商场	广场	餐厅	健身房	街	基地
Prepositions:	左	右	上	下	里	外	前	后

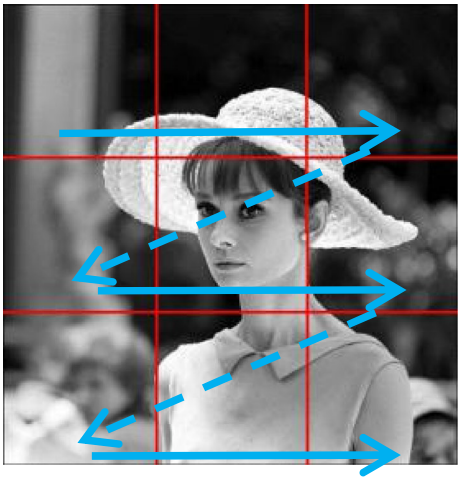

Fig. 2 The connective order of sub-images

In order to map the secret information with the image, we first partition the secret information into four segments according to the Chinese dictionary. Then we get the position information of each segment in the dictionary. There is a consistent one-to-one match between the position information and the hash label, and the label information will be obtained. Then we can get the corresponding hash sequences according to Table 2. Finally, the images with the corresponding hash sequences can be indexed. Thus, the images can carry the secret information.

2.3 Multi-level index structure

The key to coverless information hiding is to find the stego-images quickly from a huge image database. This is very time-consuming if we directly retrieve a conditional image from a image database. In order to solve this problem, we propose a multi-level index structure that greatly improves the retrieval efficiency, which is shown in Fig. 3.

As shown in Fig. 3, we can get 20-bit hash sequences in the corresponding hash array (M_1, M_2, M_3 and M_4) respectively according to the label at first. The 20-bit hash sequences are marked as B_1s, B_2s, B_3s and B_4s respectively. Then, the images that contain B_1s in M_1 are retrieved from the image database, which is marked as $Image_1s$. Then, the images that contain B_2s in M_2 are retrieved from $Image_1s$, which is marked as $Image_2s$. Then, the images that contain B_3s in M_3 are retrieved from $Image_2s$, which is marked as $Image_3s$. Finally, the images that contain B_4s in M_4 are retrieved from $Image_3s$, which is marked as $Image_4s$. $Image_4s$ is the Stego-images.

Table 2 The relationship of label and binary corresponding decimal

Label:	1	2	3	4	5	6	7	8
Binary corresponding decimal:	[0,U)	[U,2 U)	[2 U,3 U)	[3 U,4 U)	[4 U,5 U)	[5 U,6 U)	[6 U,7 U)	[7 U,8 U]

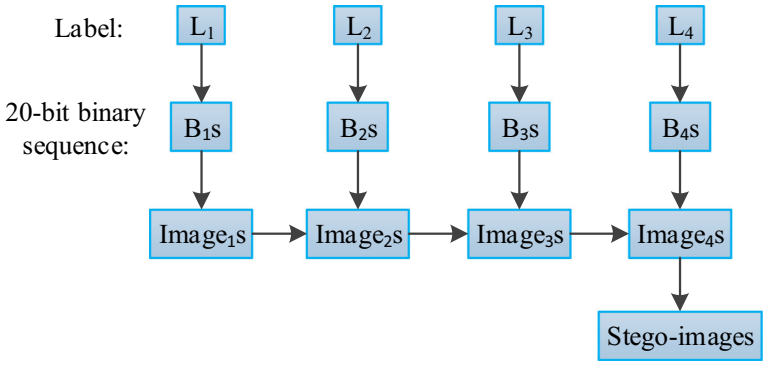

Fig. 3 Multi-level index structure

2.4 Information hiding

In this paper, we represent the secret information with a hash sequence generated according to the average pixel value of the sub-images.The process of information hiding is illustrated in Fig. 4.

Step 1: First, the secret information is divided into four segments, denoted as $\{I_1, I_2, I_3, I_4\}$, according to the subject, the predicate, the object and the preposition. Then, we can get the positions of the four segments in W, denoted as $\{P_1, P_2, P_3, P_4\}$.

Step 2: We can get the label of the 20-bit hash sequence, donated as $\{L_1, L_2, L_3, L_4\}$, according to the mapping relationship with the position information. According to the hash array $M = \{M_1, M_2, M_3, M_4\}$, we can get the corresponding 20-bit hash sequences, donated as $\{B_1s, B_2s, B_3s, B_4s\}$ with each label.

Step 3: With the help of the index method in Fig. 3, we are able to get all the corresponding stego-images from the image database.

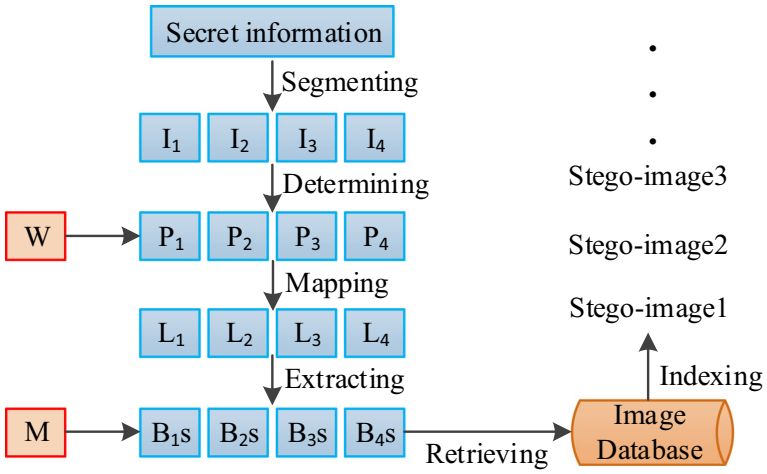

Fig. 4 The process of information hiding

2.5 Information extraction

The process of information extraction is illustrated as Fig. 5.

Step1: After received the stego-image, the receiver is supposed to divide the stego-image into 80 sub-images and calculate the average pixel value of each sub-image. Then a 80-bit hash sequence could be obtained according to the hashing algorithm.

Step2: The 80-bit hash sequence will be segmented into four 20-bit hash sequences, denoted as $\{B_1, B_2, B_3, B_4\}$. Next, the receiver add the label $\{L_1, L_2, L_3, L_4\}$ to each 20-bit hash sequence according to the hash array $M = \{M_1, M_2, M_3, M_4\}$ and Table 2.

Step3: The receiver could get the position information $\{P_1, P_2, P_3, P_4\}$ of each segment of secret information according to the mapping relationship. Then, the four segments $\{I_1, I_2, I_3, I_4\}$ of secret information can be extracted from W according to the position information. Finally, the secret information can be gotten by combining the four segments together.

3 Experiment and analysis

The experiment of this paper is carried out on the platform of MATLAB R2016b. For example, if we want to send the secret information of '老师在学校里'. First, we could divide the secret information into four segments, which are '老师', '在', '学校' and '里'. Then we can get the position of the four segments, which are 6, 8, 2 and 5 according to the dictionary. The labels of the four 20-bit hash sequences are obtained according to the mapping relationship, which are 6, 8, 2 and 5 respectively. According to the hash array $M = \{M_1, M_2, M_3, M_4\}$ and Table 2, we can get the corresponding 20-bit hash sequences with each label. Finally, the stego-images could be indexed according to the multi-level index structure. After the process of coverless information hiding, we can obtain the corresponding stego-images as shown in Fig. 6. Each stego-image in Fig. 6 contains the same secret information of '老师在学校里'.

The sender can transmit the stego-images to the receiver through the public network. Because each stego-image contains the same secret information, for simplicity, we can randomly select one stego-image to send to the receiver. After received the stego-image, the receiver divides the stego-image into 80 sub-images and calculate the average pixel value of

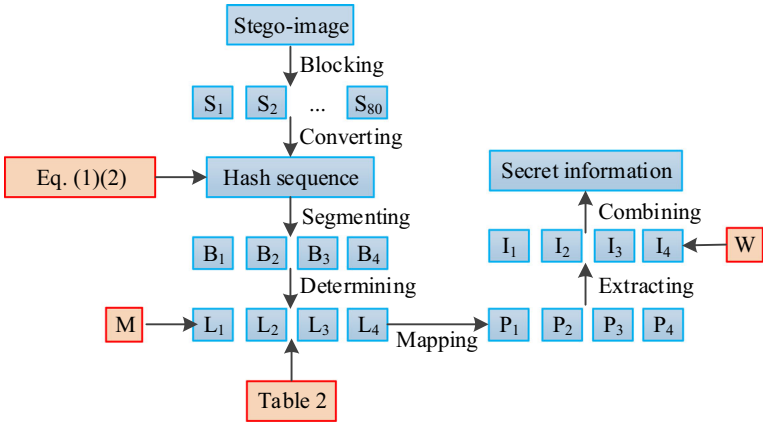

Fig. 5 The process of information extraction

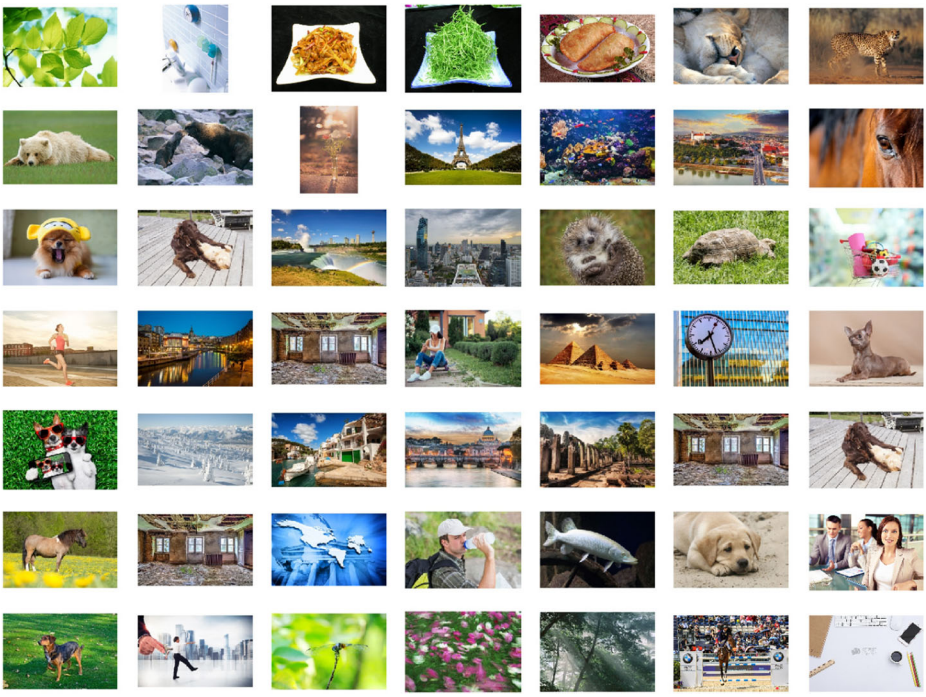

Fig. 6 Stego-images with the secret information of "老师在学校里"

each sub-image at first. Then the receiver can get a 80-bit hash sequence according to the hashing algorithm. Then the receiver segment the 80-bit hash sequence into four 20-bit hash sequences and get the labels of four 20-bit hash sequences, which are 6, 8, 2 and 5 respectively, according to Table 2. Next, the position of four segments of secret information can be obtained, which are 6, 8, 2 and 5 respectively, according to the mapping relationship. Then, the four segments of secret information can be extracted from W based on the position information, which are '老师', '在', '学校' and '里' respectively. Finally, the secret information '老师在学校里' can be gotten by combining the four segments together. The experimental results show that the secret information '老师在学校里' can be correctly extracted. In addition, we also analyze the capacity of information hiding, the security, the robustness to image attacks and the hiding success rate based on image database.

3.1 The capacity of information hiding

In the experiment of this paper, we generate 80-bit hash sequence to hide secret information in each image. As shown in Table 3 [1], the information capacity of our proposed coverless information hiding method is much higher than the other methods.

And our approach is not limited to 80-bit hiding capacity. We can divide the images into more sub-images to generate longer hash sequence according to our actual needs. At the same time, the Chinese dictionary needs to be expanded according to the actual needs. However, when generating longer hash sequence to hide more secret information, the image database should be enlarged at the same time. Otherwise, the probability of failure of retrieving the corresponding stego-images will be increased.

Table 3 The capacity of proposed methods

Methods	Capacity(bits·carrier $^{-1}$)
Zhou's method [34]	8
Yuan's method [29]	8
Zheng's method [33]	18
Our method	80

3.2 Security

In our coverless information hiding method, we block the image into 80 sub-images, and then calculate the average pixel values of the sub-images to get the hash sequence of the image. There is no change in the carrier, so it can completely resist the detection of human eyes and all the steganalysis algorithms.

Furthermore, we have a variety of images in our image database, where every secret information can index several corresponding stego-images. And we could send different stego-images to different receivers. In this case, even if the attackers obtain the stego-images, they can hardly extract the secret information. Therefore, the proposed method of coverless information hiding has higher security.

3.3 The robustness to image attacks

An ideal coverless information hiding method based on images should be robust to various typical image attacks, so that the secret information can be accurately recovered from the stego-images. As far as we know, the typical image attacks include luminance change, contrast enhancement and so on. Luminance change is an illumination change that will cause a constant to be added to each image pixel, and a contrast enhancement will cause each pixel value multiplied by a constant. However, the two attacks will not affect the average pixel value correlation between the sub-images. That is because all pixels in each sub-image will be added by the same value or multiplied by the same factor, and the average pixel value correlation between the sub-images remains the same. Therefore, the hash sequence of the image attacked by luminance change or contrast enhancement remains the same unchanged.

3.4 Hiding success rate based on image database

In addition to the above analysis, we also analyze the influence of the size of image database on the hiding success rate of secret information. First, we analyze the relationship based on 50,968 images, which are downloaded from the Internet. We take 2000 images as an interval. We randomly selected 2000 images from the 50,968 images database at first, then we randomly selected 4000, 6000, ..., 50,000 and 50,968 images in turn. For each selection, we selected the same number of images for 10 times to calculate their hiding success rate. For each selection, we use *suc_num* to represent the number of secret information from the selected images. So we can define the average number of different secret information from the 10 times selected images as:

$$ave\_num = \frac{\sum_{i=1}^{10} suc\_num_i}{10} \tag{3}$$

From the Chinese dictionary that we build in the section 2.1, we can know that the number of secret information is 4096($8 \times 8 \times 8 \times 8$). Therefore, we define the hiding success rate as:

$$suc\_rate = \frac{ave\_num}{4096} \tag{4}$$

Therefore, we could get the relationship between the hiding success rate and the size of images database based on the 50,968 images as show in Fig. 7.

To further analyze the relationship between the hiding success rate and the size of images database. We do the same analysis on the 164,062 images selected from the MSCOCO database and the 172,943 images selected from the ImageNet database. For each database, we do six experiments and every experiment contains 100,000 images randomly selected from 164,062 MSCOCO images and 172,943 ImageNet images respectively. In addition to define the interval as 5000 images, we do the same experiment on each 100,000 images randomly selected from the MSCOCO database and the ImageNet database. And we get six relationships based on the 100,000 images randomly selected from 164,062 MSCOCO database as show in Fig. 8 and six relationships based on the 100,000 images randomly selected from 172,943 ImageNet database as shown in Fig. 9 respectively.

From the above experiment results, we can see that the hiding success rate increases rapidly along with the increase of the number of images in the early stage. In the result of the relationship based on the 50,968 images in Fig. 7, the hiding success rate is close to 1 when the number of images is 50,968. However, in the six results of the relationship based on the MSCOCO database, the hiding success rate has reached 1 when the numbers of images are (a) 80,000, (b) 90,000, (c) 95,000, (d) 85,000, (e) 85,000 and (f) 95,000 respectively. And in the six results of the relationship based on the ImageNet database, the hiding success rate has reached 1 when the numbers of images are (a) 75,000, (b) 80,000, (c) 75,000, (d) 85,000, (e) 70,000 and (f) 75,000 respectively.

Therefore, we can get the conclusion that the hiding success rate is able to be 1 when the number of images is about ninety thousand. In other words, when the number of images is about ninety thousand, it is capable to hide all the 4096 secret information.

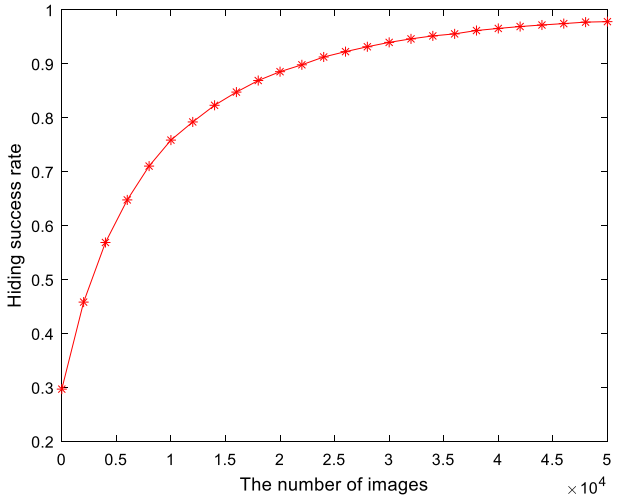

Fig. 7 The relationship based on the 50,968 images

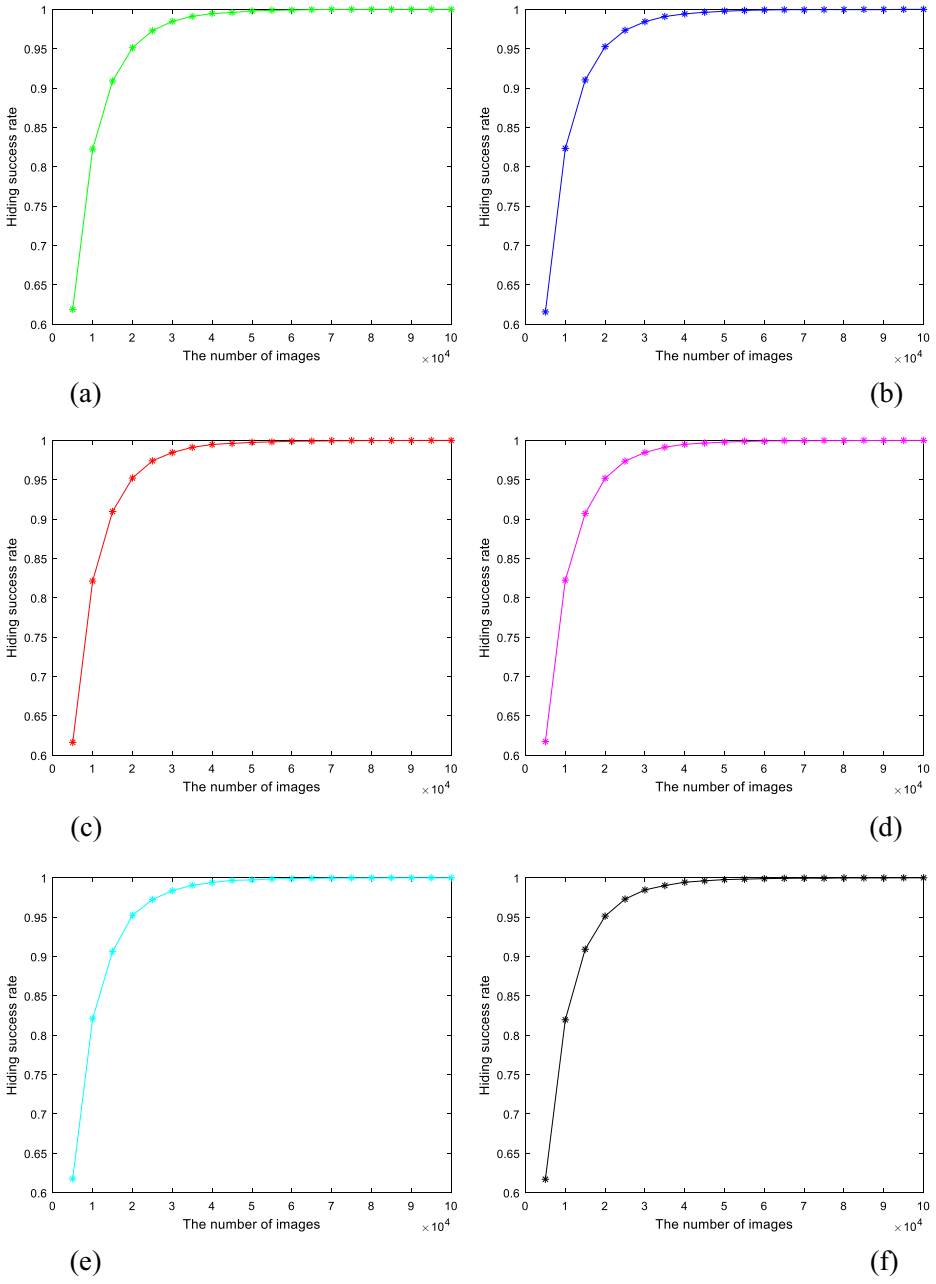

Fig. 8 Six relationships based on the 100,000 images selected from MSCOCO database

4 Conclusion and future work

In this paper, we propose a novel coverless information hiding method based on the average pixel values of the sub-images. We build a Chinese dictionary and a hash array. If the secret information are English words, this method will still work, as long as we make the English

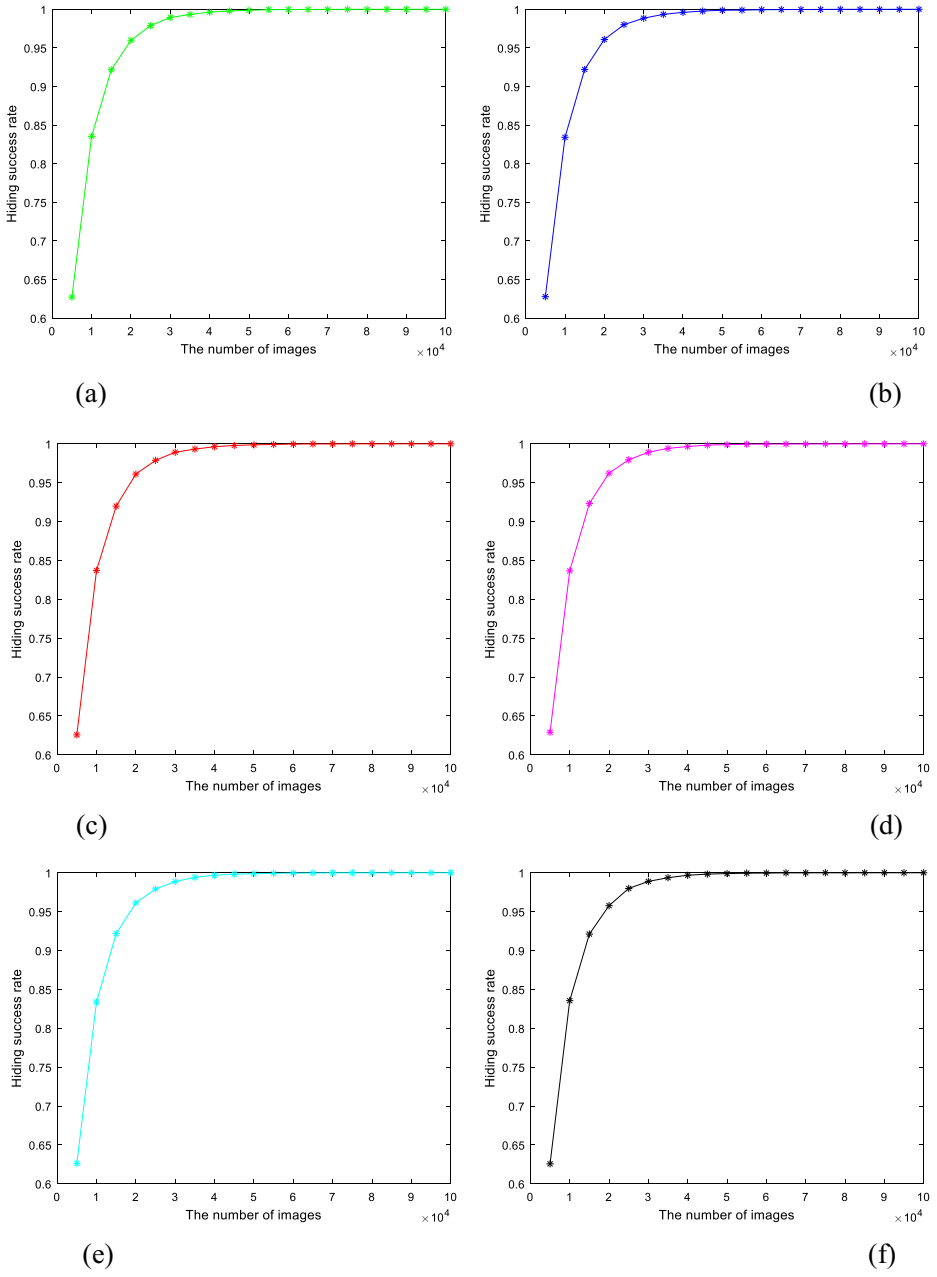

Fig. 9 Six relationships based on the 100,000 images selected from ImageNet database

dictionary is built correspondingly. We propose a novel mapping relationship to link the secret information with the carriers. And we also build a multi-level index structure for retrieving the stego-images efficiently. The experimental results and analysis show that our method has a good performance in the capacity, the security, the robustness to image attacks and the hiding success rate based on different image databases. Furthermore, we can divide the image into

more sub-images according to actual needs, and produce a longer hash sequence to achieve higher information hiding capacity. However, when generating longer hash sequence to hide more secret information, the image database should be enlarged at the same time. Otherwise, the probability of failure of retrieving the stego-images will be increased.

Acknowledgements This work is supported by the Natural Science Foundation of China (U1736122), the Natural Science Foundation for Distinguished Young Scholars of Shandong Province (JQ201718) and Shandong Provincial Key Research and Development Plan (2017CXGC1504).

References

1. Cao Y, Zhou Z, Sun X, Gao C (2018) Coverless information hiding based on the molecular structure images of material. CMC: Comput Mater Continua 54(2):197–207
2. Chang CC, Kieu TD, Chou YC (2009) Reversible information hiding for VQ indices based on locally adaptive coding[J]. J Vis Commun Image Represent 20(1):57–64
3. Cheddad A, Condell J, Curran K et al (2010) Review: digital image steganography: survey and analysis of current methods[J]. Signal Process 90(3):727–752
4. Chen WY (2007) Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation[J]. Appl Math Comput 185(1):432–448
5. Cox IJ, Miller ML (2002) The First 50 Years of Electronic Watermarking. J Appl Sign Proc (2): 126–132
6. Guo L, Ni J, Su W et al (2015) Using statistical image model for JPEG steganography: uniform embedding revisited[J]. IEEE Trans Info Forensic Sec 10(12):2669–2680
7. Hirohisa H (2002) A data embedding method using BPCS principle with new complexity measures[J]
8. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen[J]. Computer 31(2):26–34
9. Kawaguchi E (2005) BPCS-Steganography – Principle and Applications[C]// International Conference on Knowledge-Based and Intelligent Information and Engineering Systems. Springer Berlin Heidelberg 289–299
10. Ker AD (2004) Improved detection of LSB steganography in grayscale images[C]// International Conference on Information Hiding. Springer-Verlag 97–115
11. Ker AD (2005) Steganalysis of LSB matching in grayscale images[J]. IEEE Sign Proc Lett 12(6):441–444
12. Li X, Wang J (2007) A steganographic method based upon JPEG and particle swarm optimization algorithm. Inf Sci 177(15):3099–3109
13. Li Z, Chen X, Pan X et al (2009) Lossless data hiding scheme based on adjacent pixel difference[J]. IEEE 1(1):588–592
14. Lin W, Horng S, Kao T (2008) An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans Multimed 10(5):746–757
15. Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited[J]. IEEE Trans Info Forensic Sec 5(2):201–214
16. Ma Y, Luo X, Li X, et al. (2018) Selection of Rich Model Steganalysis Features Based on Decision Rough Set 𝛼-Positive Region Reduction[J]. IEEE Trans Circuits Syst Video Technol (99):1–1
17. Mckeon RT (2007) Strange fourier steganography in movies[C]// IEEE International Conference on Electro/information Technology. IEEE 178–182
18. Meng R, Steven G, Wang J, Sun X (2018) A fusion Steganographic algorithm based on faster R-CNN. CMC: Comput Mater Continua 55(1):1–16
19. Mielikainen J (2006) LSB matching revisited[J]. IEEE Sign Proc Lett 13(5):285–287
20. Pevny T, Fridrich J (2013) Merging Markov and DCT features for multi-class JPEG steganalysis. Proc SPIE - Int Soc Opt Eng 3:650503–650503
21. Ren X, Zheng Y, Zhao Y et al (2018) Drusen segmentation from retinal images via supervised feature learning. IEEE Acces 6:2952–2961
22. Wan W, Liu J, Sun J, et al. (2013) Logarithmic spread-transform dither modulation watermarking based on perceptual model[C]//Image Processing (ICIP), 2013 20th IEEE International Conference on. IEEE 4522–4526

23. Wan W, Liu J, Sun J et al (2015) Logarithmic STDM watermarking using visual saliency-based JND model[J]. Electron Lett 51(10):758–760
24. Wang J, Li T, Shi YQ et al (2017) Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics[J]. Multimed Tools Appl 76(22):23721–23737
25. Wu HC, Wu NI, Tsai CS et al (2005) Image steganographic scheme based on pixel-value differencing and LSB replacement methods[J]. Vision, Image Sign Proc IEE Proc 152(5):611–615
26. Xia Z, Wang X, Sun X et al (2014) Steganalysis of least significant bit matching using multi-order differences[J]. Sec Commun Netw 7(8):1283–1291
27. Xia Z, Wang X, Sun X et al (2016) Steganalysis of LSB matching using differences between nonadjacent pixels[J]. Multimed Tools Appl 75(4):1947–1962
28. Yang C, Weng C, Wang S (2008) Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans Info Forensic Sec 3(3):488–497
29. Yuan C, Xia Z, Sun X (2017) Coverless Image Steganography Based on SIFT and BOF[J]. Internet J Technol 18
30. Yuan Z, Guan Z, Feng H (2017) An improved information hiding algorithm based on image[C]// IEEE, International Conference on Software Engineering Research, Management and Applications. IEEE 169–172
31. Zhang J, Shen J, Wang L et al. (2016) Coverless Text Information Hiding Method Based on the Word Rank Map[M]// Cloud Computing and Security. Springer International Publishing 145–155
32. Zhang Y, Qin C, Zhang W, et al. (2018) On the Fault-tolerant Performance for a Class of Robust Image Steganography[J]. Signal Processing
33. Zheng S, Wang L, Ling B (2017) Coverless Information Hiding Based on Robust Image Hashing. Int Conf Cloud Comput Sec 536–547
34. Zhou Z, Sun H, Harit R, et al. (2015) Coverless Image Steganography Without Embedding[C]// International Conference on Cloud Computing and Security. Springer, Cham 123–132
35. Zhou Q, Qiu Y, Li L, Lu J et al (2018) Steganography using reversible texture synthesis based on seeded region growing and LSB. CMC: Comput Mater Continua 55(1):151–163

Liming Zou received the bachelor degrees in School of Information Science and Engineering, from Shandong Normal University, Jinan, Shandong, in 2017. He is currently working toward the master degree of Communication and Information Systems at the Shandong Normal University. His research interests include multimedia security, computer vision and machine learning. He is a student member of the CCF.

Jiande Sun received the Ph.D. degree in communication and information system from Shandong University, Jinan, China, in 2000 and 2005, respectively. From September 2008 to August 2009, he was a Visiting Researcher with the Institute of Telecommunications System, Technical University of Berlin, Berlin, Germany. From October 2010 to December 2012, he was a Post-Doctoral Researcher with the Institute of Digital Media, Peking University, Beijing, China, and with the State Key Laboratory of Digital-Media Technology, Hisense Group, respectively. From July 2014 to August 2015, he was a DAAD Visiting Researcher with Technical University of Berlin and University of Konstanz, Germany. From October 2015 to November 2016, he was a Visiting Researcher with the Language Technology Institute, School of Computer Science, Carnegie Mellon University, USA. He is currently a Professor with the School of Information Science and Engineering, Shandong Normal University. He has published more than 60 journal and conference papers. He is the co-author of two books. His current research interests include multimedia content analysis, video hashing, gaze tracking, image/video watermarking, 2D to 3D conversion, and so on.

Min Gao received the bachelor degrees in School of Information Science and Engineering, from Shandong Normal University, Jinan, Shandong, in 2016. She is currently working toward the master degree of Communication and Information Systems at the Shandong Normal University. Her research interests include computer vision, deep learning. She is a student member of the CCF.

Wenbo Wan received Ph.D. degree in Shandong University, Jinan, China in 2015. Now he is a Lecturer with the School of Information Science and Engineering, Shandong Normal University. His research interests include image/video processing and image/video watermarking.

Dr. B.B. Gupta is currently working as an Assistant Professor in Department of Computer Engineering, National Institute of Technology Kurukshetra, India. He received PhD degree from Indian Institute of Technology Roorkee, India. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada Award ($10,000). He spent more than 6 months in University of Saskatchewan (UofS), Canada to complete a portion of his research work. He has published more than 45 research papers in International Journals and Conferences of high repute. He has visited several countries to present his research work. His biography is selected to publish in the 30th Edition of prestigious Marquis Who's Who in the World, 2012. Dr. Gupta is also holding position of editor of various International Journals and magazines. He has also served as Technical program committee (TPC) member of more than 20 International conferences worldwide. Dr. Gupta is member of IEEE, ACM, SIGCOMM, The Society of Digital Information and Wireless Communications (SDIWC), Internet Society, Institute of Nanotechnology, Life Member, International Association of Engineers (IAENG), Life Member, International Association of Computer Science and Information Technology (IACSIT). He also worked as a post doctoral research fellow in UNB, Canada. His research interest includes Information security, Cyber Security, Cloud Computing, Web security, Intrusion detection, Computer networks and Phishing.