Computers, Materials & Continua CMC, vol.64, no.2, pp.1281-1295, 2020

Coverless Image Steganography Based on Image Segmentation

Yuanjing Luo[1], Jiaohua Qin[1,*], Xuyu Xiang[1], Yun Tan[1], Zhibin He[1] and Neal N. Xiong[2]

Abstract: To resist the risk of the stego-image being maliciously altered during transmission, we propose a coverless image steganography method based on image segmentation. Most existing coverless steganography methods are based on whole feature mapping, which has poor robustness when facing geometric attacks, because the contents in the image are easy to lost. To solve this problem, we use ResNet to extract semantic features, and segment the object areas from the image through Mask RCNN for information hiding. These selected object areas have ethical structural integrity and are not located in the visual center of the image, reducing the information loss of malicious attacks. Then, these object areas will be binarized to generate hash sequences for information mapping. In transmission, only a set of stego-images unrelated to the secret information are transmitted, so it can fundamentally resist steganalysis. At the same time, since both Mask RCNN and ResNet have excellent robustness, pre-training the model through supervised learning can achieve good performance. The robust hash algorithm can also resist attacks during transmission. Although image segmentation will reduce the capacity, multiple object areas can be extracted from an image to ensure the capacity to a certain extent. Experimental results show that compared with other coverless image steganography methods, our method is more robust when facing geometric attacks.

Keywords: Coverless steganography, semantic feature, image segmentation, Mask RCNN, ResNet.

1 Introduction

Due to the wide application of multimedia data, the communication of secret information needs digitization urgently. Steganography transmits secret information in a hidden way. Typically, it hides the secret information in the appropriate image, audio, or video, making secret information difficult to be detected. Coverless steganography has developed rapidly since it was formally proposed in May 2014 [Zhou, Cao and Sun (2016)], and it has been widely applied in the field of computer vision with its absolute anti-steganalysis. The existing coverless steganography methods can meet the needs of secret information transmission, their capacity and robustness have been greatly

[1] College of Computer Science and Information Technology, Central South University of Forestry & Technology, Changsha, 410114, China.

[2] Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, 74464, USA.

[*] Corresponding Author: Jiaohua Qin. Email: qinjiaohua@163.com.

Received: 02 April 2020; Accepted: 17 April 2020.

improved. However, stego-images are still facing the risk of malicious modification in the transmission. Meanwhile, the existing coverless steganography has poor robustness in the face of geometric attacks. To solve this problem, we consider using areas of the image to hide information, which can resist malicious modification and geometric attacks. Images are generally divided into object areas and background areas. The object area, with its luxurious texture, is an appropriate place to hide important information without being discovered. Nevertheless, the area is too visible to be robust of the attack, and the background area is too simple to hide secret information. In order to solve the above problems, we focus on the object areas which have good structural integrity from the multiple object areas in an image.

Mask RCNN, as a fully differentiable network architecture for instance and panoptic segmentation that can generate pixel-accurate object masks to accurately segments objects of complex shape. Therefore, it is very popular in the field of object detection. ResNet is selected as the backbone network of Mask RCNN to extract features, generate the corresponding mask, segment the image. The selected object area is less visible than the visual center of the image, so the risk of being attacked is greatly reduced. In the field of object detection, subtle attacks will make the extracted area different. In order to ensure the robustness, we use semantic features and select the object areas with good structural integrity. It is worth noting that the semantic features of the visual center may easily expose secret information, so the less visible object areas are selected, whose semantic features can ensure security. In our scheme, the robust hash algorithm is more suitable to process the extracted object areas, which can generate corresponding sequences. An inverted index structure is constructed to optimize retrieval. Only the corresponding stego-images with a key can be transmitted to present secret information. The receiver can use Mask RCNN model to segment images and select the object areas according to the semantic feature points, then use the same hash algorithm to obtain the secret information. The contributions of this paper are as follows:

(1) Instead of using the whole image, we extract the need object areas based on bounding box by Mask RCNN to represent information. These areas have chances to avoid geometric attacks on the image, which improved the robustness. Meanwhile, the used CNN model is robust and improves the security of information transmission.

(2) In object detection, subtle attacks can cause changes in the detection bounding box. The semantic features selected by ResNet are robust when the object areas change, thus ensuring the robustness of feature points and accuracy of object area extraction, which makes our method more secure.

(3) An image may have multiple object areas, if we choose enough object areas to represent the information, the capacity is considerable. However, not all areas are suitable for information hiding, the object areas should be filtered based on the requirements to construct a database that can meet most of the requirements of information transmission.

The important remaining parts of this paper are as follows: Section 2 introduces the related works. Section 3 presents the proposed coverless image steganography. We analyze the performance of this method in section 4. Finally, Section 5 summarizes the method and puts forward the next work plan.

2 Related work

2.1 Coverless image steganography

In the image steganography field, the most easy-to-implement algorithm is the Least Significant Bit (LSB) algorithm [Yang, Weng, Wang et al. (2008)]. There are other algorithms for information hiding: HUGO [Pevný, Filler and Bas (2010)], WOW [Holub and Fridrich (2012)], S-UNIWARD [Holub and Fridrich (2013)], and others. Then many transform domain steganography methods have been proposed, such as the hidden method in the DWT domain [Lin, Horng, Kao et al. (2008)], DFT domain [McKeon (2007)], DCT domain [Cox, Kilian, Leightonet et al. (1997)] and IWT domain [Valandar, Ayubi and Barani (2017)]. Nevertheless, the traditional image steganography modifies the content of the image, so that it is hard to resist the detection of steganalysis [Xiang, Wu, Li et al. (2018)]. In order to radically resist the detection of steganalysis algorithms and improve the robustness of image steganography, Bilal et al. proposed "Zero-steganography" in 2013 [Bilal, Imtiaz, Abdul et al. (2013)]. In order to improve security, Zhou et al. proposed the new concept of "coverless" in May 2014 [Zhou, Cao and Sun (2016)]. It does not need to designate and modify a cover image to hide the secret information. Instead, the hiding process is implemented by finding an image or text that already contains the secret information [Zhou, Qin, Xiang et al. (2020)]. As we know, any image contains a lot of information. It is possible to map some relationships between these features and secret information with a proper feature description [Li, Qin, Xiang et al. (2018)], such that the secret text information can be hidden into natural images without modifying [Cao, Zhou, Yang et al. (2018)]. The standard coverless image steganography method is to build mapping relationships between the hash sequences and the secret messages [Xiang, Shen, Qin et al. (2019)].

2.2 Image segmentation

Relying on the development of deep learning, computer vision systems have been substantially improved [Chen, Wang, Xia et al. (2019)]. Semantic segmentation is classifying all pixels of the image, and not restricted by the bounding box. Object detection contains two problems: determining whether objects belonging to a category appear in the image and locating the objects. Instance segmentation combines semantic segmentation with object detection. It can predict the location and category of the objects in the image and segment the detected objects. Panoptic segmentation not only detects all objects in the image and segments the detected objects but also detects and segments the background. Mask RCNN is the preferred network for this type of task, visual examples of object detection, instance segmentation and panoptic segmentation by Mask RCNN is shown in Fig. 1.

Figure 1: Visual examples of object detection and image segmentation

2.3 Mask RCNN

Mask RCNN is an extension of Faster RCNN, which is the preferred network for object detection. It introduces RoI Align, which cancels all quantization operations and stops rounding, so that the output can be in pixel-to-pixel alignment. Accuracy improved significantly from 10% to 50%. It also introduces a semantic segmentation branch to realize the decoupling of the relationship between Mask and class prediction. The loss function of Mask RCNN is calculated as:

$$L = L_{cls} + L_{box} + L_{mask} \tag{1}$$

where L_{cls} is the classification loss, L_{box} is the bounding-box loss, and L_{mask} is used to sort each pixel, which contains $K \times m \times n$ dimensions of output, K is the number of categories, and $m \times n$ is the size of the extracted RoI image.

Mask RCNN has good generalization adaptability and can be combined with various RCNN frameworks, such as Faster RCNN/ResNet. Fig. 2 shows the framework of Mask RCNN with ResNet. First, the segmentation layer outputs the mask with the K channels. Each mask corresponds to a category. The sigmoid function is used to make a dichotomy to determine whether it belongs to this category. When calculating loss, if the ground truth corresponding to RoI is K_i, only the loss corresponding to the K_i th mask is calculated.

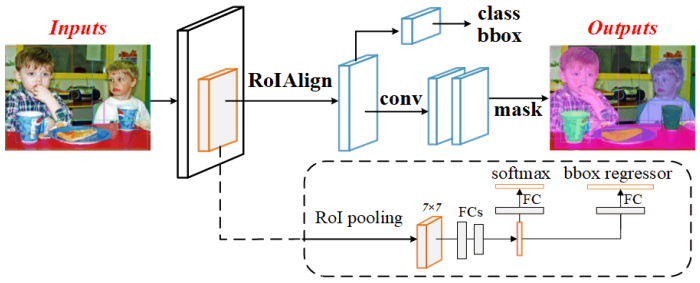

Figure 2: The framework of Mask RCNN with ResNet

3 The proposed steganography scheme

In this section, the proposed steganography scheme is demonstrated. In this framework, a large number of object areas are segmented through Mask RCNN. Then, the needed object areas are selected. We also use robust hash algorithms to generate sequence of the object areas and establish an index for feature matching [Zhou, Jonathan and Sun (2019)]. Therefore, stego-images will be matched and transmitted to the receiver. The main parts of this method include image segmentation, construction of inverted index and steganography process.

3.1 Detection-first instance image segmentation

In our scheme, ResNet is used as the backbone network for Mask RCNN. Considering the mask edge of the object is sensitive, which may reduce the accuracy. Therefore, we use detection-first methods for instance segmentation relied on the detection bounding box. The input image is transmitted through a ConvNet and some learning region

proposal networks. Once these region proposals are given, them will be projected into the convolutional feature map [Wang, Qin, Xiang et al. (2019)]. Mask RCNN performs pixel-level segmentation by adding a branch to Faster RCNN. SoftMax is used to calculate the probability value of each classification, which is calculated as:

$$S_i = \frac{e^{a_i}}{\sum_{k=1}^{T} e^{a_k}} \tag{2}$$

Where, a_i represents the score calculated by the network forward propagation of category i, and S_i represents the probability of category i after the Softmax function.

The cross-entropy formula based on SoftMax is defined as follows:

$$L = -\sum_{i=1}^{T} y_i log S_i \tag{3}$$

Where, y_i represents the real label, S_i represents the probability, and the derivative result of L is as follows:

$$\frac{\partial L}{\partial x_j} = -\sum_k y_k \frac{\partial log S_i}{\partial x_j} = S_j(\sum y_i) - y_j = S_j - y_j \tag{4}$$

Then, the bounding box regression is used obtain the position offset of each region proposal, which is used for regression to obtain more accurate object detection box through Smooth L_1 Loss:

$$smooth_{L_1}(x) = \begin{cases} 0.5x^2 & if\ |x| < 1 \\ |x| - 0.5 & otherwise \end{cases} \tag{5}$$

All positions of the pixel belonging to the object are represented by 1 and the rest by 0 according to the following loss function:

$$loss = -\sum_{j=1}^{n} \hat{y}_j log y_j + (1 - \hat{y}_j) log(1 - \hat{y}_j) \tag{6}$$

where, y_i represents the probability and $\hat{y}_j$ represents the real label. The loss function is shown as follows:

$$\frac{\partial loss}{\partial y} = -\sum_{j=1}^{n} \frac{\hat{y}_j}{y_j} - \frac{1-\hat{y}_j}{y_j} \tag{7}$$

Finally, as shown in Fig. 3, each object can be denoted as (x_0, y_0, x_1, y_1), where (x_0, y_0) represents the position of the top left in each bounding box, (x_1, y_1) represents the position of the bottom right in each bounding box.

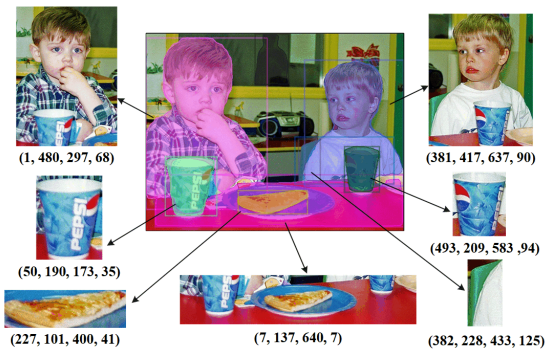

Figure 3: The object areas and the corresponding position points

3.2 Selection of object areas

In our method, the image must have multiple objects in order to convey secret information. However, even the image meets the above requirement, not all areas are suitable for representing secret information. It can be found that the smaller object area might be lost in transmission, while the larger object area could not resist the geometric attack and the content would be destroyed in transmission. By setting a threshold, the appropriate object areas are selected, which can escape geometric attacks. Mask RCNN is used to segment all the object areas of 1000 images, and count the number of object areas with different sizes. The ratio is shown in Fig. 4. The areas of 0-5 KB are easy to be lost and cannot hide enough information. And the number of areas >50 KB is few. The object areas of 5-25 KB are more suitable to be selected.

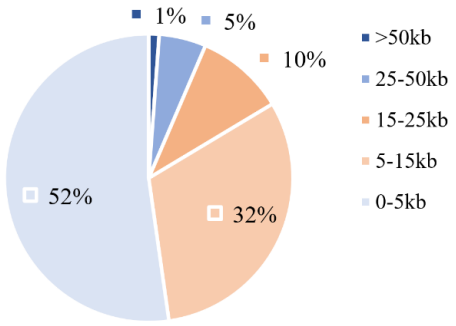

Figure 4: Ratio of different object areas

All object areas are screened in the image, and the image without suitable object area are discarded. At the same time, the selected object areas should contain as few objects as possible. A database is constructed that conforms to these selected object areas and the original images. The sample images are shown in Fig. 5. It can be seen that the selected object areas still have good structural integrity when being randomly attacked.

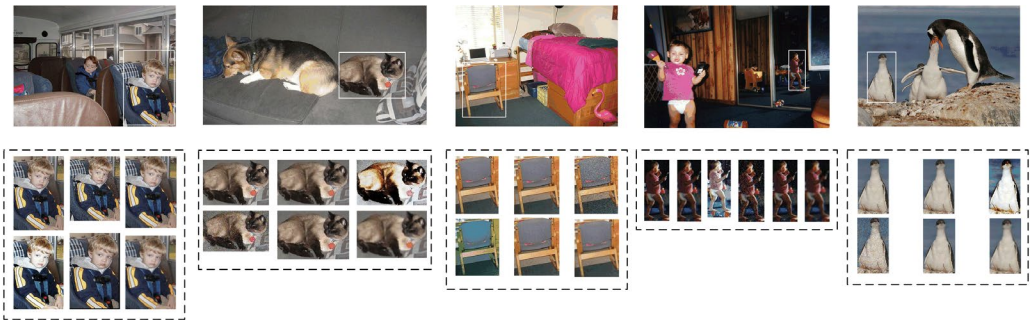

Figure 5: Selection of object area under attack

3.3 Construction of inverted index

After extracting the object areas, we need to generate hash sequence of the object areas, such that the secret information can be represented by the sequence. To speed up the

matching of secret information and object areas, an index needs to be constructed. As shown in Fig. 6, the inverted index structure contains all possible 8 bits hash sequences as entries. Under each entry is a set of object areas, which including the corresponding stego-images, and feature points that can be used to find the object areas. Note that there should be at least one image under each entry of sequence codes to ensure that for any combination of sequence codes, the corresponding image can be found in the index structure. If an image has multiple suitable object areas, this stego-image can be searched through its different object area (X).

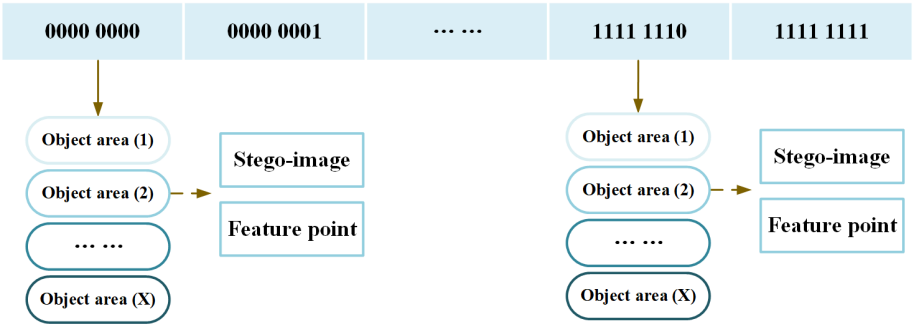

Figure 6: The inverted index

3.4 Steganography process

As shown in Fig. 7, information transmission includes the following three parts:

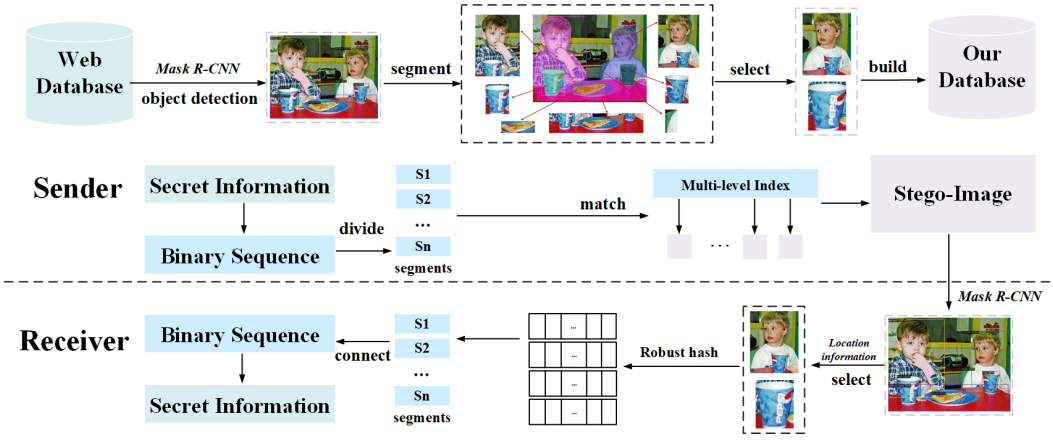

Figure 7: Coverless image steganography based on image segmentation

(1) Image pre-processing. A large number of suitable images are selected from COCO and VOC for building our dataset. Then the robust hash algorithm is used to generate the hash sequence of object areas. Based on it, an inverted index is constructed.

(2) The sender segments the secret information, match them to the object areas and obtain the corresponding stego-image and feature points. To ensure the security,

theses feature points will be encrypted in reverse order. After that, these images are sent to the receiver. The corresponding algorithm is described as follows.

Algorithm 1: Secret information hiding

Input: Secret information: S

Output: Stego-image: $I = \{I1, I2, \ldots, In\}$, Feature points: $P = \{P1, P2, \ldots, Pn\}$

1: Convert *S* into binary string

2: Divide the binary string

3: *for* binary segments, do

4: match it in the inverted index

5: get the corresponding stego-image and feature points

6: end *for*

7: Arrange *P* in reverse order

8: Get $I = \{I1, I2, \ldots, In\}$ and $P = \{P1, P2, \ldots, Pn\}$

(3) The receiver uses Mask RCNN to obtain the object areas from stego-images according to feature points. Next, the sequences of the object areas are generated by hash algorithm and sequentially concatenated to obtain secret information. The algorithm is described as follows.

Algorithm 2: Secret information extraction

Input: Stego-image: $I = \{I1, I2, \ldots, In\}$, Feature points: $P = \{P1, P2, \ldots, Pn\}$

Output: Secret information: S

1: Arrange P in reverse order

2: Get the correct feature points

3: *for* I, do

4: segment the object area by Mask RCNN

5: select the correct object area by *P*

6: end *for*

7: Get a set of object areas

8: *for* object area

9: generate binary sequence through hash algorithm

10: end *for*

11: Connect all binary sequence in order

12: Get S

4 Experimental results and analysis

Experimental environment: Intel® Core (TM) i7-9700KF CPU @ 3.60GHz, 16.00 GB RAM and one Nvidia GeForce GTX 2080 Ti GPU. The pytorch 1.3.1 framework is adopted. All experiments are completed in MATLAB 2016a and Pycharm.

Data sets: MS COCO 2014, Cityscapes and VOC 2007 are used to train Mask RCNN and ResNet 101. All images in COCO and VOC are screened to construct our data set in advance. The details of these data sets are described below and the sample images of these datasets are shown in Fig. 8.

(1) MS COCO 2014 includes 91 categories. It has 82,783 training, 40,504 validation, and 40,775 testing images with 270k segmented people and 886k segmented objects.

(2) Cityscapes has 5000 images of urban driving scenes, which are divided into 2975,500 and 1525 images for training, verification, and testing respectively.

(3) PASCAL VOC 2007 is divided into four categories with a total of 20 subclasses. The training set contains 2501 images and 6301 objects. The testing set contains 9,963 images and 24,640 objects.

(4) PASCAL VOC 2012 is similar to VOC 2007. Its training set contains 5,717 images and 13,609 objects, and its testing set contains 23,080 images and 54,900 objects.

(a) MS COCO 2014 (b) Cityscapes

(c) PASCAL VOC 2007 (d) PASCAL VOC 2012

Figure 8: The sample images of datasets (a) MS COCO 2004 (b) Cityscapes (c) PASCAL VOC 2007 (d) PASCAL VOC 2012

Experimental setting: All images are resized to 128×128 for the experiment. The details of the compared mainstream coverless image steganography methods are shown as follows:

(1) Pixel-based method [Zhou, Cao and Sun (2016)] divides the image into image blocks evenly and extracts the average pixel value of each image block to generate a hash sequence in Zig-zag order for information hiding.

(2) SIFT-based method [Yuan, Xia and Sun (2017)] divides the image into image blocks evenly and extracts the SIFT features of each image block to generate hash sequence in Zig-zag order for information hiding.

(3) DCT-based method [Luo, Qin, Xiang et al. (2020)] binarizes the image to generate hash sequence through a discrete cosine transform for information hiding [Bilal, Imtiaz, Abdul et al. (2013)].

(4) DWT-based method [Liu, Xiang, Qin et al. (2020)] is similar to DCT, and binarizes the image to generate hash sequence through discrete wavelet transform for information hiding.

The above hash algorithms are all applied to our scheme for experiments. For example, Pixel (ours) divides the object areas into blocks evenly and extracts the average pixel value of each block to generate a hash sequence in Zig-zag order for information hiding.

In order to ensure the safe transmission of secret information, we will evaluate our method in three aspects: anti-steganalysis, capacity, and robustness.

4.1 Anti-steganalysis

Steganalysis consists of two parts: steganalysis and secret information extraction, it reveals the existence of secret information in the image. Most steganalysis methods analyze the influence of embedded secret information, which utilize the correlation between different color channels on the statistical characteristics of images [Kang, Liu, Yang et al. (2019)]. The traditional image steganography methods embed the secret information into the image by modifying the content or structure of the image. Therefore, steganalysis tools can detect the existence of secret information through the modification traces left in the image. However, instead of modifying the content or structure of the image, we transmit a set of stego-images without modification. Meanwhile, although these images aroused the suspicion of the attackers, the secret information cannot be extracted without the corresponding mapping relationships. Therefore, our method is resistant to steganalysis tools and has a strong anti-steganalysis.

4.2 Capacity

The capacity of coverless steganography is limited by the hash length of the image. How to improve the capacity in coverless image steganography has become the focus, capacity becomes a critical evaluation index. In this section, the bits per image is used as the measure of capacity. With the improvement of steganography, the capacity is gradually improved [Qin, Luo, Xiang et al. (2019)]. In our scheme, we segmented the image, extracted the needed areas to hide information. If DCT is used in our method to generate the sequence of each object area, it can hide 8-15 bits secret information. Although image segmentation will reduce the capacity, multiple object areas can be selected from an image to ensure the capacity. As shown in Tab. 1, where N is the number of object areas in an image. Method [Zhou, Cao and Sun (2016)] [Yuan, Xia and Sun (2017)] all divide image into 3×3 blocks to generate binary sequence, which can hide 8 bits information. Method [Luo, Qin, Xiang et al. (2020); Liu, Xiang, Qin et al. (2020)] both based on transform domain, which can generate 1~15 bits binary sequence. Above all, our capacity can meet the needs of most information transmission.

Table 1: The capacity comparison

Method	Capacity(bits/image)
Ours	(8-15)×N
[Zhou, Cao and Sun (2016)]	8
[Yuan, Xia and Sun (2017)]	8
[Luo, Qin, Xiang et al. (2020)]	1-15
[Liu, Xiang, Qin et al. (2020)]	1-15

4.3 Robustness

In the process of transmission, the image will inevitably be attacked, and the information needs to resist these attacks. In evaluating the robustness, the most important index is the success rate of secret data extraction, which is calculated as:

$$SR = \frac{\sum_{i=1}^{m} h_i \cap e_i}{m} \tag{8}$$

where m represents the number of transmitted object areas, h_i represents the hided bits of each area and e_i represents the corresponding extracted bits.

In order to prove the effectiveness of our scheme, we randomly selected 100 images from our dataset to test robustness against 3 common geometric attacks. The selected geometric attacks are shown in Fig. 9, and their parameters are shown in Tab. 2.

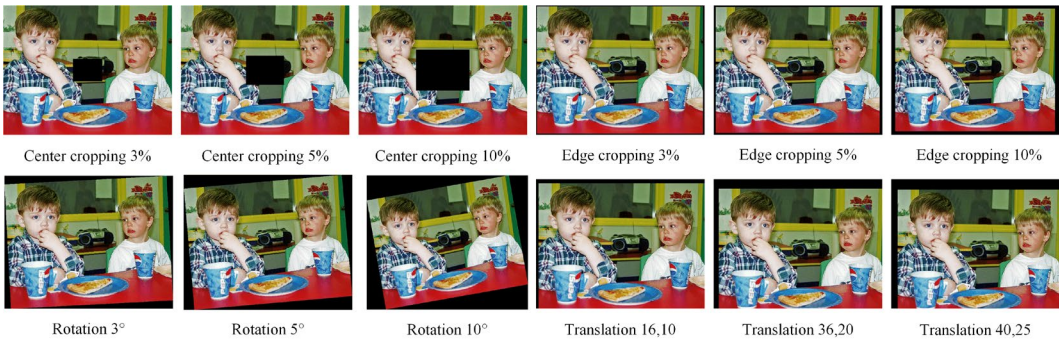

Figure 9: The geometric attack schemes

Table 2: The specific parameters of geometric attacks

Attack	The specific parameters
Center cropping	3%, 5%, 10%
Edge cropping	3%, 5%, 10%
Rotation	3°, 5°, 10°
Translation	(16, 10), (36, 20), (40, 25)

Because geometric attacks will affect the integrity of the image. In theory, as long as the object areas are not maliciously damaged, it can be regarded as not being attacked. The success rates of extraction of different methods under geometric attack are shown in the

Tabs. 3-6. Notably, "ours" represents we use the same hash method to generate the sequence of the object areas for information hiding.

Table 3: The success rate of extraction of different methods under cropping

Attack	Ours	Pixel	Ours	SIFT	Ours	DCT	Ours	DWT
Center cropping 3%	**68%**	67%	37%	47%	63%	72%	**63%**	63%
Center cropping 5%	**61%**	44%	**42%**	31%	**61%**	50%	**60%**	44%
Center cropping 10%	**52%**	25%	**27%**	17%	**46%**	29%	**46%**	23%

From Tab. 3, in the face of center cropping, the smaller the attack scope, the less content is lost. For example, if the cropping area is only 3%-5%, the existing scheme can ignore the loss of this content and achieve better robustness. However, when the cropping area reaches 10%, our scheme can significantly avoid the areas under attack, so it is more robust than the existing coverless steganography scheme.

Table 4: The success rate of extraction of different methods under cropping

Attack	Ours	Pixel	Ours	SIFT	Ours	DCT	Ours	DWT
Edge cropping 3%	64%	85%	39%	47%	58%	82%	70%	85%
Edge cropping 5%	62%	77%	33%	34%	60%	74%	65%	77%
Edge cropping 10%	57%	62%	**31%**	13%	**58%**	58%	**61%**	58%

From Tab. 4, in the face of edge cropping, our scheme does not show great advantages. Because different from the central cropping, edge cropping attacks the image at the edge, so it is easier to ignore its impact on the image if the cropping area is small. It is not difficult to infer that our method will be more advantageous in comparison with the increase of the cropping areas.

Table 5: The success rate of extraction of different methods under cropping

Attack	Ours	Pixel	Ours	SIFT	Ours	DCT	Ours	DWT
Rotation 3°	50%	53%	**17%**	5%	50%	55%	**45%**	42%
Rotation 5°	**38%**	33%	**14%**	4%	**35%**	33%	**34%**	29%
Rotation 10°	**20%**	9%	**8%**	3%	**24%**	8%	**17%**	8%

From Tab. 5, in the face of rotation, the pixels are affected, our method is also affected by rotation. Since only the selected object areas are used for information hiding, our method could avoid the content loss caused by rotation in a small range, so it has better robustness.

Table 6: The success rate of extraction of different methods under cropping

Attack	Ours	Pixel	Ours	SIFT	Ours	DCT	Ours	DWT
Translation 16,10	**58%**	50%	**32%**	7%	**59%**	53%	**53%**	41%
Translation 36,20	**50%**	24%	**24%**	1%	**46%**	23%	**49%**	13%
Translation 40,25	**47%**	16%	**14%**	3%	**45%**	14%	**49%**	12%

From Tab. 6, in the face of translation, as the position of the whole image changes, the pixel points change, so the robustness of the existing steganography is poor. However,

our scheme is not affected by the position, and only a small part of the content is lost when being attacked, which obviously has better robustness.

From the above experimental results, it can be found that among the four existing mainstream hash algorithms, almost all algorithms can be well combined with our scheme except SIFT+HASH. The main reason is that SIFT+HASH is calculated based on SIFT feature points, the change in the bounding box will bring errors in our scheme. It also can be found that compared with the existing 4 mainstream coverless image steganography methods, our method has a significant advantage when being geometric attacked, which ensures the security of secret information.

5 Conclusions

In this paper, we propose a coverless image steganography method based on image segmentation. In our scheme, object detection is introduced, coverless steganography and image segmentation are well combined. We extract semantic features based on ResNet and use Mask RCNN to segment the object areas from COCO and VOC dataset. To ensure the integrity of the image, the suitable object areas are choosen for information hiding. Then, sequence codes of these object areas are generated through the robust hash algorithm. Only a set of stego-images with corresponding feature points are transmitted, which are unrelated to the secret information, it fundamentally resists steganalysis and guarantees the security of secret information. Compared with the existing methods, this method can extract multiple object areas from the image, which guarantees the capacity to some extent. Meanwhile, this method has better robustness, especially when facing geometric attacks. In future work, we will consider expanding our data set while ensuring the efficiency of time and space.

Acknowledgment: I would like to thank my partners: Wenyan Pan and Qiang Liu. They provided me with technical support and helped me revise the manuscript. I would also lik e to thank my alumnus: Wentao Ma and Zhuo Zhou, I successfully completed the format requirements of the manuscript with their help.

Funding Statement: This work was supported in part by the National Natural Science Foundation of China under Grant 61772561, author J. Q, http://www.nsfc.gov.cn/; in part by the Key Research and Development Plan of Hunan Province under Grant 2018NK2012, author J. Q, http://kjt.hunan.gov.cn/; in part by the Science Research Projects of Hunan Provincial Education Department under Grant 18A174, author X. X, http://kxjsc.gov.hnedu.cn/; in part by the Degree & Postgraduate Education Reform Project of Hunan Province under Grant 2019JGYB154, author J. Q, http://xwb.gov.hnedu.cn/**;** in part by the Postgraduate Excellent teaching team Project of Hunan Province under Grant [2019]370-133, author J. Q, http://xwb.gov.hnedu.cn/**;**and in part by the Postgraduate Education and Teaching Reform Project of Central South University of Forestry & Technology under Grant 2019JG013, author X. X, http://jwc.csuft.edu.cn/.

Conflicts of Interest: We declare that we have no conflicts of interest to report regarding the present study.

References

Bilal, M.; Imtiaz, S.; Abdul, W.; Ghouzali, S. (2013): Zero-steganography using DCT and spatial domain. *Proceedings of AICCSA*, pp. 1-7.

Cao, Y.; Zhou, Z. L.; Yang, C. N.; Sun, X. M. (2018): Dynamic content selection framework applied to coverless information hiding. *Journal of Internet Technology*, vol. 19, no 4, pp. 1179-1186.

Chen, Y. T.; Wang, J.; Xia, R. L.; Zhang, Q.; Cao, Z. H. et al. (2019): The visual object tracking algorithm research based on adaptive combination kernel. *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 4855-4867.

Cox, I. J.; Kilian, J. J.; Leightonet, T.; Shamoon, T. (1997): Secure spread spectrum watermarking for images, audio and video. *Proceedings of 3rd IEEE International Conference on Image Processing*, vol. 3, pp. 243-246.

Holub, V.; Fridrich, J. (2012): Designing steganographic distortion using directional filters. *IEEE International Workshop on Information Forensics and Security*, pp. 234-239.

Holub, V.; Fridrich, J. (2013): Digital image steganography using universal distortion. *ACM Workshop on Information Hiding and Multimedia Security*, pp. 59-68.

Kang, Y. H.; Liu, F. L.; Yang, C. F.; Xiang, L. Y.; Luo, X. Y. et al. (2019): Color image steganalysis based on channel gradient correlation. *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, pp. 1-13.

Li, H.; Qin, J. H.; Xiang, X. Y.; Pan, L. L.; Ma, W. T. et al. (2018): An efficient image matching algorithm based on adaptive threshold and RANSAC. *IEEE Access*, vol. 6, no. 1, pp. 66963-66971.

Lin, W. H.; Horng, S. J.; Kao, T. W.; Fan, P. Z.; Lee, C. L. et al. (2008): An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia*, vol. 10, no 5, pp. 746-757.

Liu, Q.; Xiang, X. Y.; Qin, J. H.; Tan, Y.; Tan, J. S. et al. (2020): Coverless steganography based on image retrieval of Dense Net features and DWT sequence mapping. *Knowledge-Based Systems*, vol. 192, pp. 105375-105389.

Luo, Y. J.; Qin, J. H.; Xiang, X. Y.; Tan, Y.; Liu, Q. et al. (2020): 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.

McKeon, R. T. (2007): Strange fourier steganography in movies. *IEEE International Conference on Electro/Information Technology*, pp. 178-182.

Pevný, T.; Filler, T.; Bas, P. (2010): Using high-dimensional image models to perform highly undetectable steganography. *Proceedings of Information Hiding*, pp. 161-177.

Qin, J. H.; Luo, Y. J.; Xiang, X. Y.; Tan, Y.; Huang, H. J. (2019): Coverless image steganography: a survey. *IEEE Access*, vol. 7, no. 1, pp. 171372-171394.

Valandar, M. Y.; Ayubi, P.; Barani, M. J. (2017): A new transform domain steganography based on modified logistic chaotic map for color images. *Journal of Information Security and Applications*, vol. 34, no. 2, pp. 142-151.

Wang, J.; Qin, J. H.; Xiang, X. Y.; Tan, Y.; Pan, N. (2019): CAPTCHA recognition based on deep convolutional neural network. *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 5851-5861.

Xiang, L. Y.; Shen, X.; Qin, J. H.; Hao, W. (2019): Discrete multi-graph hashing for large-scale visual search. *Neural Processing Letters*, vol. 49, no. 3, pp. 1055-1069.

Xiang, L. Y.; Wu, W. S.; Li, X.; Yang, C. F. (2018): A linguistic steganography based on word indexing compression and candidate selection. *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28969-28989.

Yang, C. H.; Weng, C. Y.; Wang, S. J.; Sun, H. M. (2008): 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.

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

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

Zhou, Z. L.; Jonathan, W.; Sun, X. M. (2019): Multiple distance-based coding: toward scalable feature matching for large-scale web image search. *IEEE Transactions on Big Data*, pp. 1-1.

Zhou, Z. L.; Mu, Y.; Jonathan, W. (2018): Coverless image steganography using partial-duplicate image retrieval. *Soft Computing*, vol. 23, pp. 4927-4938.

Zhou, Z.; Qin, J. H.; Xiang, X. Y.; Tan, Y.; Liu, Q. et al. (2020): News text topic clustering optimized method based on TF-IDF algorithm on spark. *Computers, Materials & Continua*, vol. 62, no. 1, pp. 217-231.