EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Coverless image steganography based on DenseNet feature mapping

Qiang Liu[1], Xuyu Xiang[2,1*], Jiaohua Qin[1], Yun Tan[1] and Yao Qiu[1]

*Correspondence:
xyuxiang@163.com
[1]College of Computer Science and Information Technology, Central South University of Forestry and Technology, Changsha 410004, China
[2]College of Information Technology and Management, Hunan University of Finance and Economics, Changsha 410205, China

Abstract

Since the concept of coverless information hiding was proposed, it has been greatly developed due to its effectiveness of resisting the steganographic tools. Most existing coverless image steganography (CIS) methods achieve excellent robustness under non-geometric attacks. However, they do not perform well under some geometric attacks. Towards this goal, a CIS algorithm based on DenseNet feature mapping is proposed. Deep learning is introduced to extract high-dimensional CNN features which are mapped into hash sequences. For the sender, a binary tree hash index is built to accelerate index speed of searching hidden information and DenseNet hash sequence, and then, all matched images are sent. For the receiver, the secret information can be recovered successfully by calculating the DenseNet hash sequence of the cover image. During the whole steganography process, the cover images remain unchanged. Experimental results and analysis show that the proposed scheme has better robust compared with the state-of-the-art methods under geometric attacks.

Keywords: Coverless image steganography, Deep learning, DenseNet convolutional neural network, CNN features

1 Introduction

Information hiding is the most common way to protect secret information. Information encryption is the earliest means of protecting secret information, and it is using computer encryption to change the digital structure of load information in digital communication. However, the encryption technology is easy to be detected, it cannot ensure confidentiality of information, and the computational complexity is high. Therefore, researchers began to use image steganography to realize the secret transmission of important information, and it is mainly embedding the secret information into the carrier. It keeps the maximum visual similarity between the carrier and the original object, so as to avoid the abnormalities during transmission process. In the last few decades, many image steganography approaches [1–8] have been proposed. However, most of them embed the hidden secret information into the carrier to replace the hidden secret information in the pixels, which can be easily detected by steganographic analysis tools [9, 10]. Therefore, how to hide information effectively without modifying the carrier is a breakthrough and challenging point.

Springer Open

© The Author(s). 2020 **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

To radically resist the steganographic analysis tools, Zhou et al. [11] firstly proposed the concept of coverless in 2014. The "coverless" means that it can realize the transmission of secret information without modifying the carrier, and it is the most essential difference from traditional steganography which embeds secret information. Instead, the hiding process is implemented by constructing a mapping relationship between the secret information and an image or text. The first proposed concept of coverless information hiding is based on text due to the text is the most frequently and widely used carrier. The key point of coverless text steganography is to establish a mapping relationship between text features and secret information, and it mainly includes feature-based word [12] and frequency-based word [13]. Compared with the text, image contains more information. In 2015, Zhou et al. proposed the coverless image steganography method [11], which divided the image into several bolcks and generated the hash sequence generated through robust hash algorithm. Subsequently, to enhance the robustness of the algorithm, Zheng et al. [14] generated the hash sequence based on SIFT feature points. On this basis, Yuan et al. [15] proposed a CIS method based on SIFT and bag-of-features (BOF), in which robustness is further enhanced. Considering the carrier selection and robustness, Zhang et al. [16] proposed a CIS method based on DCT and LDA topic classification. Inspired by the Ref. [16], Liu et al. [17] use a preselection scheme based on DenseNet feature selected images and robust hash sequence generated by DWT transform, which effectively improves robustness and security. Then, Qin et al. [18] publish a survey of coverless information hiding to summarize the existing methods of CIS. Meanwhile, Zhou et al. [19] used a set of appropriate similar blocks of a given secret image as steganographic images to transmit the hidden image. To improve the robustness and retrieval accuracy of the Ref. [19], Luo et al. proposed a CIS method based on deep learning [20]. With the continuous development of coverless information hiding, it has become a hotspot in the field of information security and attracted many interests. However, existing CIS methods are hard to resist the content loss. At the same time, the spread of deep learning provides us new ideas. The pre-trained deep CNN model can still keep the global features of the image in a certain when image under geometric attacks. Therefore, the hash sequence mapped through CNN feature can still be recovered when it is suffering from geometric attacks.

Based on the above analysis, this paper proposed a CIS algorithm based on DenseNet feature mapping, which aims to improve the robustness of secret information under geometric attacks. This method introduces deep learning to capture the high-level semantic features of cover images, so it can effectively overcome the shortcomings of the traditional scheme. We summarize the main contributions of this work as follows:

1. We propose a novel hash mapping rules based on CNN feature, and it improves the robustness against geometric attacks. Compared with other manual features, it is more able to capture the global features of the image when losing some content. Besides, we also do a series of experiments on existing network model and chose the optimal network model (DenseNet).
2. An efficient binary tree hash index based on bitwise indexing is designed to speed up the search of cover images for secret information.
3. Extensive experiments on four datasets demonstrate that the proposed method better than the state-of-the-art CIS methods.

The remainder of this paper is organized as follows. Preliminaries are introduced in Section 2 and the details of proposed CIS algorithm based on DenseNet feature are presented in Section 3. Experimental results and discussions are given in Section 4. Section 5 concludes this paper, highlighting the main conclusions and future works.

2 Preliminaries

With the rapid development of deep learning, CNNs have made a great progress in many fields of image processing. Compared with traditional image processing algorithms, it needs a process of deep learning and efficient feature expression. Due to the explosive growth of data, a large number of CNNs have been proposed in the past decade(AlexNet [21], VGGNet [22], GoogLeNet [23], ResNet [24], and DenseNet [25]). CNNs have been widely applied to steganalysis [26], image classification, and image recognition such as CAPTCHA recognition [27, 28], food recognition [29], citrus diseases recognition [30], and image retrieval [31–33]. Therefore, most existing deep learning networks in the field of image processing either combine them or make improvements based on them. Among them, ResNet is the most widely used in industry, while DenseNet has the best effect in feature extraction.

The DenseNet's proposal is to overcome the information in the network training process may gradually disappear after repeating convolution. Therefore, it designed the Dense block structure to solve this problem. The structure of DenseNet is shown in Fig. 1.

Each layer of the DenseNe receives the output of all the previous layers. For the traditional convolutional structure, the l layer has l connections. But for the DenseNet, the l layer has $l(l-1)/2$ connections. The input of the model is x_0 and the nonlinear transformation function of each layer is $H_l(\cdot)$, the input of l_{th} is

$$x_l = H_l\left(\left[x_0, x_1, \ldots, x_{l-1}\right]\right) \tag{1}$$

where x_l represents the input feature map from the output of previous layers. Because of the excellent performance of DenseNet and the analysis of the experimental results, we use pre-trained DenseNet model to extract features.

3 Methods

The process of secret information hiding and extraction is shown in Fig. 2. The framework of the proposed approach is composed of three parts, which are implemented in four steps: generation of hash sequence, construction of binary tree hash index, coverless image steganography, and extraction of secret information. In our approach, the pre-trained DenseNet model is firstly used to extract the features of the image database. For the feature of each image, it is divided into D blocks and the feature coefficient Me of each

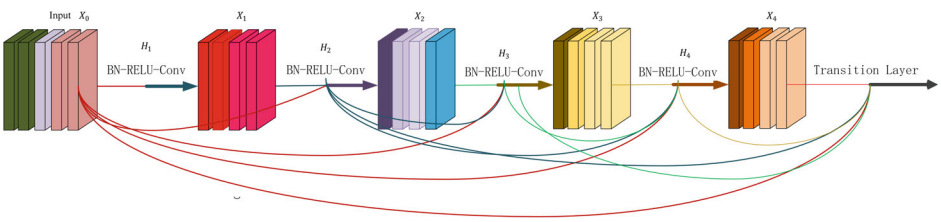

Fig. 1 The structure of DenseNet

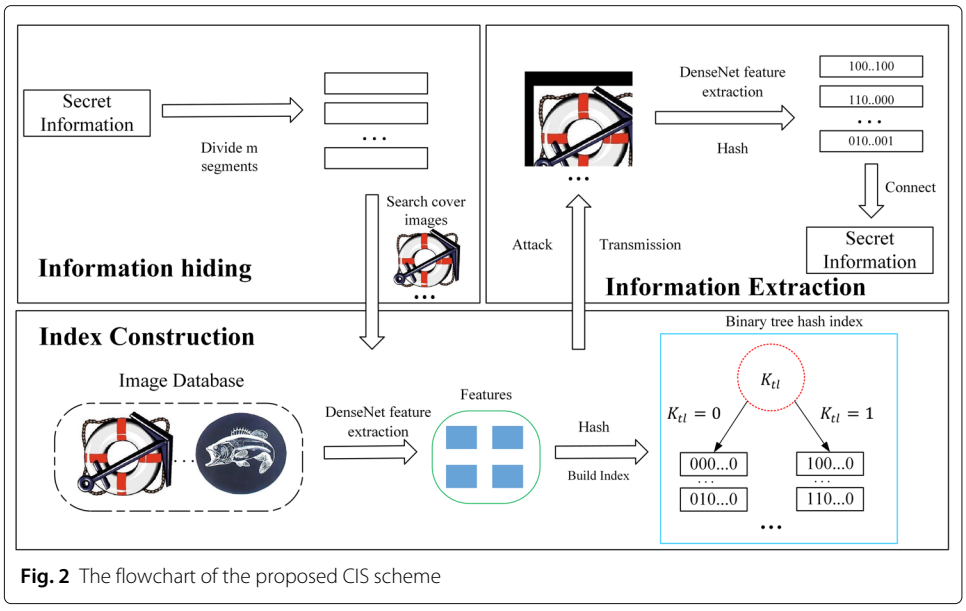

Fig. 2 The flowchart of the proposed CIS scheme

block is calculated. Then, feature coefficients *Me* are scanned by "arithmetic scan"(step-length set to *sl*) to generate the hash sequence. Next, the secret information is divided into segments equal to the hash sequence *N*, and the search cover images are searched through matching with the hash sequence. Finally, all cover images sent to the receiver in order, such that the receiver could recover secret information by calculating received images under the same hash algorithm. Considering that the length of the sequence may not be a multiple of *N*, 0 is filled in the last segment of the partition, and the number of 0 is recorded in the last image.

3.1 Generation of hash sequence

The generation method of hash sequence is crucial to the CIS based on mapping rules, which determined the steganography scheme's ability to resist attacks. Figure 3 shows the process of generating hash sequence, and the detailed steps are described as follows.

1. Firstly, we use the pre-trained DenseNet121 network to extract features of image database, It is described as

$$F_{ic} = DenseNet(Pi_{ic}) \tag{2}$$

where $DenseNet(\cdot)$ is the DenseNet extraction function, F_{ic}, which size is $1 \times 1 \times w$, is the DenseNet feature of ic_{th} image Pi_{ic} in image database, and w is the channel number of global average pooling layer.

2. Then, F_{ic} is partitioned to D blocks and the blocks B_{ib} is obtained

$$B_{ib} = \{B_1, B_2, \ldots, B_D\}, 0 < ib \leq D < w \tag{3}$$

3. For each block B_{ib}, feature coefficient Me_{ib} calculated by

$$Me_{ib} = \begin{cases} \frac{D}{w} \sum_{w(ib-1)/D}^{w \cdot ib/D} f_{iw}, & if \ 0 < ib \leq D-1 \\ \frac{D}{w} \sum_{w(ib-1)/D}^{w} f_{iw}, & if \ ib = D \end{cases}, 0 < iw < w \tag{4}$$

where f_{iw} is the feature of iw_{th} dim of F_{ic}, Me_{ib} is the mean of each feature block B_{ib} in essence.

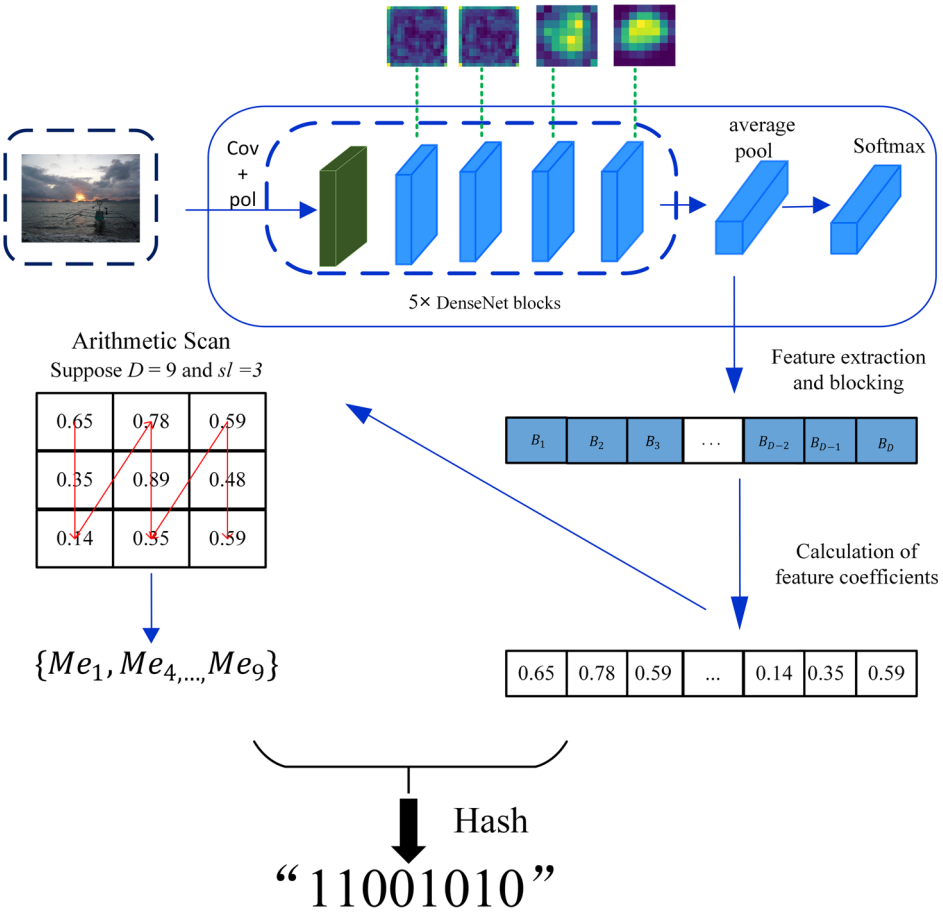

Fig. 3 The process of generating hash sequence

4. After calculating all feature coefficients, we adopt the method called "arithmetic scan" to scanning *Me*, the schematic diagram is shown in Fig. 3. For example, if the input array is $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and step-length *sl* set to 3, the output should be $\{1, 4, 7, 2, 5, 8, 3, 6, 9\}$ .Therefore, Me_{is} can be obtained with arithmetic scan order

$$Me_{is} = \{Me_1, Me_{1+sl}, \ldots, Me_2, Me_{2+sl}, \ldots, Me_{D-sl}, \ldots, Me_D\} \quad 0 < is \leq D, 0 < sl < D \tag{5}$$

5. To obtain the hash sequence, we compare each feature coefficient *Me* of adjacent block from Eq. (5), so each bit of hash sequence f_{ic} is

$$f_{ic} = \begin{cases} 1, & if\ Me_{is} > Me_{is+1} \\ 0, & \text{otherwise} \end{cases}, 0 < is < D \tag{6}$$

Finally, repeat the above steps until the hash sequences of all blocks in each image are obtained.

3.2 Construction of binary tree hash index

In the field of CIS, the search for cover images is time-consuming. To improve the matching speed of secret information and inspired by Ref.[34], we design a binary tree hash index based on bitwise indexing, its structure shown in Fig. 4. From Fig. 4, the height of

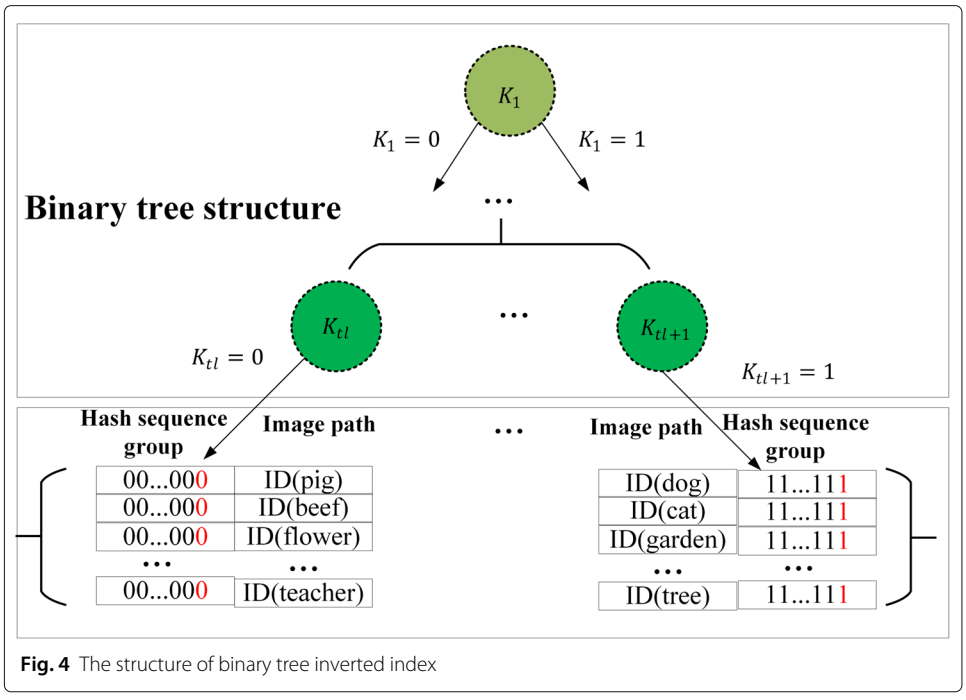

Fig. 4 The structure of binary tree inverted index

the complete binary tree is *tl*, and each leaf node corresponds to a hash sequence group composed of same hash sequence calculated by different images. Each leaf node contains the hash sequence group and the file path corresponding to the cover images.

The time complexity of binary tree hash index establishment is $O(n)$, and it is an offline phase. During the search stage, most of the existing schemes are adopting the way of sequential search, which time complexity is $O(n)$. However, the time complexity of establishing the binary tree hash index is $O(log_2 n) < O(n)$, and our approach has certain advantages in time-consuming. With the development of indexing technology, we can build such an indexing structure in existing mature databases such as MySql.

3.3 Coverless image steganography

In the field of CIS, the essence is to match the carrier image to the secret information. The steganography can be divided into four steps, and the whole steps are shown as in Algorithm 1.

1. For a given secret information S needed to be hidden, we should divide it into m segments.

$$m = \begin{cases} \frac{p}{N}, & if \quad p\%N = 0 \\ \frac{p}{N} + 1, & \text{otherwise} \end{cases} \tag{7}$$

   where the length of hash sequence is N and the length of secret information is p. If p is not a multiple of N, 0 is added in the last image and the number of 0 is recorded in added image.
2. For the image database, we need to calculate the hash sequence of all images and the details of hash sequence are described in 3.1.
3. Building a binary tree hash index.

4. For the secret information M_{cg}, the matched cover image Pc_{cg} with the same hash sequence as follows.

$$Pc_{cg} = Pi_{ic}, \quad if \quad M_{cg} = f(Pi_{ic}) \tag{8}$$

where $f(Pi_{ic})$ represents the hash sequence of ic_{th} image in image database Pi. 0 is filled in the last segment of the partition, and the number of 0 is recorded with the last image.

5. Repeat step 4 until the corresponding cover images of all secret information are obtained.
6. All cover images are sent to the receiver in order. It is important to note that to ensure the sender and receiver use the same hash algorithm, the specific trained model, step size sl of the arithmetic scan, and the number of feature blocks D used should be negotiated in advance.

Algorithm 1 : Coverless Image steganography

Input: Image database $Pi = \{Pi_1, Pi_2, \ldots, Pi_{ic}\}$, Secret information S.

Output: Cover images $Pc = \{Pc_1, Pc_2, \ldots, Pc_{cg}\}$.

Link binary tree hash database
Get Num = getNum(Pi)
for ic = 1:Num
    Extract DenseNet feature:F_{ic}=DenseNet(Pi_{ic})
    Divide DenseNet feature into D blocks
    for ib = 1:D
        For each feature block B_{ib}, using Eq.(4) to calculate the feature coefficient Me_{ib}
    end
    Using Eq.(6) to obtain the hash sequence f_{ic} according to arithmetic scan
    Update index database: **Index item**$\rightarrow$ $\{f_{ic}, ID\}$
end
Cut secret information S: M = $Cut(S)$
For cg = 1:m
    Matching cover image for M from index database: $Pc_{cg} = Pi_{ic}, if \quad M_{cg} = f(Pi_{ic})$
end
Return the selected cover image: Pc

3.4 Extraction of secret information

After receiving all cover images in order, the receiver can successfully restore the secret information by using same hash method to calculate hash sequence. This is a reversible process of secret information hidden. The pseudocode is shown in Algorithm 2, and the process is as follows.

1. For the receiver cover image Pc_{cg}, we need to extract its DenseNet feature same as Eq. (2).

2. Dividing the feature F_{cg} of each cover image into D blocks, the details described as Eq. (3).
3. Calculating the feature coefficient for each feature block B by Eq. (4).
4. According to Eqs. (5) and (6), we can generate the hash sequence of cover image Pc_{cg}.
5. Repeat steps 1–4 until all hash sequence of received cover images are obtained. According to the number of 0 recorded in the last image, subtract the corresponding 0 from the last paragraph to get the secret information.

Algorithm 2 : Extraction of Secret information

Input: Cover images $Pc = \{Pc_1, Pc_2, \ldots, Pc_{cg}\}$.

Output: Secret information S'.

for cg = 1:m
    Extract DenseNet feature:F_{cg}=DenseNet(Pc_{cg})
    Divide DenseNet feature into D blocks
    for ib = 1:D
        For each feature block B_{ib}, using Eq.(4) to calculate the feature coefficient Me_{ib}
    end
    Using Eq.(6) to obtain the hash sequence f_{cg} according to arithmetic scan
    Connect the M: S' += f_{cg}
end
Return the$M$: S'

4 Experimental results and discussions

In this section, we evaluate the performance of the proposed method for the secret information transmission and compare it with several state-of-the-art CIS methods. The details of experimental environment, datasets, and settings are described as follows.

Experimental environment: Intel (R) Core (TM) i7-7800xcpu @ 3.50g hz, 64.00 gb ram, and two NVIDIA GeForce GTX 1080 Ti GPUs are used. Deep learning adopts the Keras framework. All experiments are completed in MATLAB 2016a and Pycharm.

Datasets: Four widely used benchmark datasets, i.e., INRIA Holidays [35], ImageNet [36], Caltech-101 [37], and Caltech-256 [38] are adopted for evaluation. The detailed descriptions are as follows:

1) INRIA Holidays: It has 1491 holiday pictures and is created by Herve Jegou et al. There is no fixed category. Five hundred images are used in our experiment.
2) ImageNet: It has 15 million images and more than 22,000 categories, and it is created by the Stanford University Computer Vision Lab. 1120 images are used in our experiment.
3) Caltech-101: It has 9145 images and composed of 102 object categories, and it is created by Caltech. 1025 images are used in our experiment.
4) Caltech-256: It has 29780 images and 257 categories. Compared with Caltech-101, it has more images and rich categories. 1048 images are used in our experiment.

Table 1 The statistics of experiment in four datasets

Datasets	Holidays	ImageNet	Caltech-101	Caltech-256
Datasets size	1491	150 million	9145	29780
Category	-	22000	102	257
Experimental image	500	1120	1025	1048
Normalized image size	512×512	128×128	128×128	128×128
Text image	500	1120	1025	1048

Experimental setting: we compared the proposed method with various state-of-the-art CIS methods under capacity and robustness. In the experiment of capacity, the selected CIS methods are respectively denoted as PIX-CIS [11], HASH-CIS [14], BOF-CIS [15], DCT-CIS [16], and DWT-CIS [17]. In the experiment of robustness, due to Ref. [15] does not specify the generated hash algorithm, the remaining four methods are selected for comparisons. More details of the experimental statistics of the four datasets are summarized in Table 1. Before mapping into hash sequences, the image needs to be normalized and with different resolutions may have different normalized sizes. In this paper, the normalized image size of each dataset is consistent with Ref. [16, 17], and since the robustness experiment is tested on each image, we randomly selected the tested image from the dataset without considering to cover the value range of the message, and it does not affect the results.

4.1 Analysis of capacity

Table 2 shows the number of images needed when the same data is hidden, and the bits number of generated hash sequences determines the capacity of information hiding. The length of the hash sequences is $N(0 < N < D)$ which is determined by the number of feature block D. It's an obvious fact that the upper limit on N increases as D increases, but it is worth noting that the increase in capacity is accompanied by the expansion of the image database. The definition of N_h is:

$$N_h = \frac{p}{N} \tag{9}$$

Precisely, the capacity and robustness are mutually limiting. As can be seen from Table 2, our capacity, which is maintained at an appropriate level and obtained by robustness experiments in Section 4.2, is consistent with PIX-CIS and BOF-CIS. HASH-CIS has the maximum capacity, but it requires at least 2^{18} images which is not realistic. DWT-CIS is consistent with DCT-CIS, and they both can adjust the capacity according to the situation. In fact, our method can increase D and N adapt to realistic requirements of capacity in a good condition.

Table 2 Steganographic capacity

Method	N_h				N
	1B	10B	100B	1kB	
PIX-CIS	1	10	100	1024	8
HASH-CIS	2	6	46	457	18
BOF-CIS	1	10	100	1024	8
DCT-CIS	2∼9	7∼81	55∼801	548∼8193	1∼15
DWT-CIS	2∼9	7∼81	55∼801	548∼8193	1∼15
Proposed method (D=9)	1	10	100	1024	8

To further explore the richness of sequence mapping, we define the sequence mapping rate *Mr* to reflect capacity of cover secret information. The *Mr* definition is

$$Mr = \frac{\sum_{i=1}^{Am} P(A_i)}{2^N}, 1 < \mathrm{Am} \leq 2^N \tag{10}$$

where

$$P(A_i) = \frac{1}{Num(M_i)} \tag{11}$$

where $Num(M_i)$ is the number of images mapping to sequence M_i in image database and Am is the maximum number of sequence type mapped by all images.

In the experiment, we unified the scanning rule of mapping algorithm to observe the differences between different schemes. The experimental results are shown in Table 3. The higher the mapping rate, the smaller the number of images covering secret information 2^N. From Table 3, HASH-CIS has the highest *Mr*, while PIX-CIS, DCT-CIS, and DWT-CIS have the similar *Mr*. However, our scheme has the lowest *Mr*, which means it needs a larger image database when we want to cover the sequence. In fact, The information segment length of the existing scheme is about $N = 8$, which can maintain high robustness and be more convenient for application. This means that our method can be used effectively even if the mapping rate is low, which is also be analyzed in the last discussion.

4.2 Robustness comparison

In the process of transmission, the image is damaged by various contents inevitably. Without loss of generality, we used all selected images in the robustness experiment. The accuracy rate is calculated as:

$$RC = \frac{\sum_{cg=1}^{m} g\left(M_{cg'}\right)}{m} \tag{12}$$

where

$$g\left(M'_{cg}\right) = \begin{cases} 1, \ if \quad M'_{cg} = M_{cg} \\ 0, \quad \text{otherwise} \end{cases} \tag{13}$$

where m is the number of information segments, M_{cg} and M'_{cg} is the cgth hidden secret information and recover secret information of cover images, respectively. In the robustness experiment, to fairly compare the proposed method with the existing ones, we calculated the recovery rate of the test images selected from each image dataset. In other words, we default that the secret information segment m is equal to the number of test images, which can avoid that the random deviation of robustness calculation caused by same secret information matching different carriers because of different mapping algorithm.

Table 3 The mapping rate (%) comparison with four CIS methods in four benchmark datasets

Datasets	*Mr*				
	PIX-CIS	HASH-CIS	DCT-CIS	DWT-CIS	Proposed method
Caltech-101	29.65	37.80	30.38	30.38	11.85
Caltech-256	34.26	43.81	36.26	36.71	14.90
ImageNet	32.20	36.36	34.95	34.95	10.82
Holidays	35.61	40.68	34.57	34.57	08.86

4.2.1 Comparison under geometric attacks

To verify the robustness of proposed method, we compare it with the four state-of-the-art CIS methods [11, 14, 16, 17]. More details are described as follows.

The existing methods have shown excellent robustness in conventional noise, but it is also a challenge to resist geometric attacks. In this experiment, we will test the robustness of our approach to the geometric image attacks. Figure 5 shows the attacks on the cover images. Several kinds of geometric attacks, which are applied to the cover images, are described below. The robustness of all the methods on Holidays, ImageNet, Caltech-101, and Caltech-256 are reported in Figs. 6, 7, 8, and 9.

1. Centered cropping with ratios of 5%, 10%, 15%, and 20%, respectively.
2. Edge cropping with ratios of 5%, 10%, 15%, and 20%, respectively.
3. Rotation. The rotation angles are 5°, 10°, 15°, and 20°, respectively.
4. Translation. Since the image size of the databases is different, the translation distances in Holidays database are (80, 50), (160, 100), (240,150), and (320, 200), respectively. The translation distances in the other three databases are (16, 10), (36, 20), (40, 25), and (45,30), respectively.

From the experimental results in Figs. 6, 7, 8, and 9, it can be found that the overall extraction accuracy of proposed method is obviously higher than that of existing CIS methods. From the respective of datasets, the overall robustness performance in Holidays is slightly worse than other three datasets, which is opposed to performance under non-geometric attacks will be reported in the next section. From the respective attack ways, the performance under edge cropping decreases the most as the attack level increases but achieve the highest extraction accuracy. Especially under edge cropping with ratios of 5%, previous methods achieve extraction accuracy of 100% which are slightly higher than proposed method. Under center cropping, rotation, and translation, the robustness performance of all methods varies very gently as the level of attack increases, but the proposed method achieved optimal performance. Therefore, the experimental results clearly show that proposed method has better robustness under geometric attacks.

4.2.2 Comparison under non-geometric attacks

To fully verify the effectiveness of the proposed method, we also test the robustness of the proposed method under non-geometric attack. Figure 10 show the several typical image attack ways and the specific parameters are described below.

1. JPEG compression with a fact of 10.

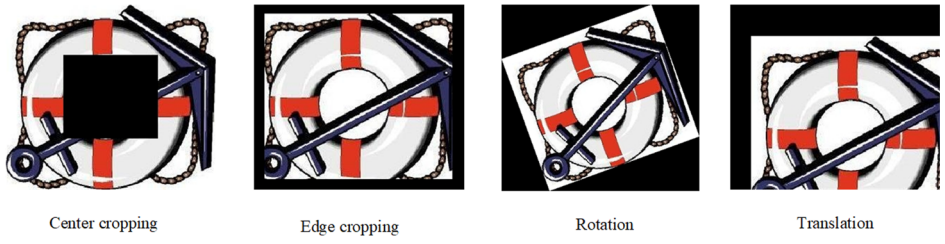

Fig. 5 The geometric attack ways on the cover image, center cropping (20%), edge cropping(20%), Rotation(20°), and translation: (45,30)

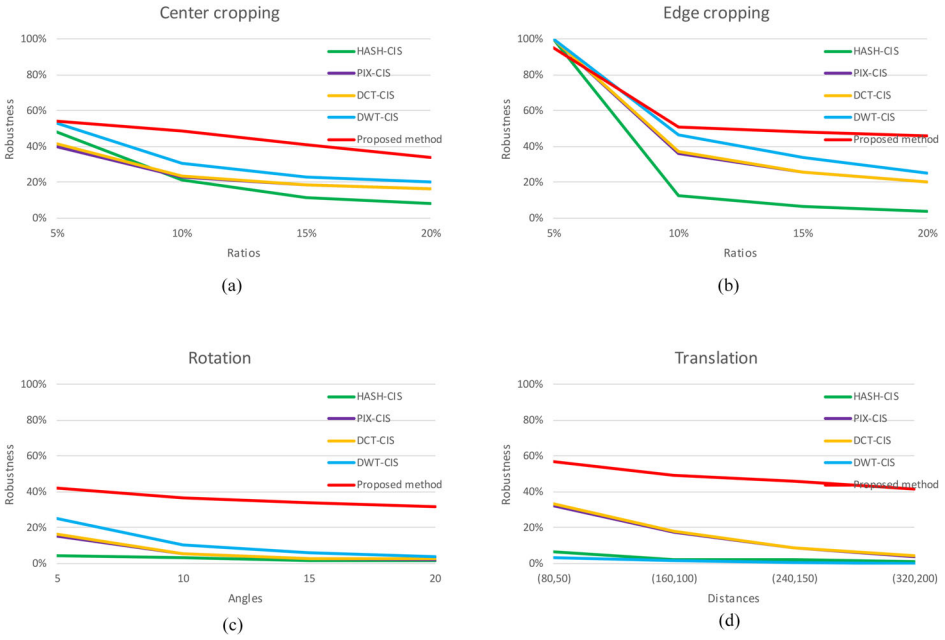

Fig. 6 Robustness curves on Holidays with respect to different geometric attacks: **a** center cropping, **b** edge cropping, **c** rotation, and **d** translation

2. Gauss noise. The mean μ is 0, and the variances σ are 0.001.
3. Gaussian filtering with 3 $\times$3 window.
4. Scaling with ratio 3.
5. Color histogram equalization.
6. Gamma correction with 0.6.

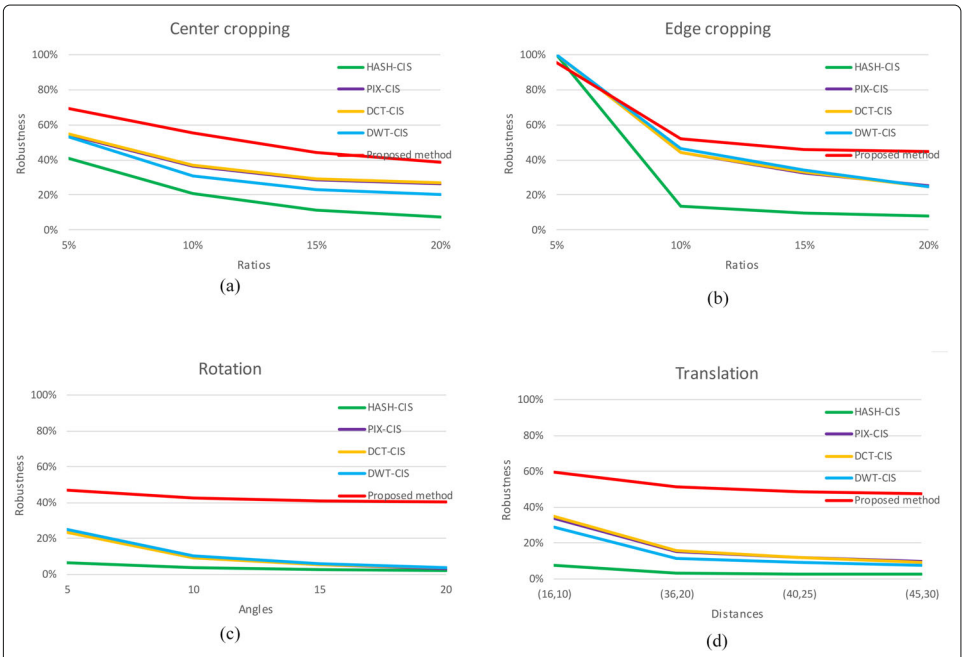

Fig. 7 Robustness curves on ImageNet with respect to different geometric attacks: **a** center cropping, **b** edge cropping, **c** rotation, and **d** translation

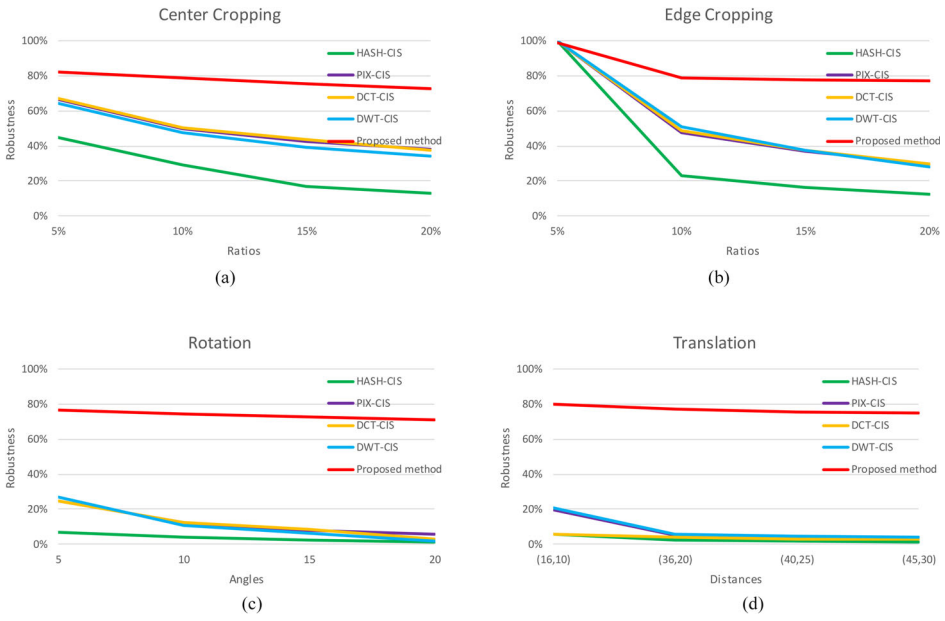

Fig. 8 Robustness curves on Caltech-101 with respect to different geometric attacks: **a** center cropping, **b** edge cropping, **c** rotation, and **d** translation

In the experiment, we also compare the proposed method with four existing CIS methods in four datasets. We adopt six widely used typical attack ways, i.e., JPEG compression, Gauss noise, Gaussian filtering, scaling, color histogram equalization, and gamma correction. The comparison results are shown in Table 4. From Table 4, we can find that the existing CIS methods perform excellent under typical image attack, which has been

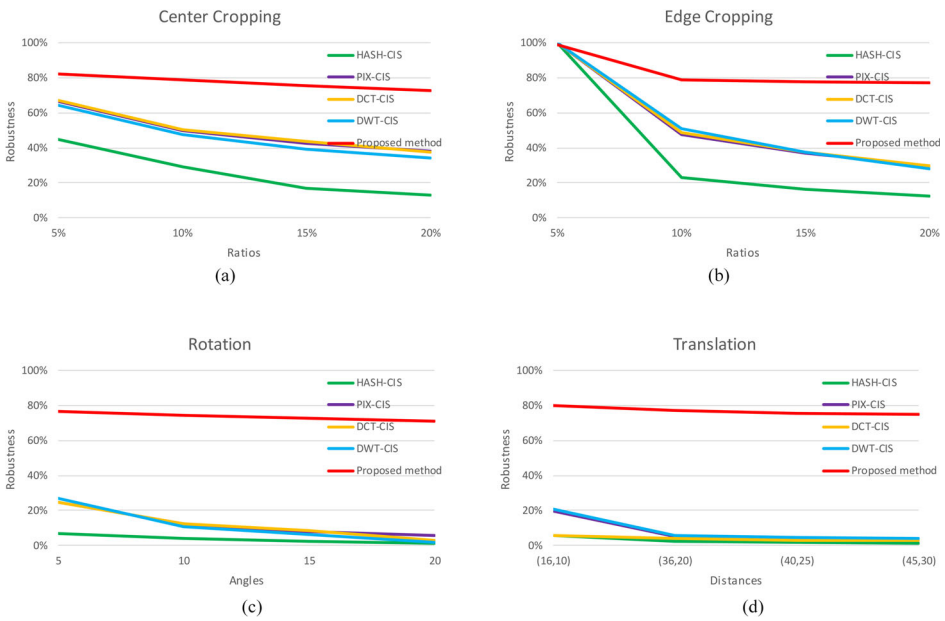

Fig. 9 Robustness curves on Caltech-256 with respect to different geometric attacks: **a** center cropping, **b** edge cropping, **c** rotation, and **d** translation

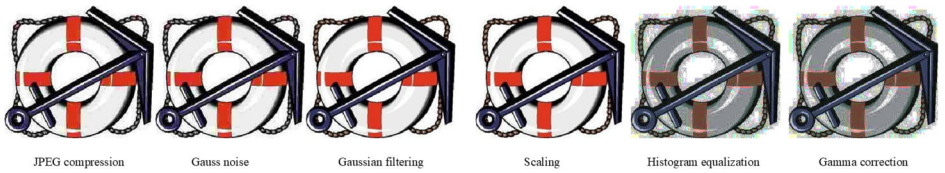

Fig. 10 The typical non-geometric attack ways on the cover image

proved experimentally in our previous work of DWT-CIS [17]. For datasets, the overall robustness performance in Holidays is more robustness than other three datasets, which is opposed to performance under geometric attacks. Compared with state-of-art CIS methods, our method only achieves optimal performance under color histogram equalization and gamma correction, which implies that our method does not have absolute advantage under non-geometric attacks. For traditional attack ways such as compression, filtering and so on, the existing CIS methods have achieved high robustness. However, the improvement of robust performance under geometric attacks is the most challenging task at present. Therefore, our method still has high potential research value. At the same time, we can choose the appropriate method according to the specific situation in the actual application process.

4.3 Analysis of robustness

4.3.1 Parameter analysis

In this section, we empirically analyze the sensitivity of D(the number of feature block) on robustness. In the experiment, D is varied from the range of {9,13,16,20} and the used

Table 4 Robustness (%) comparison with four CIS methods in four benchmark datasets

Dataset	Method	Compression	Gauss noise	Gauss filtering	Scaling	C-H-E	Gramma
Holidays	HASH-CIS	74.00	94.80	96.20	97.40	28.20	41.00
	PIX-CIS	**95.40**	99.80	**100.00**	**100.00**	72.80	82.80
	DCT-CIS	94.80	**100.00**	99.80	**100.00**	**73.00**	**83.00**
	DWT-CIS	94.38	99.73	99.91	99.91	70.98	79.55
	Proposed method	62.40	81.80	92.20	89.00	54.60	71.20
ImageNet	HASH-CIS	52.77	87.23	90.18	93.04	23.84	33.84
	PIX-CIS	**95.27**	**99.64**	**99.91**	99.82	**71.07**	79.73
	DCT-CIS	92.77	99.82	**99.91**	**100.00**	69.91	78.75
	DWT-CIS	94.29	**99.64**	**99.91**	99.91	70.89	79.29
	Proposed method	49.20	89.38	89.11	96.70	69.11	**84.29**
Caltech-101	HASH-CIS	55.41	89.27	89.76	92.00	27.12	42.15
	PIX-CIS	94.63	97.66	99.51	99.61	66.54	66.54
	DCT-CIS	94.54	98.05	**100.00**	99.90	67.02	80.88
	DWT-CIS	**95.61**	**99.51**	99.90	**100.00**	67.80	79.12
	Proposed method	80.59	92.10	95.32	99.12	**81.27**	**89.85**
Caltech-256	HASH-CIS	52.10	87.98	88.55	93.80	19.94	41.70
	PIX-CIS	93.03	93.32	99.33	99.62	64.41	82.06
	DCT-CIS	91.60	94.08	99.71	99.81	64.50	82.54
	DWT-CIS	**94.37**	**95.42**	**99.90**	**100.00**	66.79	82.92
	Proposed method	73.57	87.12	93.89	98.57	**75.19**	**87.98**

datasets is Caltech-101. Attack ways and the specific parameters and experiment results are shown in Table 5. From Table 5, we see that with the increase of D, the robustness has an obviously downward trend. Theoretically, the larger D is, the lower the dimension of feature block is and the lower the anti-attack stability is. Therefore, the experimental results are in line with the theoretical analysis. However, we learn that robustness increases rather than decreases from D=16 to 20. In other words, D has a critical value and it is in the range of 16, which indicate that D is not completely inversely related to robustness. Finally, the results demonstrate that D=9 is best for our method to obtain superior performance.

4.3.2 CNN model analysis

To explore the effect of different CNN model on robustness, four CNN model, i.e., InceptionResNetV2, ResNet50, InceptionV3, and DenseNet121 are adopted for evaluation. We select (D=9, N=8) and Caltech-101 for this experiment and report the performance results with varying CNN model, which all used ImageNet for pre-training. Form Table 6, we observe that DenseNet12 achieve optimal performance and InceptionResNetV2 maintains comparable performance with InceptionV3, ResNet50 obtain the worst robustness. Although these models are suitable for image classification, the performance of classification remains consistent with robustness in the CIS. These results demonstrate that a good classified CNN model can improve the robustness in CIS.

4.4 Analysis of safety

In the field of traditional steganography, the secret information is embedded in the cover image. Therefore, the modifications in cover image can be detected by steganography analysis tools. The advantage of CIS is that it use natural unmodified image as carriers. In this paper, our method establishes the mapping rules by DenseNet features between secret information and cover images, and it mainly converts information hiding into searching cover images, which can effectively resist the detection of steganographic analysis tools.

4.5 Discussion

All the aforementioned experiments have validated the effectiveness of the proposed method. In this section, we will further discuss some problems encountered during the

Table 5 Robustness(%) with respect to the different number of feature block in Caltech-101

Attack	Parameter	(D=9, N=8)	(D=13, N=8)	(D=16, N=8)	(D=20, N=8)
Compression	Q(10)	**80.59**	54.93	45.66	46.15
Gauss Noise	σ(0.001)	**92.10**	76.29	66.24	63.12
Gauss filtering	(3 × 3)	**95.32**	83.41	81.27	76.78
Scaling	3	**99.12**	97.66	96.20	96.88
C-H-E	–	**81.27**	49.95	36.68	38.63
Gramma	0.6	**89.85**	70.93	52.00	63.32
Centered cropping	20%	**72.88**	47.71	32.88	39.51
Edge cropping	20%	**76.98**	60.49	35.51	36.10
Rotation	20°	**71.02**	20.59	17.66	19.90
Translation	(45,30)	**75.02**	56.39	38.34	39.71

Table 6 Robustness(%) with respect to the different CNN model in Caltech-101

Attack	Parameter	InceptionResNetV2	ResNet50	InceptionV3	DenseNet121
Compression	Q(10)	32.10	27.80	34.44	**80.59**
Gauss noise	$\sigma(0.001)$	57.17	47.32	55.90	**92.10**
Gauss filtering	(3×3)	71.41	62.83	67.02	**95.32**
Scaling	3	95.02	93.85	91.61	**99.12**
C-H-E	–	29.37	21.56	32.88	**81.27**
Gramma	0.6	55.61	48.10	53.27	**89.85**
Centered cropping	20%	5.56	15.90	15.71	**72.88**
Edge cropping	20%	41.95	23.90	39.41	**76.98**
Rotation	20°	12.10	6.24	16.78	**71.02**
Translation	(45,30)	23.61	21.66	24.59	**75.02**

experiment and give analysis and suggestions. It is mainly divided into the following two parts.

(1) In the field of CIS, in addition to analyzing the steganographic capacity which is an ideal value, we also need to consider the number of images corresponding to a hash sequence—that is, the number of repeated hash sequences. The repetition of the hash sequence is necessary to provide more cover images for the same secret information segment. However, too many repeated hash sequences can lead to secret information that may not be fully expressed, which can happen with smaller image databases. Therefore, how to balance the relationship between the two is also a factor we should consider when applying to specific application. In our experiment, the number of repeated hash sequences is corresponding to the basis of the mapping algorithm and the scanning rule. Compared to the existing CIS method, our approach is more sensitive in this regard. The purpose of this article, of course, is to focus on methodological heuristics. At the same time, increasing the number of image database should be a good solution.

(2) In the above experiment, we verified that the classification ability of a CNN network is positively correlated with the steganographic ability of CIS method. However, we have not considered what the result of the overfitting network will be. In our experiment, the pre-trained network models are all trained through the ImageNet dataset (15 million images) while robustness experiments usually test about 1000 images. In fact, we also fine-tuned the network during the experiment with the test images. After only one or two rounds of training, the classification accuracy reached 100%. However, the robustness of testing in the field of CIS is very poor. Although we have also done the data augmentation which added to the noise image together as the training set, the effect is still poor. Obviously, this kind of overfitting network does not apply to the above experimental conclusions. In theory, if we do data augmentation on ImageNet, the robustness should improve. However, it is difficult to experiment with such calculation cost.

5 Conclusion

This work focuses on the challenging problem of CIS. We propose a novel CIS scheme and choose pre-train CNN model to extract high-level semantic information of image database, then map it to a robust hash sequence. The stability of CNN feature against geometric attacks can improve the robustness of steganography. During the whole process, the cover images have not been modified so that this scheme can resist the detection of steganalysis. Compared to the existing CIS methods, this proposed method has higher

efficiency. Extensive experiments demonstrate that this method achieves satisfactory extraction accuracy under geometric attacks than the state-of-the-art CIS methods. In the future work, we will try to optimize the scheme and enhance the robustness against non-geometric attacks.

Abbreviations

CIS: Coverless image steganography; CNN: Convolutional neural networks; SIFT: Scale invariant feature transform; BOF: Bag-of-features; DCT: Discrete cosine transformation; LDA: Latent dirichlet allocation; DWT: Discrete wavelet transformation; C-H-E: Color histogram equalization

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Authors' contributions

QL designed the algorithm. XYX carried out the experiments and drafted the manuscript. JHQ gave suggestions on the structure of manuscript and participated in modifying the manuscript. YT built the dataset and gave suggestions on the experiment alanalysis. YQ participated in the survey of large motion and gave suggestions on the experiment analysis. The authors read and approved the final manuscript.

Funding

This work was supported in part by the National Natural Science Foundation of China under Grant 61772561, in part by the Key Research and Development Plan of Hunan Province under Grant 2018NK2012 and 2019SK2022, in part by the Science Research Projects of Hunan Provincial Education Department under Grant 18A174 and 19B584, in part by the Degree & Postgraduate Education Reform Project of Hunan Province under Grant 2019JG YB154, in part by the Postgraduate Excellent teaching team Project of Hunan Province under Grant [2019]370-133, and in part by the Postgraduate Education and Teaching Reform Project of Central South University of Forestry & Technology under Grant 2019JG013.

Availability of data and materials

Please contact author for data requests.

Competing interests

The authors declare that they have no competing interests.

Received: 25 February 2020 Accepted: 29 July 2020
Published online: 09 September 2020

References

1. X. Zhang, S. Wang, Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Process. Lett. **12**(1), 67–70 (2004)
2. C. Yang, C. Weng, S. J. Wang, H. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Secur. **3**(3), 488–497 (2008)
3. W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inf. Forensics Secur. **5**(2), 201–214 (2010)
4. T. Pevnỳ, T. Filler, P. Bas, in *International Workshop on Information Hiding*, Using high-dimensional image models to perform highly undetectable steganography, (2010), pp. 161–177. https://doi.org/10.1007/978-3-642-16435-4_13
5. V. Holub, J. Fridrich, in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, Designing steganographic distortion using directional filters, (2012), pp. 234–239. https://doi.org/10.1109/wifs.2012.6412655
6. Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan, N. N. Xiong, A robust watermarking scheme in YCBCR color space based on channel coding. IEEE Access. **7**, 25026–25036 (2019). https://doi.org/10.1109/ACCESS.2019.2896304
7. Y. Zhang, X. Luo, Y. Guo, C. Qin, F. Liu, Multiple robustness enhancements for image adaptive steganography in lossy channels. IEEE Trans. Circ. Syst. Video Technol. (2019). https://doi.org/10.1109/tcsvt.2019.2923980
8. C. Qin, W. Zhang, F. Cao, X. Zhang, C.-C. Chang, Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection. Signal Process. **153**, 109–122 (2018)
9. J. Qin, X. Sun, X. Xiang, C. Niu, Principal feature selection and fusion method for image steganalysis. J. Electron. Imaging. **18**(3), 033009 (2009). https://doi.org/10.1117/1.3206961
10. T. Qiao, X. Luo, T. Wu, M. Xu, Z. Qian, Adaptive steganalysis based on statistical model of quantized DCT coefficients for jpeg images. IEEE Trans. Dependable Secure Comput. (2019). https://doi.org/10.1109/tdsc.2019.2962672
11. Z. Zhou, H. Sun, R. Harit, X. Chen, X. Sun, in *International Conference on Cloud Computing and Security*, Coverless image steganography without embedding, (2015), pp. 123–132
12. Z. Zhou, J. Qin, X. Xiang, Y. Tan, Q. Liu, N. N. Xiong, News text topic clustering optimized method based on TF-IDF algorithm on spark. Comput. Mater. Continua. **62**(1), 217–231 (2020). https://doi.org/10.32604/cmc.2020.06431
13. J. Zhang, H. Huang, L. Wang, H. Lin, D. Gao, Coverless text information hiding method using the frequent words hash. Int. J. Netw. Secur. **19**(6), 1016–1023 (2017)
14. S. Zheng, L. Wang, B. Ling, D. Hu, in *International Conference on Intelligent Computing*, Coverless information hiding based on robust image hashing, (2017), pp. 536–547. https://doi.org/10.1007/978-3-319-63315-2_47
15. C. Yuan, Z. Xia, X. Sun, Coverless image steganography based on sift and BOF. J. Int. Technol. **18**(2), 435–442 (2017)
16. X. Zhang, F. Peng, M. Long, Robust coverless image steganography based on DCT and LDA topic classification. IEEE Trans. Multimedia. **20**(12), 3223–3238 (2018)

17. Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, Y. Luo, Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. Knowl-Based Syst. **192**, 105375–105389 (2020). https://doi.org/10.1016/j.knosys.2019.105375
18. J. Qin, Y. Luo, X. Xiang, Y. Tan, H. Huang, Coverless image steganography: a survey. IEEE Access. **7**, 171372–171394 (2019). https://doi.org/10.1109/ACCESS.2019.2955452
19. Z. Zhou, Y. Mu, Q. J. Wu, Coverless image steganography using partial-duplicate image retrieval. Soft Comput. **23**(13), 4927–4938 (2019)
20. Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, L. Xiang, Coverless real-time image information hiding based on image block matching and dense convolutional network. J. Real-Time Image Process., 1–11 (2019). https://doi.org/10.1007/s11554-019-00917-3
21. A. Krizhevsky, I. Sutskever, G. E. Hinton, in *Advances in Neural Information Processing Systems*, Imagenet classification with deep convolutional neural networks (Advances in neural information processing systems, 2012), pp. 1097–1105
22. K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition (2014). arXiv preprint arXiv:1409.1556
23. C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, A. Rabinovich, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Going deeper with convolutions, (2015), pp. 1–9. https://doi.org/10.1109/cvpr.2015.7298594
24. K. He, X. Zhang, S. Ren, J. Sun, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Deep residual learning for image recognition, (2016), pp. 770–778. https://doi.org/10.1109/cvpr.2016.90
25. G. Huang, Z. Liu, L. Van Der Maaten, K. Q. Weinberger, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Densely connected convolutional networks, (2017), pp. 4700–4708. https://doi.org/10.1109/cvpr.2017.243
26. L. Xiang, G. Guo, J. Yu, V. S. Sheng, P. Yang, A convolutional neural network-based linguistic steganalysis for synonym substitution steganography. Math. Biosci. Eng. **17**(2), 1041–1058 (2020)
27. W. Ma, J. Qin, X. Xiang, Y. Tan, Y. Luo, N. N. Xiong, Adaptive median filtering algorithm based on divide and conquer and its application in captcha recognition. Comput. Mater. Continua. **58**(3), 665–677 (2019). https://doi.org/10.32604/cmc.2019.05683
28. J. Wang, J. Qin, X. Xiang, Y. Tan, N. Pan, Captcha recognition based on deep convolutional neural network. Math. Biosci. Eng. **16**(5), 5851–5861 (2019). https://doi.org/10.3934/mbe.2019292
29. L. Pan, J. Qin, H. Chen, X. Xiang, C. Li, R. Chen, Image augmentation-based food recognition with convolutional neural networks. Comput. Mater. Continua. **59**(1), 297–313 (2019). https://doi.org/10.32604/cmc.2019.04097
30. W. Pan, J. Qin, X. Xiang, Y. Wu, Y. Tan, L. Xiang, A smart mobile diagnosis system for citrus diseases based on densely connected convolutional networks. IEEE Access. **7**, 87534–87542 (2019). https://doi.org/10.1109/ACCESS.2019.2924973
31. H. Li, J. Qin, X. Xiang, L. Pan, W. Ma, N. N. Xiong, An efficient image matching algorithm based on adaptive threshold and RANSAC. IEEE Access. **6**, 66963–66971 (2018). https://doi.org/10.1109/ACCESS.2018.2878147
32. J. Qin, H. Li, X. Xiang, Y. Tan, W. Pan, W. Ma, N. N. Xiong, An encrypted image retrieval method based on harris corner optimization and LSH in cloud computing. IEEE Access. **7**, 24626–24633 (2019). https://doi.org/10.1109/ACCESS.2019.2894673
33. L. Xiang, X. Shen, J. Qin, W. Hao, Discrete multi-graph hashing for large-scale visual search. Neural Process. Lett. **49**(3), 1055–1069 (2019). https://doi.org/10.1007/s11063-018-9892-7
34. D. Schlegel, G. Grisetti, HBST: a hamming distance embedding binary search tree for feature-based visual place recognition. IEEE Robot. Autom. Lett. **3**(4), 3741–3748 (2018)
35. H. Jegou, M. Douze, C. Schmid, in *European Conference on Computer Vision*, Hamming embedding and weak geometric consistency for large scale image search, (2008), pp. 304–317. https://doi.org/10.1007/978-3-540-88682-2_24
36. A. Krizhevsky, I. Sutskever, G. E. Hinton, in *Advances in Neural Information Processing Systems*, Imagenet classification with deep convolutional neural networks, (2012), pp. 1097–1105
37. L. Fei-Fei, R. Fergus, P. Perona, in *2004 Conference on Computer Vision and Pattern Recognition Workshop*, Learning generative visual models from few training examples: an incremental Bayesian approach tested on 101 object categories, (2004), pp. 178–178. https://doi.org/10.1109/cvpr.2004.383
38. G. Griffin, A. Holub, P. Perona, Caltech-256 object category dataset, Technical Report 7694 Caltech, (2007)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.