Copyright © 2019 Tech Science Press JIHPP, vol.1, no.1, pp.43-48, 2019

A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography

Ruohan Meng[1, 2], Zhili Zhou[1, 2], Qi Cui[1, 2], Xingming Sun[1, 2, *] and Chengsheng Yuan[1, 2, 3]

Abstract: At present, the coverless information hiding has been developed. However, due to the limited mapping relationship between secret information and feature selection, it is challenging to further enhance the hiding capacity of coverless information hiding. At the same time, the steganography algorithm based on object detection only hides secret information in foreground objects, which contribute to the steganography capacity is reduced. Since object recognition contains multiple objects and location, secret information can be mapped to object categories, the relationship of location and so on. Therefore, this paper proposes a new steganography algorithm based on object detection and relationship mapping, which integrates coverless information hiding and steganography. In this method, the coverless information hiding is realized by mapping the object type, color and secret information in object detection method. At the same time, the object detection method is used to find the safe area to hide secret messages. The proposed algorithm can not only improve the steganographic capacity of the two information hiding methods but also make the coverless information hiding more secure and robust.

Keywords: Steganography, faster R-CNN, coverless information hiding.

1 Introduction

Coverless information hiding was formally put forward by experts in 2014. Because the information hiding method is to hide information by modifying the pixels of the cover image, this means that the cover image will be changed. As long as the cover image changes, there is the possibility of being discovered by the detector. In order to transfer secret information without changing the cover image, coverless information hiding is proposed. Coverless information hiding refers to the natural image which is driven by secret information and searches for the corresponding feature information according to the mapping dictionary of secret information and feature information without changing

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

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

[2] Department of Electrical and computer Engineering, University of Windsor, Windsor, ON, Canada N9B 3P4.

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

the cover image. By sharing the mapping dictionary of secret information and characteristic information with the receiver, the receiver extracts secret information according to certain index relationship after the natural image with certain information. In the field of coverless information hiding, there have been some research results. Zhou et al. [Zhou, Sun, Harit et al. (2015); Yuan, Xia and Sun (2017); Yuan, Li, Wu et al. (2017); Cao, Zhou, Sun et al. (2018)] proposed to combine coverless information hiding with image retrieval and fingerprint liveness detection techniques to increase the hiding capacity and make it safer. In addition to using traditional statistical feature method to hide information without a carrier, some people combine deep learning model with coverless information hiding. Liu et al. [Liu, Zhang, Liu et al. (2017)] proposed using the corresponding categories of generative adversarial networks to replace the secret information as the driver to map the secret information. The generator generates the image corresponding to the secret information directly and uses the discriminator to extract the secret information. Ke et al. [Ke, Zhang, Liu et al. (2017)] proposed a generative coverless information hiding method based on Kerckhoffs' Principle and generative adversarial networks. In addition, some people combined coverless with deep learning and have improved [Duan, Song, Qin et al. (2018)].

In image steganography algorithm, the least significant bit (LSB) steganography algorithm is the most representative one in the early stage. But it cannot resist statistical characteristics. In recent years, adaptive steganography algorithms hide information by searching for areas with complex texture and rich noise in images. This kind of algorithm has been greatly improved in resisting steganalysis. In addition to using traditional methods for steganography, information hiding combined with deep learning model has also been paid too much attention. Steganography algorithm based on deep learning Meng et al. [Meng, Cui and Yuan (2018)] proposed that it can be divided into three categories: steganographic algorithms of adversarial method [Hayes and Danezis (2017); Shi, Dong, Wang et al. (2017); Yang, Liu, Kang et al. (2018)], steganographic algorithms of hiding entire secret image [Baluja (2017); Rahim and Nadeem (2017); Zhang, Dong and Liu (2018)] and steganographic algorithms of selecting embedding location and others [Wu, Wang and Shi (2016); Atee, Ahmad, Noor et al. (2017)].

In the kind of steganographic algorithms of selecting embedding location and others, Meng et al. [Meng, Rice, Wang et al. (2018)] proposed to select the security area in the image for information hiding. In certain cases, the texture of object area is more complex than the background area. Therefore, by using object detection method to select the object area, combined with a variety of adaptive steganography algorithm for information hiding. In this process, because the object area is limited and the background is abandoned, the hiding capacity of an image will be reduced relatively. Secondly, because object regions can be proposed independently, and object regions have different classifications and meanings, as well as certain location information between objects, these features are conducive to coverless information hiding. Therefore, this paper proposes to combine the coverless information hiding with the steganography algorithm proposed by Meng et al. [Meng, Rice, Wang et al. (2018)]. It can solve the problem of low capacity of coverless information hiding, and also deal with the problem of steganographic capacity reduction of the algorithm proposed by Meng et al. [Meng, Rice, Wang et al. (2018)]. In addition, the content steganography in the object area can be an indication of the extraction order in the coverless information hiding method, and the two methods complement each other.

2 The proposed scheme

This part mainly describes the model we proposed. First, we need to build a mapping dictionary between secret information and feature information. We choose three aspects of feature information: (1) object category; (2) position characteristics between objects; (3) number of objects; (4) the color of objects. As shown in Fig. 1, it is an experiment result by faster region-based convolutional neural networks (faster R-CNN) with a nature image. Object category refers to which category each selected object belongs to, such as people, dogs, cars, etc. The location characteristics between objects refer to the information of a man riding a horse and a dog on the left side of a horse. The number of objects refers to the number of objects in each category and the sum of the number of objects in each category. The color of objects means that the objects contain the information of colors. For examples, a brown horse, a gray car. The examples of the dictionary as can be seen in Tab. 1. By establishing this mapping dictionary, the secret information corresponds to the feature information.

Table 1: The examples of the dictionary

Category	Category combination tags
Horse	0001
Brown horse	0031
People ride on the horse	0500
One cars	2005
Four objects	8503

As shown in Fig. 2, it is the overall architecture of the model. First, the secret information is converted to a binary sequence and then driven by the binary sequence. Searching for feature information corresponding to secret information. Second, the image that meets the requirement of secret information is input into the faster R-CNN model as a cover image. In turn, feature extraction, target box selection, feature map size normalization, border regression and classification are performed. Among them, Visual Geometry Group (VGG) is a kind of deep convolution network. This is used to extract image features. Regional proposal network (RPN) generates Proposals through the use of sliding window + anchor mechanism. An image of the object area is selected. Third, we use existing adaptive steganography algorithms such as highly undetectable steganography algorithm (HUGO), spatial-universal wavelet relative distortion (S-UNIWARD) and wavelet obtained weights (WOW) to hide secret information into the object area. At the same time, all kinds of characteristic information corresponding to secret information. Finally, the stego images are got and sent to the receiver. The total loss function of faster R-CNN is shown in Eq. (1).

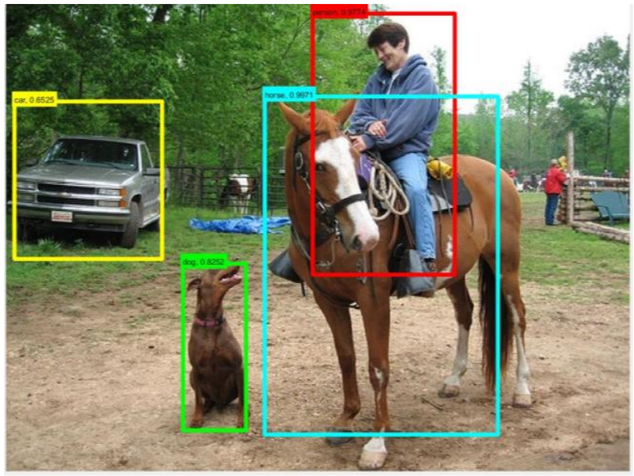

Figure 1: An experiment result by faster R-CNN with a nature image

$$L(\{p_i\},\{t_i\}) = \frac{1}{N_{cls}}\sum_i L_{cls}(p_i, p_i^*) + \lambda \frac{1}{N_{reg}}\sum_i p_i^* L_{reg}(t_i, t_i^*) \tag{1}$$

Here, p_i refers to the probability of judging that the anchor i is an object. $t_i = \{t_x, t_y, t_w, t_h\}$ is the coordinate value of the predicting the bounding box. p_i^* as shown in function (2).

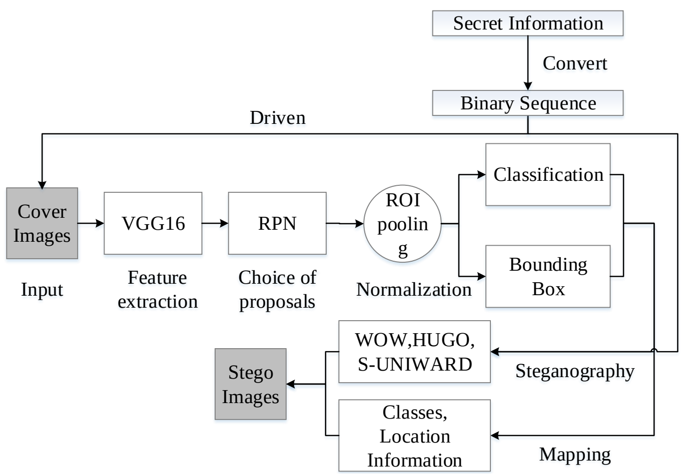

Figure 2: The structure of our proposed scheme

$$p_i^* = \begin{cases} 0 & negative\,lable \\ 1 & positive\,lable \end{cases} \tag{2}$$

$L_{cls}(t_i, t_i^*)$ is the loss of target and non-target. And $L_{reg}(t_i, t_i^*)$ is the regression loss.

When using coverless information hiding, we need to tell receiver about the index relation. The process is to connect binary codes in the right order when secret information is restored. Therefore, in the steganography process, the index relation can be converted to binary code hidden in the image. Besides, other secret information can also be hidden in images.

In the process of extraction, as can be seen in Fig. 3, the secret binary is extracted by the corresponding extraction algorithm of the steganography algorithm. According to the mapping relation between binary code and secret information, secret message is recovered. The secret information contained in the recovered information contains the index relation in coverless information hiding. While extracting secret information according to the extraction algorithm, receiver recovers secret binary code according to the mapping dictionary. Then, sort binary codes according to index relations. Finally, the secret information obtained through two ways will be merged.

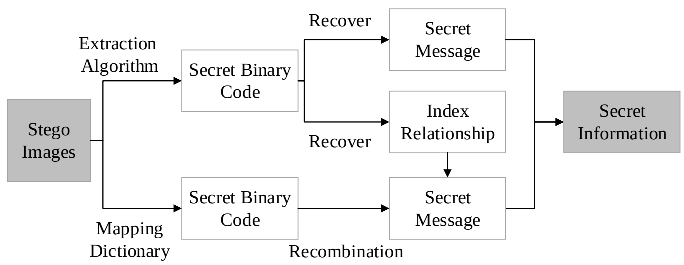

Figure 3: The process of extraction

3 Conclusion and future work

In this paper, a method combining coverless information hiding with embedded steganography is proposed. It can not only solve the problem of low hiding capacity of coverless information hiding and steganography proposed by Meng et al. [Meng, Rice, Wang et al. (2018)], but also increase the security of information hiding. The steganographic capacity and the steganography ability of the method can be illustrated by experiments in the future. In the same time, we will try to find a more suitable way to combine coverless information hiding with steganography algorithm.

Acknowledgement: This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant U1836208, U1536206, U1836110, 61602253, 61672294; by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20181407; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

References

Atee, H. A.; Ahmad, R.; Noor, N. M.; Rahma, A. M. S.; Aljeroudi, Y. (2017): Extreme learning machine based optimal embedding location finder for image steganography. *Plos One*, vol. 12, no. 2, e0170329.

Baluja, S. (2017): Hiding images in plain sight: deep steganography. *Advances in Neural Information Processing Systems*, pp. 2069-2079.

Cao, Y.; Zhou, Z.; Sun, X.; Gao, C. (2018): Coverless information hiding based on the molecular structure images of material. *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197-207.

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

Hayes, J.; Danezis, G. (2017): Generating steganographic images via adversarial training. *Advances in Neural Information Processing Systems*, pp. 1954-1963.

Ke, Y.; Zhang, M.; Jia, L.; Su, T.; Yang, X. (2017): Generative steganography with Kerckhoffs' principle based on generative adversarial networks. arXiv:1711.04916.

Liu, M.; Zhang, M.; Liu, J.; Zhang, Y.; Ke, Y. (2017): Coverless information hiding based on generative adversarial networks. arXiv:1712.06951.

Meng, R.; Cui, Q.; Yuan, C. (2018): A survey of image information hiding algorithms based on deep learning. *Computer Modeling in Engineering & Sciences*, vol. 117, no. 3, pp. 425-454.

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

Rahim, R.; Nadeem, M. S. (2017): End-to-end trained CNN encode-decoder networks for image steganography. arXiv:1711.07201.

Shi, H.; Dong, J.; Wang, W.; Qian, Y.; Zhang, X. (2017): SSGAN: secure steganography based on generative adversarial networks. *Pacific Rim Conference on Multimedia*, pp. 534-544.

Wu, H. Z.; Wang, H. X.; Shi, Y. Q. (2016): Can machine learn steganography? implementing LSB substitution and matrix coding steganography with feed-forward neural networks. arXiv:1606.05294.

Yang, J.; Liu, K.; Kang, X.; Wong, E. K.; Shi, Y. Q. (2018): Spatial image steganography based on generative adversarial network. arXiv:1804.07939.

Yuan, C.; Li, X.; Wu, Q. J.; Li, J.; Sun, X. (2017): Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. *Computers, Materials & Continua*, vol. 53, no. 3, pp. 357-371.

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

Zhang, R.; Dong, S.; Liu, J. (2018): Invisible steganography via generative adversarial networks. arXiv:1807.08571.

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