Reversible Sub-Feature Retrieval: Toward Robust Coverless Image Steganography for Geometric Attacks Resistance

Qiang Liu, Xuyu Xiang*, Jiaohua Qin, Yun Tan, and Qin Zhang
College of Computer Science and Information Technology, Central South University of Forestry & Technology
Changsha, 410004, China
[e-mail: liuqiang_ch@163.com, xyuxiang@csuft.edu.cn, qinjiaohua@163.com, tantanyun@hotmail.com, 18915966589@163.com]
*Corresponding author: Xuyu Xiang

Received Septebmer 6, 2020; revised January 20, 2021; accepted February 9, 2021; published March 31, 2021

Abstract

Traditional image steganography hides secret information by embedding, which inevitably leaves modification traces and is easy to be detected by steganography analysis tools. Since coverless steganography can effectively resist steganalysis, it has become a hotspot in information hiding research recently. Most coverless image steganography (CIS) methods are based on mapping rules, which not only exposes the vulnerability to geometric attacks, but also are less secure due to the revelation of mapping rules. To address the above issues, we introduced camouflage images for steganography instead of directly sending stego-image, which further improves the security performance and information hiding ability of steganography scheme. In particular, based on the different sub-features of stego-image and potential camouflage images, we try to find a larger similarity between them so as to achieve the reversible steganography. Specifically, based on the existing CIS mapping algorithm, we first can establish the correlation between stego-image and secret information and then transmit the camouflage images, which are obtained by reversible sub-feature retrieval algorithm. The received camouflage image can be used to reverse retrieve the stego-image in a public image database. Finally, we can use the same mapping rules to restore secret information. Extensive experimental results demonstrate the better robustness and security of the proposed approach in comparison to state-of-art CIS methods, especially in the robustness of geometric attacks.

Keywords: Coverless Image Steganography, Camouflage Image, Sub-Feature, Reversible Retrieve

http://doi.org/10.3837/tiis.2021.03.014 **ISSN : 1976-7277**

1. Introduction

With the rapid development of multimedia technology and the enhancement of people's information interaction, information security has become the focus of people's attention. As an effective means of information security, information hiding mainly embeds the secret information into multimedia data, it is divided into watermarking and steganography according to different applications. Watermarking is the process of marking digital media to realize copyright protection [1], while steganography is mainly used for covert communication [2-6]. Different steganography schemes consider different types of media data as carriers, including text, video, audio and so on. Traditional image steganography is to make tiny changes in the space domain or transform domain to embed the secret information. However, these modification traces will cause some distortion in the cover images, which make the steganographic analysis [7] possible and lead to the disclosure of secret information.

To radically resist the steganographic detection, the researchers proposed the coverless information hiding without any modification-"coverless image Steganography". It is not necessary to designate and modify a carrier to hide the secret information. Instead, the hiding process is implemented by finding an image [8], text [9] or video [10] that already establish a relationship with the secret information. Zhou et al. [8] first proposed a CIS method based on robust hash algorithm, which divides the image into 9 blocks and generates an 8-bit hash sequence according to adjacent coefficients. Subsequently, many CIS schemes [11-17] were proposed to improve robustness and security. Zheng et al. proposed a robust hash algorithm based on SIFT Features [11] and then Yuan et al. use SIFT and bag-of-features (BOF) [12] to further optimize the scheme. Due to the frequency domain has good stability, Zhang et al. proposed a CIS technology based on DCT and LDA topic classification [13]. Inspired by the work of Ref. [13], Liu et al. proposed a CIS technology based on image retrieval of DenseNet features and DWT sequence mapping [14] to further improve robustness and security. Moreover, Zhou et al. used a set of appropriate similar blocks of a given secret image as steganographic images to transmit the hidden image and proposed a new CIS method [15]. Subsequently, Luo et al. introduced the deep learning and DCT to improve the robustness and retrieval accuracy of Ref. [16] and also proposed to use Faster RCNN to detect muti-object of image and establish mapping rules [17]. In the same year, Qin et al. summarized the above methods [18]. With the continuous iteration and optimization of the scheme, the mapping expression shows a bottleneck. From the perspective of robustness, although the above methods have achieved excellent performances in non-geometric attacks, the map-based also approaches expose the vulnerability to geometric attacks. Due to the existing mapping rules depending on the spatial position comparison of the partition coefficient, once the stego-image is attacked by geometrically, the spatial position will be changed and the mapping rules cannot adapt to geometric attack, so that the secret information fails to extract. From the perspective of security, although the mapping rule has certain stability, we still cannot completely exclude the possibility of rule leakage or cracking because the existing hash algorithm is relatively simple.

Therefore, to address the above issues for CIS, one effective way involves designing a steganographic scheme that is able to send fake stego-image without carrying confidential information to the receiver. The receiver can restore the stego-image and secret information with this "fake"-camouflage image. To this end, by conducting extensive experiments, we find a phenomenon that although the two images are very similar, their corresponding hash sequences are different, which is shown in **Fig. 1**. It means that the technology of image retrieval can be introduced to select camouflage images. However, the reversibility of two

images in direct retrieval requires very high similarity between them. In fact, there are still a large number of irreversible images in image databases. To improve the reversibility performance, we can try to use the sub-features of different dimensions instead of limiting ourselves to use the whole dimension feature for retrieval.

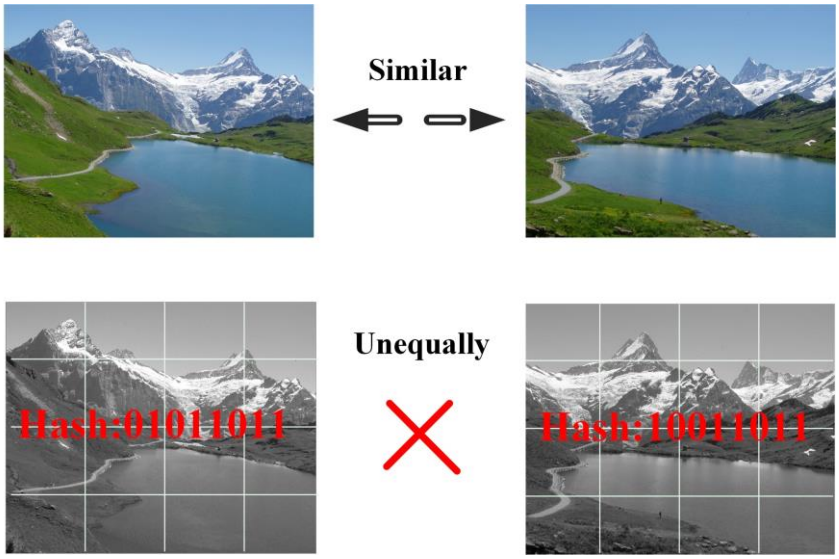


Fig. 1. Similar images correspond to different hash sequences, which length is set as 8, and the hash algorithm adapted from [8](As shown in **Fig. 8**). The tested images are from the Holidays database with a high resolution, and the image size is normalized to 512×512.

Motivated by the above phenomenon and analysis, we propose a reversible sub-feature retrieval (RSR-CIS) scheme for steganography. Specifically, instead of directly sending stego-image, we compute the distances of sub-features of each steganography image and its first K similar images and then selected reversible objects as camouflage images. By reversible retrieving the stego-image and camouflage image, we successfully convert the mapping steganography to the retrieval steganography, which makes up for the deficiency of map-based methods effectively. The main contributions of this paper are summarized as follows:

1. The observation of the reversible properties of the sub-feature retrieval. As reported in Section 3.1, we observe that direct reversible retrieval of images is easier to find within K similar images and some local feature of the image is likely to make images more similar to each other in image retrieval. Based on the above observation, it motivates us to suppose the similar sub-features can be found in similar images to make their retrieval reversible in the irreversible case. The conjecture has been verified by extensive experiments.
2. The reversible sub-feature retrieval (RSR-CIS) scheme. The proposed CIS scheme can stably match the camouflage image for stego-image. To further improve the retrieval accuracy, we introduce deep learning, use the feature of high-level semantic CNN as the retrieval benchmark, and effectively combine cutting-edge image retrieval technology.

2. Related Work

Early image retrieval methods are all based on manual features of images, where SIFT [19] is typical. Its local feature descriptors are not easily affected by translation, rotation, view

transformation and messy scenes, etc., and the extraction speed is fast, which is widely used in theory and practical production. However, because it cannot represent the high-level semantic information of the image well, it obviously cannot adapt to the task with higher requirements. At the same time, studies show that CNN is able to extract the deep semantics of images, showing remarkable performance in the field of computer vision, which are elaborated as follows:

The deep learn-based approach "learns" the high-level semantic features of the image by iteratively running a simple extraction process, and converges to different model parameters for different datasets. Due to the explosive growth of data, a large number of CNNs have been proposed in the past decade (AlexNet [20], VGGNet [21], GoogLeNet [22], ResNet [23] and DenseNet [24]). CNNs have been widely applied to steganalysis [25], image classfication, image recognition such as CAPTCHA recognition [26, 27], food recognition [28], citrus diseases recognition [29] and image retrieval [30-32] et al.

DenseNet is one of CNN's most popular networks, it makes significant innovations based on ResNet, such as alleviating the disappearance of gradients, enhancing the propagation of features, reducing the number of parameters, and promoting the development of related fields of deep learning. The DenseNet network structure is shown in **Fig. 2**. Therefore, the DenseNet feature is adopted as the retrieval benchmark in our work.

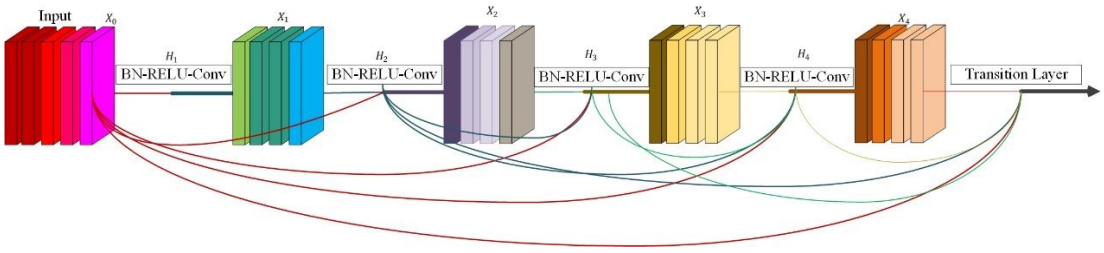


Fig. 2. The network structure of DenseNet

3. The Proposed Reversible Sub-feature Retrieval Scheme

In Section 3.1, we introduce the motivation of the reversible sub-feature retrieval scheme. Then, we verify that stego-image can always find a camouflage image among its retrieval similar *K* images by experiments. In Section 3.2, we detail the proposed reversible sub-feature retrieval scheme for camouflage image generation.

3.1 Motivation

In image retrieval, there is a research on the problem of nearest neighbor reversibility. A very interesting phenomenon simple diagram is shown in **Fig. 3**. Capital letters represent the image, and the radius of the circle represents the distance between the image shown at the center of the circle and the image in its third neighbor, it can be found in the **Fig. 3** that the nearest neighbor of image A contains G, but the A is not belong to nearest neighbor retrieved by image G. In the case of the diagram, image A and image G don't satisfy the nearest neighbor reversibility.

In fact, nearest neighbor reversibility can be used to improve retrieval performance [33]. In general, it can improve retrieval order based on whether or not the nearest neighbor relationship is satisfied. However, if we want to use this property directly for our task, we need a huge cost of on-line computation and auxiliary information. Therefore, we decide to do it in

a more direct way. Extending to our concerns, our required immediate neighbours may be even stricter. Assuming that k_1 and k_2 represent the number of nearest neighbours of image A and image B , C , G respectively. In our task, $k_1=k_2=1$ is the condition for reversible retrieval. In particular, the experiments and observations given below will clarify the idea of CIS in this paper.

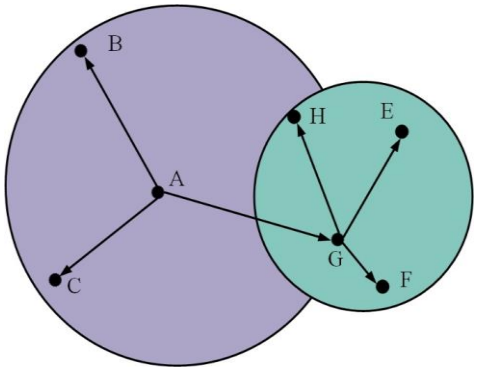


Fig. 3. Toy example of neighbor nonreversibility in image retrieval

Observation 1. For query images, most of its reversible objects can be found in the K nearest neighbors.

To study the relationships between reversible objects in *K* nearest neighbors. We conducted an experiment on Holidays dataset [34] to see the correlation of the retrieved results respectively. In fact, the reversible phenomenon of the nearest neighbor in image retrieval is also common. **Fig. 4** shows the actual result of image retrieval conducted in Holidays dataset. The image in the upper left corner is the original query image, the image in the left vertical column is the similar image retrieved from the original query image, in which the truly similar images are distributed in the first, second and first, third rows respectively, and the black outer box image is the reversible object.

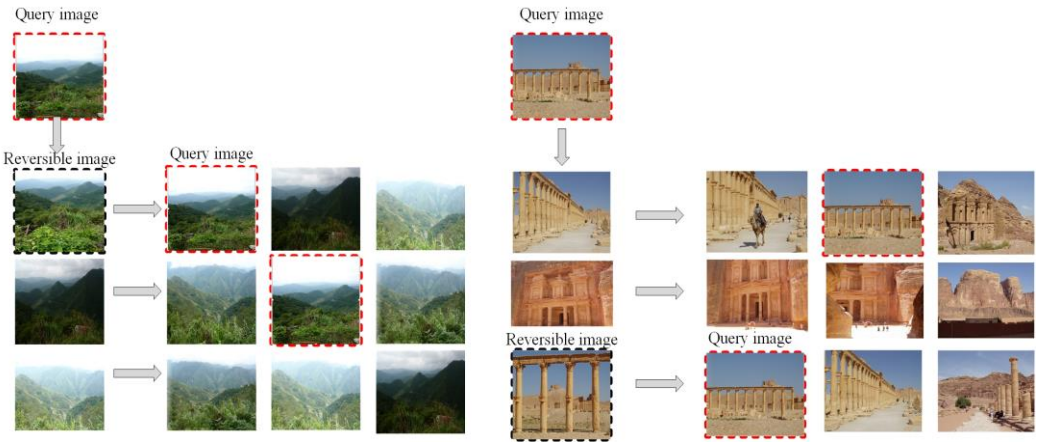


Fig. 4. Partial retrieval results in the Holidays

From the above observations, we not only confirm that images that satisfy reversibility seem to be similar in true meaning, but also observe that the reversible objects seem to be directly found in the nearest neighbors.

Observation 2. Some local feature of the image is likely to make images more similar to each other in image retrieval.

Observation 1 inspires us to find reversible images directly from the nearest neighbors. However, this non-reversible condition is also common and will vary across image datasets. Therefore, we must ensure that all images will find their reversible objects, so we propose a reversible sub-feature retrieval scheme to address this problem. Similarly, **Fig. 5** is built on the inspiration provided by observation 2. As can be seen from **Fig. 5**, analyzing the image examples from a visual perspective, we can see that the main reason for irreversibility between image A and G is that they share less similar parts (streams) than the ones of image G and F (trees). However, it also inspires us to use a local feature in the image for retrieval, so we intercept the sub-feature used for image retrieval in our design scheme.

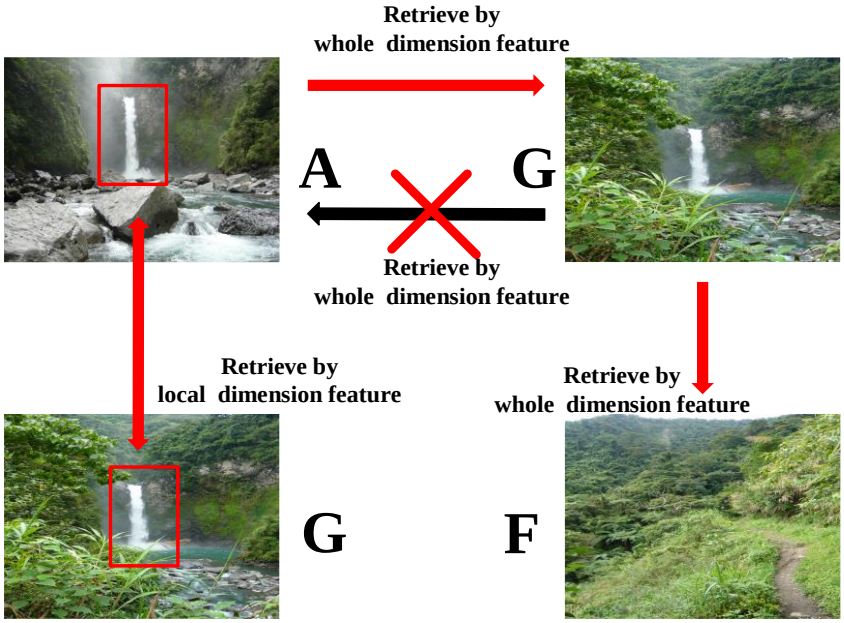


Fig. 5. The illustration of reversible sub-feature retrieval when nonreversibility in normal image retrieval

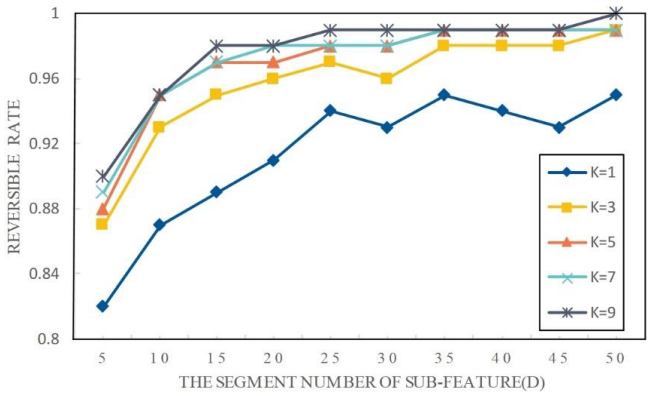


Fig. 6. The experimental results for observing the reversible rate by sub-features retrieval

To verify the feasibility of the scheme, we conducted an experiment on 1024 dimensions of DenseNet feature extracted form Holidays dataset. The above experimental results demonstrate that when the nearest neighbor *K* and the number of sub-features *D* are sufficient, we can accurately find the reversible object of each image.

3.2 Acquisition of Camouflage Image

Let us consider a feature vectors denoted as X . First, we split *Dn*-dimensional feature X into D distinct sub-feature $DF_i(1 \le i \le D)$, whose dimension D_i^* is calculated by (1). Then, for each sub-feature pair DF_i and $\overset{\frown}{DF_i}$, we compute the cosine distance between them, which are denoted as $C(DF_i, \overset{\frown}{DF_i})$.

$$D_i^* = \begin{cases} \left\lceil \frac{Dn}{D} \right\rceil, & if\ i < D \\ Dn - (i-1) \times \left\lceil \frac{Dn}{D} \right\rceil, & if\ i = D \end{cases} \tag{1}$$

Subsequently, denote a set of DenseNet feature as $DF = \left\{ DF^1, DF^2, \ldots, DF^{ic} \right\}$ where DF^{ic} represent the corresponding feature of image *ic* and D_i^{ic} represent the i_{th} segment of feature of ic_{th} image in image database. Therefore, if any image pair (*a*,*b*) satisfy the relationship of retrieval reversible, which is described as follows

$$\begin{aligned} C\left(DF_i^a, DF_i^b\right) \le \min \left\{ C\left(DF_i^a, DF_i^{ic}\right), C\left(DF_i^b, DF_i^{ic}\right) \right\} \\ where\ 1 \le ic \le Nums(I), 1 \le i \le D \} \end{aligned} \tag{2}$$

Where $Nums(\cdot)$ is an operation to obtain the numbers of image dataset *I*.

As our designed reversible retrieval scheme is based on the distances of one sub-features of each retrieve objects, we first decompose each feature into a set of sub-features $\left\{ DF_1, DF_2, \ldots, DF_i \right\}$. Then, given a query image *q*, its *K* nearest neighbor images can be represented as

$$NH_q^K = kargmin_{ic} C\left(q, DF^{ic}\right) \tag{3}$$

For the k_{th} nearest neighbor image $NH_q^k(1 \le k \le K)$ of NH_q^K , we need to verify that there is a reversible object. Due to only the Top 1 retrieval result is needed to determine whether it is invertible. Therefore, the Top 1 image set for NH_q^k denote as $NH_q^{k'}$. Finally, we use $R(\cdot)$ to verify the $NH_q^{K'}$ whether it is satisfying the relationship of retrieval reversible. It is

described as follows:

$$R(q)=\begin{cases}1, \ if \ \ q=NH_q^{k'} \\ 0, \quad otherwise\end{cases}, 1\le k\le K \tag{4}$$

Where $R(\cdot)$ is the verify function, if its return value is 1, which mean is the q has a versible object and NH_q^k is the needed camouflage image.

4. The Coverless Image Steganography Scheme

The flowchart of our proposed framework is illustrated in **Fig. 7**. It can be roughly divided into three modules: Construction of inverted index, secret Information hiding and extraction of Secret Information. For secret information *S* and a public image database *I*, our purpose is to obtain the camouflage image whose represented secret information is different from stego-image and image content is similar to it. For this purpose, we first obtain the stego-image by hash algorithm of existing CIS schemes. Then, we propose a reversible sub-feature retrieval scheme to acquire the corresponding camouflage image. In receiver, we need to restore the stego-image by selecting effective sub-feature and secret information with the same hash algorithm.

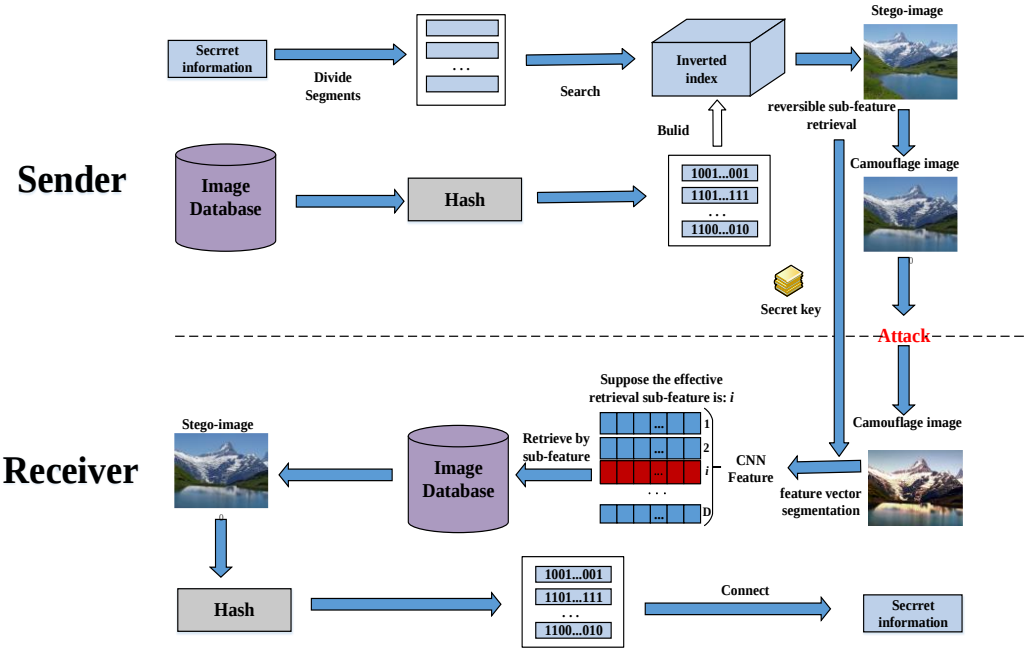


Fig. 7. The proposed framework of coverless image steganography

4.1 Construction of Inverted Index

Before acquiring camouflage images by stego-image, we need to extract hash sequences from the image database and divide binary secret information into the same segments as the hash sequences. Therefore, it is necessary to establish an effective inverted index to quickly obtain the stego-image according to secret information.

In our scheme, we adopt the hash algorithm proposed by Ref. [8] and the process of hash

is shown in **Fig. 8**. During the transmission of secret information, it is first divided into several information segments of length *N*. The hash sequence needs to search the image database for images that match the information segment, which consumes a lot of time. To improve search efficiency, the structure of the inverted index shown in **Fig. 9** is established.

As is shown in **Fig. 9**, each Hash group corresponds to four rows through *IndexID*. Considering that the order of the images received at the receiver may change, the first-row stores the pix of the average pixel value of the images that determines the order of the images, which is calculated as follows.

$$pix = \frac{\sum_{j=1}^{16} Ipix\left(b_j\right)}{16} \tag{5}$$

$Ipix\left(b_j\right)$ represents the average pixel value of the j_{th} block of the image, whose value can be calculated during the extraction of the hash sequence. The second-row stores the path of the image which is used to index the image quickly. Each Hash sequence is mapped from secret information and calculated by the hash algorithm of Ref. [8].

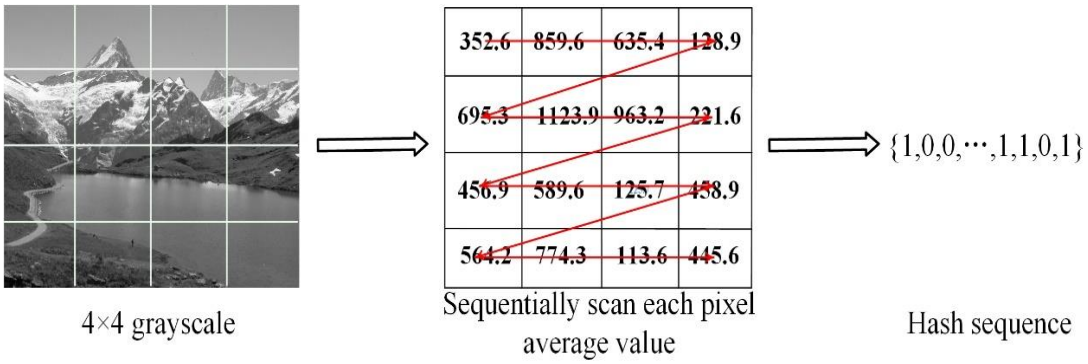


Fig. 8. The process of hash algorithm in [8]

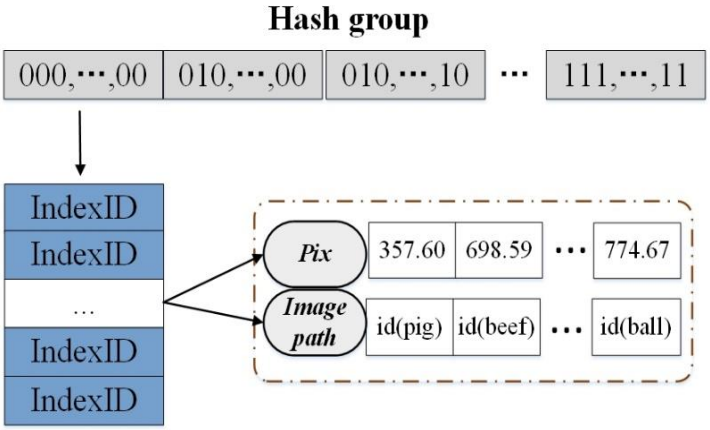


Fig. 9. The illustration of the constructed inverted index structure

4.2 Secret Information Hiding

Secret information hiding is a process of secret information selecting camouflage image. It consists of two steps: obtaining stego-image based on secret information by exciting CIS hash algorithm and retrieving camouflage image based on stego-image. The process is as follows.

1. First, the secret information *S* of length *p* is divided into *m* segments.

$$m = \begin{cases} \frac{p}{N}, if \ \ p\%N = 0 \\ \frac{p}{N} + 1, otherwise \end{cases} \tag{6}$$

Where *N* is the length of the secret information segment. If *p* cannot be divisible, 0 is added to the last portion to obtain a sequence of length *N*, and the number of 0 is recorded.

2. In the Section 4.1, we can compute the hash sequence of each image in the image database, and establish an inverted index to match the stego-image. For the given secret message segment ms_{cg}, the stego-image ps_{cg} matched by

$$\begin{gathered} PS_{cg} = I_{ic}, if \ \ f_{ic} = ms_{cg} \text{ and } pix_{ic} > pix_{ic-1} \\ where \ 1 \le cg \le m, 1 \le ic \le Nums(I) \end{gathered} \tag{7}$$

Where f_{ic} represents the hash sequence of the selected image, it is noting that the size of I_{ic} will be normalized, if size $< 512 \times 512$, *M*=128; If size $\ge 512 \times 512$, *M*=512.

3. Repeat step 2 until the stego-images corresponding to all secret information are retrieved and the recorded 0 amount of data is mapped to the last image.
4. For all stego-images *PS*, we need to find the corresponding camouflage images *PC* whose solutions have been described in Section 3.2. Therefore, we use $SR^{+}(\cdot)$ function to represent the process of forward retrieval which is described as follows

$$\begin{gathered} (PC_{cg}, d_{cg}) = SR^{+}\left(PS_{cg}, I, D\right) \\ where \ 1 \le cg \le m, 1 \le d_{cg} \le D \end{gathered} \tag{8}$$

Where d_{cg} represents the effective sub-feature segment corresponding to PC_{cg}, which can be used for reverse retrieval, and it is necessary to record d_{cg} when determining the camouflage image. When $D = d_{cg} = 1$ indicates the whole dimension of the feature to be used, $d_{cg} > 1$ indicates d_{cg}-*th* segment feature used in the retrieval task.

5. D is taken as the shared key of both receivers and receivers, and d_{cg} is recorded as auxiliary information, which is encrypted with AES encryption algorithm. After that, all camouflage images are sent to the receiver. The pseudocode of secret information hiding is shown in algorithm 1. Finally, it is worth noting that the number of images in image database should not be too small, otherwise the secret information cannot be fully expressed. In addition, we don't select databases with small associations of image content, otherwise the algorithm will not match enough camouflage images.

6.

Algorithm 1：Secret information hiding

Input：**Image database**：$I=\{I_1,I_2,\ldots,I_{ic}\}$; **Secret information:** S

Output：**Camouflage Images**：$PC=\{PC_1,PC_2,\ldots,PC_{cg}\}$; the segment number of sub-feature $d=\{d_1,d_2,\ldots,d_{cg}\}$

1: **Link MySql Database**
2: for *ic* = 1: *Nums*(*I*)
3: Resize I_{ic}
4: (a) Get the hash sequences f_{ic} by hash algorithm of Ref. [8]
5: (b) Use the (5) computer average pixel value : *pix* =*Mean*(I_{ic})
6: Update index database: **Index item**-> (f_{ic}, *pix*, I_{ic})
7: end
8: Cut secret information *S*: *ms* = *Cut*(*S*)
9: for *cg* = 1:*m*
10: Selecting stego-image for *ms*: $PS_{cg}=I_{ic}, if\ f_{ic}=ms_{cg}$ and $pix_{ic}>pix_{ic-1}$
11: Retrieving camouflage image for stego-image: $\left(PC_{cg},d_{cg}\right)=SR^{+}\left(PS_{cg},I,D\right)$
12: end
13: **Return** the selected camouflage image:*PC* and the segment number of sub-feature: *d*

4.3 Extraction of Secret Information

The extraction of secret information refers to the process in which the receiver restores secret information to the received image. It consists of two steps: recovering stego-image based on camouflage image and recovering secret information based on hash algorithm. The process is as follows.

1. At the receiver, we can know the length of feature segmentation by sharing the key *D*. Then, we extract the effective sub-feature segment d_{cg} corresponding to the camouflage image *PC* from the auxiliary information. For the given camouflage image PC_{cg} and public database I, the stego-image PS_{cg} is calculated as follows.

$$PS_{cg}=SR^{-}\left(PC_{cg},I,d_{cg}\right) \tag{9}$$

Where $SR^{-}(\cdot)$ represent the process of forward retrieval.

2. Then, the average pixel value pix of stego-image are calculated to restore the order of images, and the corresponding hash sequence *f* is calculated by hash algorithm of Ref. [8].
3. Repeat the above steps to calculate the sequence of features corresponding to each stego-image. Based on the number of 0 recorded in the last image, subtract the corresponding 0 from the information in the last paragraph to get the secret information. The pseudocode of the secret information extraction algorithm is shown in Algorithm 2.

Algorithm 2： Extraction of secret information

Input：**Image database**： $I=\{I_1,I_2,\ldots,I_{ic}\}$; **Camouflage Images**：

$PC=\{PC_1,PC_2,\ldots,PC_{cg}\}$; **Secret key:** the segment number of sub-feature ***d***

Output：**Secret information:** S'

1: for cg = 1: *Nums*(*PC*)

2: $PC_{cg}=SR^{-}(PS_{cg},I,d_{cg})$

3: end

4: Get the images by the *pix: PS* = Sort(*PS*)

5: for cg = 1: *Nums*(*PC*)

6: Resize PS_{cg}

7: Get the hash sequences ms_{cg} by hash algorithm of Ref. [8]

8: Connect the *ms*: $S'+=ms_{cg}$

9: end

10: **Return** S'

5. Experimental Classification Results and Analysis

In this section, we test and report the evaluation results of our approach and compare it with some of the state-of-the-art methods in four benchmark datasets. Then, the impacts of the parameters in our approach are studied to explore the influence of parameters in the scheme. Finally, the security of our CIS approach is analyzed in the aspects of carrier transmission and steganography.

5.1 Datasets

In our experiment, the performances of our CIS approach are evaluated on four widely used benchmark datasets, i.e., INRIA Holidays [34], Flickr, Caltech-101 [35], and Caltech-256 [36], which are described as follows:

The Holidays dataset created by Herve Jegou et al contains 1,491 images. This dataset has no fixed category and high image resolution. In this paper, 500 images are randomly choosing for comparative experiments.

The Flickr dataset is a large image dataset consisting of 1024 high-quality image pairs covering a wide variety of scenes, 500 images are randomly chosen for comparative experiments.

The Caltech-101 dataset, created by Caltech, contains 9145 images of 102 object categories. Similar to the ImageNet dataset, its images have a low resolution. In this paper, 500 images are randomly choosing for comparative experiments.

The Caltech-256 dataset contains 29780 images from 257 object categories and each containing more than 80 images. It can be regarded as an extension of the Caltech-101 dataset. 500 images are randomly chosen for comparative experiments.

5.2 Experimental Setting

In this experiment, Intel (R) Core (TM) i7-7800xcpu @ 3.50ghz, 64.00gb ram and two NVIDIA GeForce GTX 1080 Ti GPUs are used. Deep learning adopts the Keras framework. Keras is a high-level neural network API, and we can use TensorFlow more conveniently with Keras. All experiments are completed in MATLAB 2016a and Pycharm.

To verify the effectiveness of the proposed method, we compared it with the state-of-the-art methods, which are respectively denoted as PIX-CIS [8], HASH-CIS [11], BOF-CIS [12], DCT-CIS [13] and DWT-CIS [14]. Due to the difference in experimental steganographic image selection, we reproduced their experiments without using their original data. It is worth noting that, since BOF-CIS does not specify the specific hash function, it doesn't compare with it in the robustness experiment.

In the comparison experiment, there are a number of important parameters: the length of Hash sequence N is 8. In our work, K=1 and D=1 is set in robustness comparison experiment. In our experiment, the pre-training model uses ImageNet database for training and the selected model is DenseNet121. For traditional CIS methods, the image size M is set to 512 in the Holidays and Flickr dataset and M is set to 128 in the Caltech-101 and Caltech-256 datasets. The robustness is adopted for evaluating the performance of resistance to attack. In the experiment, we randomly selected 100 sequences and calculated the recovery rate of the secret information, namely the robustness, without considering the order. Extraction accuracy is defined as

$$RC = \frac{\sum_{cg=1}^{m} f(ms_{cg}')}{m}, \quad f(ms_{cg}') = \begin{cases} 1, & if\ ms_{cg}' = ms_{cg} \\ 0, & otherwise \end{cases} \tag{10}$$

Where m is the number of information segments, ms_{cg} is the cg_{th} hidden secret information of stego-images, ms_{cg}' is the cg_{th} secret information of stego-images extracted from the receiver.

5.3 Analysis of Capacity

In this Section. Five CIS methods [8, 11-14] are chosen to compared the embedding capacity with RSR-CIS. The capacity of existing CIS based on mapping rules is determined by the length N of the hash sequence. The larger the N, the larger the capacity. Like DCT-CIS, our method takes the variable sequence length, and the definition of N_h is:

$$N_h = \frac{p}{N} \tag{11}$$

Where p is the length of the secret information.

Table 1. Steganographic capacity

Algorithm	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
RSR-CIS	2 ~ 9	7 ~ 81	55 ~ 801	548 ~ 8193	1 ~ 15

Since RSR-CIS is different from the traditional CIS method, theoretically, we can take any mapping rules similar to [13-16] to generate hash sequences, so as to control steganographic capacity effectively. An increase in capacity is usually accompanied by an increase in the number of images. For a hash sequence of length N, we need at least 2^N images to express the complete secret information. In fact, when we don't have enough images to express a certain sequence, we can only use the repeated carrier, which may cause the attacker's suspicion and further destroy the private information. Therefore, we usually increase the scope of the image database or change the length of the secret message expression. However, the advantage of RSR-CIS is that the mapping rules do not need to consider robustness so that it can take the simple mapping rules with low calculation cost. In this paper, we use a pixel-based mapping approach similar to PIX-CIS.

5.4 Analysis of Robustness

5.4.1 Comparison of Different Approaches on Robustness

To evaluate the robustness of the proposed approach for CIS steganography and make a fair comparison with Four CIS methods [8, 11, 13, 14], we selected the widely image attacks in four public datasets. The specific parameters are shown in **Table 2**.

Table 2. Kind of image attacks

Attack	The specific parameters
JPEG compression	The quality factors Q: 10%.
Salt and speckle noise	The mean μ: 0, the variances σ:0.001.
Gauss low-pass filtering	The window sizes: 3×3.
Centered cropping	Ratios: 20%.
Edge cropping	Ratios: 20%.
Rotation	Rotation angles: 10°.
Translation	the translation distances: (80、50).
Scaling	The scaling ratios : 3.
Gamma correction	Factor: 0.8.

Fig. 10 shows the 9 kinds of attacked images and the original images coming from the Caltech-101 dataset. The comparison results with the four CIS methods are shown in **Table 3**, **4**, **5** and **6**. It shows that RSR-CIS generally outperform other methods in geometric attacks. In Holidays and Flickr dataset, RSR-CIS achieved excellent performance in some non-geometric attacks while it maintains well robustness in geometric attacks. However, in Caltech-101 and Caltech-256 dataset, the results show that its robustness is worse than the former while also outperform other methods in geometric attacks. Due to Holidays and Flickr are high image resolution datasets and Caltech-101 and Caltech-256 are low image resolution

datasets. Therefore, we learn that robustness performance of RSR-CIS has great potential by using high resolution camouflage image as transmission carrier. In addition, from the perspective of CNN feature extraction, this is attributed to the fact that the higher the image quality, the richer the semantic information represented by CNN, and thus the stronger its resistance to aggression.

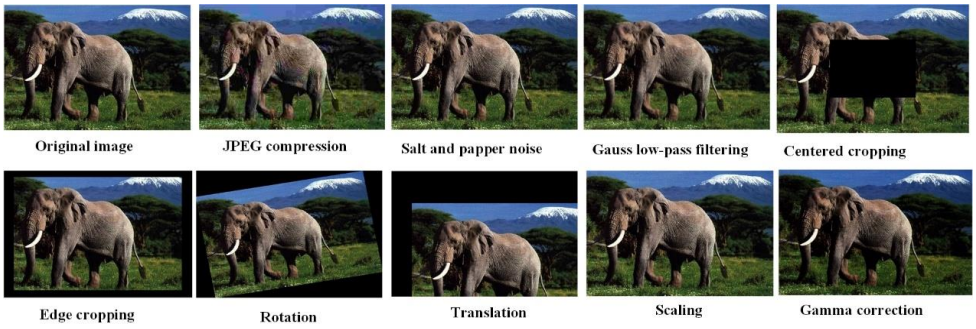


Fig. 10. The sample display of 9 widely attacked images

Table 3. Robustness (%) comparison with four CIS methods in Holidays

Attack	Parameter	HASH-CIS	PIX-CIS	DCT-CIS	DWT-CIS	RSR-CIS
Compression	Q(10)	74.64	**97.69**	94.81	97.41	89.91
Salt and Speckle Noise	σ(0.001)	96.93	99.42	**100**	99.71	94.81
Gauss Filtering	3×3	95.97	**100**	**100**	**100**	96.83
Centered Cropping	20%	6.63	14.96	14.98	12.39	**50.14**
Edge Cropping	20%	4.32	20.46	18.73	19.60	**86.46**
Rotation	10°	2.60	4.61	4.61	6.63	**59.37**
Translation	(80,50)	5.19	33.14	33.43	30.55	**87.03**
Scaling	3	96.93	**100**	**100**	**100**	96.83
Gramma	0.8	65.42	92.51	93.66	93.37	**96.54**

Table 4. Robustness (%) comparison with four CIS methods in Flickr

Attack	Parameter	HASH-CIS	PIX-CIS	DCT-CIS	DWT-CIS	RSR-CIS
Compression	Q(10)	65.80	95.00	94.40	93.80	**96.00**
Salt and Speckle Noise	σ(0.001)	93.20	**100**	99.80	99.60	99.80
Gauss Filtering	3×3	97.80	**100**	**100**	**100**	99.80
Centered Cropping	20%	9.20	28.20	28.60	19.60	**82.80**
Edge Cropping	20%	5.60	21.20	19.80	20.80	**96.80**
Rotation	10°	1.80	5.60	5.60	3.60	**55.80**
Translation	(80,50)	2.40	12.60	12.60	13.20	**83.40**
Scaling	3	97.80	**100**	**100**	**100**	99.80
Gramma	0.8	54.40	90.40	90.00	89.40	**99.80**

Table 5. Robustness (%) comparison with four CIS methods in Caltech-101

Attack	Parameter	HASH-CIS	PIX-CIS	DCT-CIS	DWT-CIS	RSR-CIS
Compression	Q(10)	52.99	**94.02**	93.16	92.74	69.66
Salt and Speckle Noise	σ(0.001)	90.60	94.01	**96.15**	95.73	78.63
Gauss Filtering	3×3	89.31	**100**	99.57	**100**	80.34

Centered Cropping	20%	9.40	35.47	36.32	23.93	**41.88**
Edge Cropping	20%	8.54	23.93	23.08	26.07	**73.93**
Rotation	10°	4.70	7.69	7.69	09.40	**63.25**
Translation	(80,50)	0.42	0	0	1.28	**55.98**
Scaling	3	91.45	100	100	100	82.05
Gramma	0.8	60.68	90.17	**90.59**	87.18	82.05

Table 6. Robustness (%) comparison with four CIS methods in Caltech-256

Attack	Parameter	HASH-CIS	PIX-CIS	DCT-CIS	DWT-CIS	RSR-CIS
Compression	Q(10)	55.00	93.75	94.58	**95.83**	78.33
Salt and Speckle Noise	σ(0.001)	87.50	95.00	94.58	**96.67**	79.59
Gauss Filtering	3×3	92.92	**100**	**100**	**100**	84.58
Centered Cropping	20%	13.75	**43.33**	42.08	29.58	40.83
Edge Cropping	20%	8.33	20.00	21.25	19.58	**78.33**
Rotation	10°	4.17	6.25	7.50	8.75	**65.83**
Translation	(80,50)	3.33	2.08	1.67	2.08	**64.17**
Scaling	3	96.25	**99.58**	**99.58**	**99.58**	85.42
Gramma	0.8	66.25	**92.50**	90.83	90.83	85.83

5.4.2 Analysis of Different Factors on Robustness

Parameter Analysis. In this subsection, we empirically analyze the sensitivity of D on robustness. In the experiment, we set K=5 and D is varied from the range of {1,2,3,4,5}. To objectively analyze the influence of parameters on the experimental results, subsequent experiments are based on the same dataset Holidays.

Table 7. Robustness(%) with respect to the different segment number of sub-feature in Holidays

Attack	Parameter	D=1	D=2	D=3	D=4	D=5
Compression	Q(10)	**87.67**	65.59	71.67	73.80	63.82
Salt and Speckle Noise	σ(0.001)	**92.76**	90.20	86.67	78.70	83.15
Gauss Filtering	3×3	94.64	**96.08**	95.00	94.31	94.83
Centered Cropping	20%	**48.53**	38.73	39.05	29.84	28.76
Edge Cropping	20%	**83.91**	22.79	25.71	19.36	18.20
Rotation	10°	**57.37**	15.93	19.52	14.81	12.36
Translation	(80,50)	**84.99**	54.41	54.52	39.18	38.65
Scaling	3	94.64	**96.32**	95.00	95.22	94.61
Gramma	0.8	**93.83**	91.67	90.90	90.43	88.54

The specific parameters and experiment results are shown in **Table 7**. From **Table 7**, we see that with the increase of D, robustness has an obvious downward trend especially in some geometric attacks and some non-geometric attacks such as compression, salt and speckle noise and so on. Theoretically, the larger D is, the lower the dimension of sub-feature and the corresponding robustness will be worse. However, we learn that robustness was not significantly affected in some less aggressive noise such Gauss filtering. Even robustness is still improved when D is set to 2. In sum, the experiment shows that the robustness of RSR-

CIS also be remained stable when images face lighter image attacks.

Table 8. Robustness(%) with respect to the different CNN model in Holidays

Attack	Parameter	InceptionResNetV2	ResNet50	InceptionV3	DenseNet121
Compression	Q(10)	81.35	**91.22**	82.33	89.91
Salt and Speckle Noise	σ(0.001)	90.35	**94.90**	91.48	94.81
Gauss Filtering	3×3	90.68	96.03	92.11	**96.83**
Centered Cropping	20%	29.26	**52.12**	19.56	50.14
Edge Cropping	20%	72.99	74.79	77.92	**86.46**
Rotation	10°	39.58	47.31	44.79	**59.37**
Translation	(80,50)	76.21	83.57	78.86	**87.03**
Scaling	3	91.00	96.03	92.43	**96.83**
Gramma	0.8	91.32	92.92	91.48	**96.54**

CNN model analysis. To explore the influence of different CNN models on robustness, four CNN models, i.e., InceptionResNetV2, ResNet50, InceptionV3, and DenseNet121 are adopted for evaluation, D=1 and Holidays selected for this experiment and reporting the performance results with varying CNN models, which all used ImageNet for pre-training. From **Table 8**, we can see that DenseNet121 obtains the optimal robustness performance, and ResNet50 obtains the suboptimal result. InceptionResNetV2 and InceptionV3 showed comparable performance, but slightly worse performance than the former. Therefore, we finally chose DenseNet121 as our benchmark model. At the same time, experimental results demonstrate that a good classified CNN model can improve the CIS's robustness.

5.5 Analysis of Time Consumption

Steganographic time will affect the security of the secret information under the transmission process of carrier, so it is also an important indicator in CIS. In this section, we compared steganographic time of RSR-CIS with other schemes and explored the impact of the number of nearest neighbor K which varied from the range of {1,2,3,4,5} and the number of sub-features D which varied from the range of {5,10,15,20,25,30,35,40} on time consumption. In the traditional CIS scheme, we calculate the time of the sequence mapping. And in our RSR-CIS, the steganographic time composed of the time of matching and feature extraction stego-image and the time of retrieving camouflage image, it is noting that the experiment parameter is consistent with the experimental setting.

Table 9 gives the average steganographic time of different approaches. From this table, we can observe that PIX-CIS requires the lowest average steganographic time due to the low computational complexity of hashing based on pixel; Because RSR-CIS adopt the hash algorithm proposed by PIX-CIS and use high performance GPU to extract features for retrieval, its steganographic time second to PIX-CIS; The time consumption of DWT-CIS is comparable to that of DCT-CIS; HASH-CIS needs much more steganographic time than the other approaches as it extracts SIFT feature points to generate feature vectors.

Table 9. The average steganographic time (second) of different approaches

	HASH-CIS	PIX-CIS	DCT-CIS	DWT-CIS	RSR-CIS
Average steganographic time	1.04	0.14	0.64	0.51	0.18

Fig. 11 show the average steganographic time (second) of different *K* and *D* in RSR-CIS. It is clear that the proposed RSR-CIS method still has a lower time consumption. With the increase of *K*, we have more nearest neighbor images to sift through, and obviously, our steganographic time goes up linearly. And with the increase of *D*, we can learn from **Fig. 11** is that the overall time consumption is going up. However, it is finding that the curve with respect to *D* has two inflection points which shows a reduction in length of sub-feature does not necessarily mean a decrease in retrieving speed, this conclusion also can be obtained by results of **Table 7**. In summary, compared with the traditional CIS schemes, RSR-CIS still needn't too much steganography time.

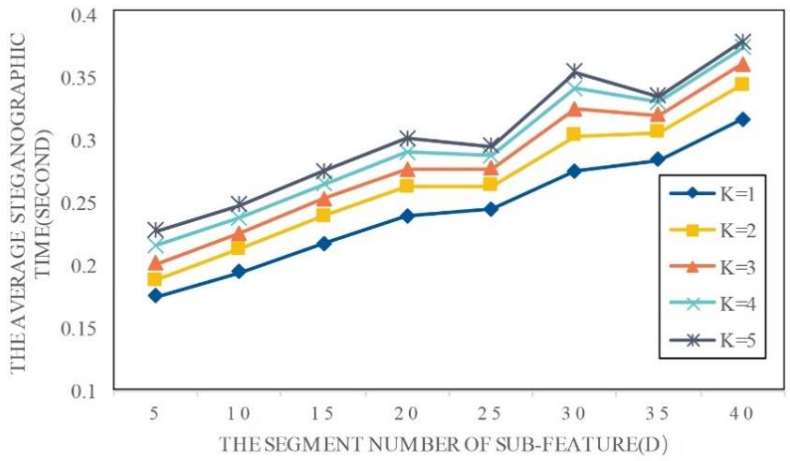


Fig. 11. The average steganographic time (second) of different *K* and *D* in Holidays

5.6 Analysis of Safety

In the field of CIS, capacity, robustness and security are usually restricted to each other. In this paper, the CR-CIS is mainly aimed at the last two points. In RSR-CIS, we introduce AES encryption algorithm to ensure the security of the scheme to prevent the leakage of auxiliary information. Overall, we provide security protection in the following aspects.

1. The advantage of CIS is that it does not modify the image at all, but instead transmits a natural set of unmodified images. Therefore, our method can resist the detection of existing steganographic analysis tools effectively.
2. Instead of sending stego-image that has a direct mapping relationship with secret information, we send a camouflage image that looks like stego-image to receiver, which is the biggest difference between RSR-CIS and the traditional CIS methods. Therefore, our method still guarantees the security of the secret information effectively even if the attacker has captured the stego-image and mastered the mapping rules.

6. Conclusion

In this paper, we have proposed a reversible sub-feature retrieval scheme for coverless image

steganography. Instead of directly sending stego-image, we transmit the camouflage image which is obtained based on the phenomenon that the contents of the images are similar but the mapping sequence is inconsistent. In this scheme, we first obtain the all hash sequences by using any of the existing CIS schemes. According to the inverted index structure created by hash sequences, all stego-images can be obtained by secret information. Finally, we can use the stego-image as a query to retrieve the camouflage image by proposed scheme. The proposed model transforms the dependency based on mapping rules into a reversible retrieval between camouflage images and stego-images, which effectively solves the deficiency of existing CIS schemes against geometric attack resistance. Also, owing to the efficient performance of CNN features on image retrieval, our approach has great potential in terms of robustness in geometric attacks.

In the future, we will focus on designing a better sub-feature retrieval scheme such as optimizing feature segmentation or using local features to further reduce the time cost while maintaining high robustness which is not limited to geometric attacks.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61772561 and 62002392, in part by the Natural Science Foundation of Hunan Province under Grant 2020JJ4141 and 2020JJ4140, in part by the Science Research Projects of Hunan Provincial Education Department under Grant 18A174,19B584 and 18C0262, in part by the Key Research and Development Plan of Hunan Province under Grant 2019SK2022, in part by the Degree & Postgraduate Education Reform Project of Hunan Province under Grant 2019JGYB154, 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.

References

[1] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan and N. N. Xiong, "A robust watermarking scheme in YCbCr color space based on channel coding," *IEEE Access*, vol. 7, pp. 25026-25036, 2019. Article (CrossRef Link)

[2] C. Yang, C. Weng, S. Wang, and H. Sun, "Adaptive data hiding in edge areas of images with spatial lsb domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488-497, 2008. Article (CrossRef Link)

[3] W. Luo, F, Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, 2010. Article (CrossRef Link)

[4] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 67-70, 2005. Article (CrossRef Link)

[5] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. of IEEE International Workshop on Information Forensics and Security*, pp. 234-239, 2012. Article (CrossRef Link)

[6] T. Pevny, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," *Lecture Notes in Computer Science*, vol. 6837, pp.161-177, 2010. Article (CrossRef Link)

[7] J. Qin, X. Sun, X. Xiang, and C. Niu, "Principal feature selection and fusion method for Image steganalysis," *Journal of Electronic Imaging*, vol. 18, no. 3, pp. 1-14, 2009. Article (CrossRef Link)

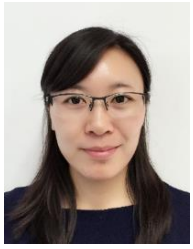
[8] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Proc. of International Conference on Cloud Computing and Security*, pp. 123-132, 2015. Article (CrossRef Link)
[9] Z. Zhou, J. Qin, X. Xiang, Y. Tan, Q. Liu, and N. N. Xiong, "News text topic clustering optimized method based on TF-IDF algorithm on spark," *Computer Materials & Continua*, vol. 62, no. 1, pp. 217-231, 2020. Article (CrossRef Link)
[10] N. Pan, J. Qin, Y. Tan, X. Xiang, and G. Hou, "A video coverless information hiding algorithm based on semantic segmentation," *EURASIP Journal on Image and Video Processing*, vol. 23, 2020. Article (CrossRef Link)
[11] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *Proc. of International Conference on Intelligent Computing*, pp. 536-547, 2017. Article (CrossRef Link)
[12] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *Journal of International and Technology*, vol. 18, no. 2, pp. 435-442, 2017. Article (CrossRef Link)
[13] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 99, no. 12, pp. 3223-3238, 2018. Article (CrossRef Link)
[14] Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, and Y. Luo, "Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping," *Knowledge-Based Systems*, vol. 192, pp. 105375-105389, 2020. Article (CrossRef Link)
[15] Z. Zhou, Y. Mu, and Q. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Computing*, vol. 23, pp. 4972-4938, 2018. Article (CrossRef Link)
[16] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L Xiang, "Coverless real-time image information hiding based on image block matching and dense convolutional network," *Journal of Real-Time Image Processing*, vol. 17, no. 1, pp. 125-135, 2020. Article (CrossRef Link)
[17] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, 2020. Article (CrossRef Link)
[18] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372-171394, 2019. Article (CrossRef Link)
[19] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proc. of the 7th IEEE International Conference on Computer Vision*, vol. 2, pp. 1150-1157, 1999. Article (CrossRef Link)
[20] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. of International Conference on Neural Information Processing Systems*, vol. 60, no. 6, pp. 1097-1105, 2012. Article (CrossRef Link)
[21] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *Computer Science*, 2014. Article (CrossRef Link)
[22] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1-9, 2015. Article (CrossRef Link)
[23] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770-778, 2016. Article (CrossRef Link)
[24] G. Huang, Z. Liu, L. Maaten, and K. Weinberger, "Densely connected convolutional networks," in *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2261-2269, 2017. Article (CrossRef Link)
[25] L. Xiang, G. Guo, J. Yu, V. S. Sheng, and P. Yang, "A convolutional neural network-based linguistic steganalysis for synonym substitution steganography," *Mathematical Biosciences and Engineering*, vol. 17, no. 2, pp. 1041-1058, 2020. Article (CrossRef Link)
[26] W. Ma, J. Qin, X. Xiang, Y. Tan, Y. Luo, and N. N. Xiong, "Adaptive median filtering algorithm based on divide and conquer and its application in captcha recognition," *Computer Materials & Continua*, vol. 58, no. 3, pp. 665-677, 2019. Article (CrossRef Link)

[27] J. Wang, J. Qin, X. Xiang, Y. Tan, N. Pan, "Captcha recognition based on deep convolutional neural network," *Mathematical Biosciences and Engineering*, vol. 16, no, 5, pp. 5851-5861, 2019. Article (CrossRef Link)
[28] L. Pan, J. Qin, H. Chen, X. Xiang, C. Li, and R. Chen, "Image augmentation-based food recognition with convolutional neural networks," *Computer Materials & Continua*, vol. 59, no. 1, pp. 297-313, 2019. Article (CrossRef Link)
[29] W. Pan, J. Qin, X. Xiang, Y. Wu, Y. Tan, and L. Xiang, "A smart mobile diagnosis system for citrus diseases based on densely connected convolutional networks," *IEEE Access*, vol. 7, pp. 87534-87542, 2019. Article (CrossRef Link)
[30] H. Li, J. Qin, X. Xiang, L. Pan, W. Ma, and N. N. Xiong, "An efficient image matching algorithm based on adaptive threshold and ransac," *IEEE Access*, vol. 6, pp. 66963-66971, 2018. Article (CrossRef Link)
[31] J. Qin, H. Li, X. Xiang, Y. Tan, W. Pan, W. Ma, and N. N. Xiong, "An encrypted image retrieval method based on harris corner optimization and lsh in cloud computing," *IEEE Access*, vol. 7, pp. 24626-24633, 2019. Article (CrossRef Link)
[32] L. Xiang, X. Shen, J. Qin, and W. Hao, "Discrete multi-graph hashing for large-scale visual search," *Neural Processing Letters*, vol. 49, no. 3, pp.1055-1069, 2019. Article (CrossRef Link)
[33] H. Jegou, H. Hedi, and S. Cordelia, "A contextual dissimilarity measure for accurate and efficient image search," in *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1-7, 2007. Article (CrossRef Link)
[34] H. Jegou, M. Douze, and C. Schmid, "Hamming embedding and weak geometric consistency for large scale image search," in *Proc. of European Conference on Computer Vision*, pp. 304-317, 2008. Article (CrossRef Link)
[35] F. Li, R. Fergus, and P. Perona, "Learning generative visual models from few training examples: an incremental Bayesian approach tested on 101 object categories," in *Proc. of 2004 Conference on Computer Vision and Pattern Recognition Workshop*, 2004. Article (CrossRef Link)
[36] G. Griffin, A. Holub, and P. Perona, "Caltech-256 object category dataset," *CalTech Report*, 2007. Article (CrossRef Link)

Qiang Liu received his BS in network engineering from Hunan University of Technology, China, in 2017. He is currently pursuing his MS in information and communication engineering at College of Computer Scienceand Information Technology, Central South University of Forestry and Technology, China. His research interests include deep learning and image steganalysis.

Xuyu Xiang received his B.S. in mathematics from Hunan Normal University, China, in 1996, M.S. degree in computer science and technology from National University of Defense Technology, China, in 2003, and PhD in computing science from Hunan University, China, in 2010. He is a professor with the College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include network and information security, image processing and machine learning.

Jiaohua Qin received the B.S. degree in mathematics from the Hunan University of Science and Technology, China, in 1996, the M.S. degree in computer science and technology from the National University of Defense Technology, China, in 2001, and the Ph.D. degree in computing science from Hunan University, China, in 2009. She was a Visiting Professor with the University of Alabama, Tuscaloosa, AL, USA, from 2016 to 2017. She is currently a Professor with the College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. Her research interests include network and information security, machine learning and image processing.



Yun Tan received the M.S. and Ph.D. degrees both from Beijing University of Posts and Telecommunications, China, in 2004 and 2016, respectively. Now she is a lecturer with College of Computer Science and Information Technology, Central South University of Forestry and Technology,China. Her research interests mainly include image security, compressive sensing and signal processing.

Qin Zhang received her BS in Electrical engineering and its automation from Nanjing Institute of Technology, China, in 2019. She is going to pursue her MS in software engineering at College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. Her research interests include pattern recognition and image processing.