Hindawi
Security and Communication Networks
Volume 2021, Article ID 6628034, 12 pages
https://doi.org/10.1155/2021/6628034

Research Article

Multimedia Communication Security in 5G/6G Coverless Steganography Based on Image Text Semantic Association

Yajing Hao,[1] Xinrong Yan,[2] Jianbin Wu ,[1] Huijun Wang,[2] and Linfeng Yuan[2]

[1]*College of Physics Science and Technology, Central China Normal University, Wuhan 430079, China*
[2]*Wuhan Maritime Communication Research Institute, Wuhan 430079, China*

Correspondence should be addressed to Jianbin Wu; wujianbin@mail.ccnu.edu.cn

Received 2 October 2020; Revised 28 November 2020; Accepted 6 January 2021; Published 16 January 2021

Academic Editor: Jinwei Wang

Recently, researchers have shown that coverless steganography is relatively safe. On this basis, to improve the payload of the coverless steganography, a novel semiconstruction coverless steganography algorithm is introduced in the paper. Firstly, web crawler technology is applied to crawl a wide range of small icons and hot news images from the Internet. These icons can be used as the training subset, and the hot news can be designed according to construction rules. Secondly, the Alex-Net network is introduced for training in the algorithm, and the adversarial samples are added to the training set. Thirdly, using the preset template, certain small icons and a hot news image are spliced into a secret carrier image according to the construction principle. The hot news image is in the top half of the carrier, and those small icons are in the bottom half. The image on the upper part of the carrier and the icons of the lower part can be connected by image and text semantics, and the semantic matching can be realized between image semantics and explanatory. The experimental results and analysis show that the proposed algorithm can resist steganalysis tools effectively and has good robustness against various image attacks. Meanwhile, the secret information payload has been greatly improved, the maximum payload can reach 180 bits of a single 512 × 512 image. This promising algorithm can be applied to build covert communications.

1. Introduction

In traditional information hiding, secret information is hidden by modifying the original carrier with a high embedding capacity. However, the traditional image steganography methods must modify the carrier to embed information, so the modification traces can be easily detected by advanced steganalysis tools. For this reason, coverless steganography [1] was proposed and has become a research hotspot. "Coverless" [2] does not mean that no cover is needed during the transmission. However, it means that the secret information can be expressed and transmitted by establishing the corresponding relationship between the feature of the carrier and the secret information without directly modifying the carrier [3]. As a branch of information hiding, the coverless image steganography was firstly proposed by Zhou et al. [4]. In general, coverless steganography can be divided into three categories: mapping [5, 6], full structured [7], and semistructured [8, 9]. For structured steganography, the original carrier is not specified in advance. The stego can be directly generated from the secret information according to certain rules [10]. On this basis, the researchers have proposed a variety of schemes for coverless structured steganography, such as coverless steganography based on the zig-zag path [11] and strong robust features [12]. To improve the work of [11], Wang proposed the novel coverless steganography based on SIFT [13], which can effectively optimize the hash coding process. Moreover, the coverless image steganography algorithm based on cartoon images was proposed in the literature [14]. Although, in full structured algorithms, the limitation of capacity can be solved, it is still difficult to resist attacks against samples and the extraction of secret information that requires powerful computing support.

Compared with structured steganography, mapping steganography constructs the existence of a mapping relationship, that is, the cover feature expression of the secret information is accomplished by establishing the

corresponding relationship between the carrier and the secret information. The idea of using local information entropy proposed by literature [15] improves the transmission efficiency of coverless steganography to some extent. Recently, a robust coverless steganography algorithm based on the grayscale gradient cooccurrence matrix was proposed in [16]. Besides, Zhou et al. proposed another coverless image steganography which used partial-duplicate image retrieval [17]. Next year, Zou et al. proposed the novel coverless steganography based on the average pixel value of the subimages [18]. In the mapping algorithms, due to the limitations of the mapping mechanism, the image samples needed will be exponentially increased with the increase of the capacity. Furthermore, the random selection of the cover images can reduce the security of the secret transmission.

Recently, researchers have proposed many improved information hiding algorithms for images storage [19, 20]. However, limitations on robustness and hidden capacity still remain unaddressed. Inspired by the theory of behavior steganography in social network proposed by Zhang [21], along with the theory of text coverless information [22] and multikeywords [23], a semistructured coverless steganography algorithm in the literature is proposed, [24] which applies the social platform's behavior habits as the construction principle. Moreover, experimental results [24] show that the proposed algorithm is obviously better than the above algorithms in effect, which shed light on our attempt to investigate coverless steganography based on image text semantic association.

Different from the above algorithm, in order to improve the secret information payload, a semistructured coverless steganography algorithm based on the image and text semantic is introduced in the paper. The secret information is hidden by adjusting small icons according to the construction rules. In general, the image semantic features are associated with the text icons through the preset template; the Alex-Net network is trained to classify text icons to build an image library, which forms a mapping relationship with secret information. In this way, it can not only meet the application requirements but also improve the visual antidetection ability; the experimental results show that the proposed algorithm in this paper has more powerful robustness and logical content; and the maximum secret information payload of a single 512×512 image can reach 180 bits. On the whole, the main contributions of this paper are as follows:

(1) The training set based on adversarial samples is proposed. The adversarial samples can be obtained by using the original icons to undergo common image attack processing. Attacking parameters and types can be adjusted according to the requirement, which can effectively balance the robustness and the capability of resisting image attacks.

(2) A semiconstruction coverless steganography algorithm based on image text semantic association is proposed. The stego image is generated by the semantic association method, and the secret information is hidden by connecting the icons in a certain order during the generation process, which can further reduce the suspicion of attackers with higher antidetection.

The rest of the paper is organized as follows: related work is introduced in Section 2. The basis of our scheme is presented in Section 3. The proposed coverless image information hiding algorithm is depicted in Section 4. Experimental results and analysis are provided in Section 5. Finally, some conclusions are drawn in Section 6.

2. Related Work

2.1. Alex-Net Network Structure. Alex-Net Neural network is a kind of feedforward neural network which was the winner of the 2012 ImageNet competition. Convolution computation is one of the representatives of the deep learning algorithms. Literature [25] shows that Alex-Net network has a good universality, and the features extracted from the pretraining model are widely used in various fields, yielding good results, such as image classification [26] and recognition [27]. There are eight layers of network structure, of which the first five layers are convolutional ones and the last three layers are fully connected ones. There are 60 million parameters and 650,000 neurons in the original Alex-Net model. Compared with the traditional convolutional neural network, Alex-Net applies the ReLU activation function to reduce training time and the dropout technique to reduce overfitting. Moreover, the last layer of neurons derived from Softmax is utilized for classification [28]. The original structure is shown in Figure 1.

Alex-Net algorithm realizes the breakthrough of the deep learning method in image recognition. Moreover, there is excellent performance in the field of image classification in it. This paper aims to improve the practicality of coverless steganography. Taking into account the trend of large-capacity coverless steganography in the future, the training of the Alex-Met network is also preparing for the recognition of large-capacity text icons. The icon library used in this paper is composed of small icons of target English labels. The small icons are regarded as pictures, whose specific features and natural image features share commonness but also with certain differences. For this reason, when using the Alex-Net network for transfer learning, the network structure needs to be adjusted to optimize the learning process. This paper uses a pretrained network, which enables a small number of training images to quickly transfer the learned features to a new task. After Alex-Net, VGGNet [29], GoogLeNet [30], and ResNet [31] has come out, other new CNN frameworks have also been proposed successively. Theoretically, the more layers of a deep learning neural network, the more superior the classification and detection performance [32]. However, in terms of icons in this paper, compared with other deeper networks, Alex-Net reduces the hidden layers, and there is a simpler network structure in it. Meanwhile, the training time is shortened, and a better performance is achieved.

2.2. Transfer Learning. The essence of transfer learning is to use the source domain D_S and the corresponding recognition T_S to transfer the knowledge learned to another task

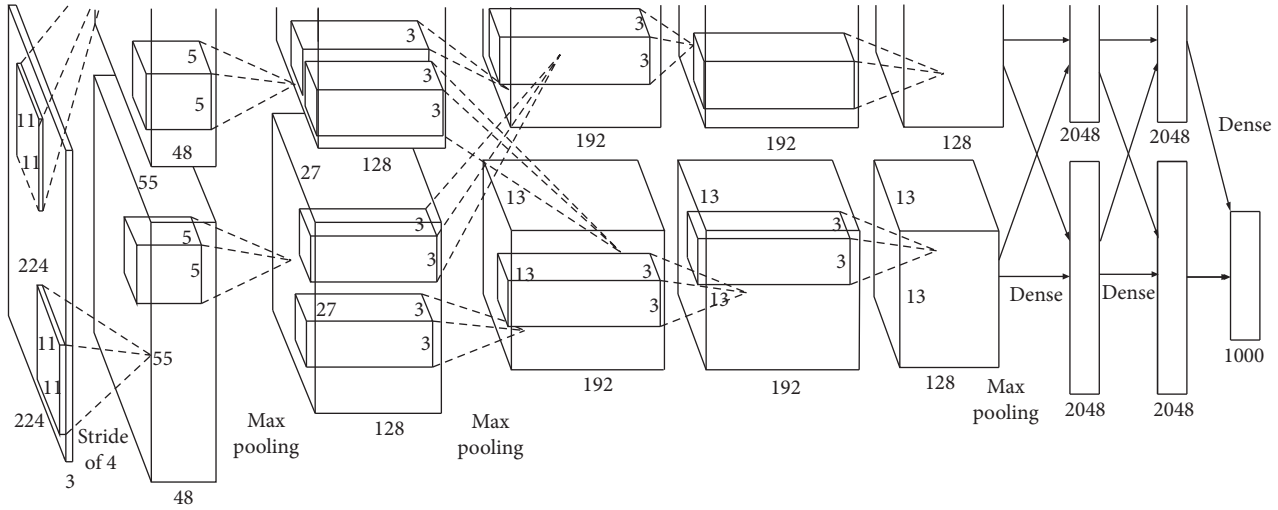

Figure 1: Alex-Net structure model with double GPU training. Dual GPU parallel processing: one GPU is responsible for the top of the image, the other GPU is responsible for the bottom of the image, but both are not completely independent.

T_T for sample recognition in the domain D_T. The transfer learning training of the convolutional neural network mainly includes the following steps:

Step 1: determine the CNN network according to the target task T

Step 2: reuse the CNN model structure according to the tasks of this paper

Step 3: fine-tune model parameters based on target samples

For reusing model structure in Step 2, because the convolutional neural network has good generalization ability in feature extraction, the network structure is carefully designed based on a number of prior datasets. In addition, simply adjusting parameters in all layers will lead to a decline in learning ability. Therefore, in transfer learning, the convolutional layer (layers 1–5) for feature extraction is often reserved. However, adjustments to the network structure are mainly concentrated on the first and the last parts: the image is preprocessed in the input layer to make it meet the input requirements of the network. The dimension, which fully connects the output vector of the last layer, is the category of the classification task. Layer 8 needs to be deleted and rebuilt according to the task during transfer learning. In addition, the input data of the seventh layer is normalized to 1024 classes through the full connection layer, while the other layers remain unchanged.

After establishing the new network structure, the learning hyperparameters are set concretely: learning mode Stochastic Gradient Descent Algorithm (Sgdm), which requires batching of training data. The amount of data in each batch is batch size, whose number is usually set to 2^n. Furthermore, iterative calculations are performed on each batch of data in order to constantly update network parameters. The number of sample training is set to 10 rounds, the learning rate began to be reduced after five rounds, and each parameter was set to 0.2. Among the basic training parameters, Initial Learn Rate is set to 0.0001 in this paper, and the other parameters are the network default parameters. In addition, by fine-tuning the model structure and neuron weights, a network model for classifying and detecting new datasets can be obtained [33].

Recently, transfer learning has been applied in various fields, such as image classification [34], software defect classification [35], and multilingual text classification [36]. In this paper, the new dataset is trained by migrating the parameters of the already trained model. The trained Alex-Net model parameters of the original ImageNet dataset are transferred to the new dataset for training. The first five convolutional layers, corresponding pooling layers, and three fully connected parameters are retained, but other layers are randomly initialized. The last Softmax layer is modified. There are 1,024 one-dimensional neurons in this layer, corresponding to the 1,024 types of text icons in this paper.

3. Basis of Our Scheme

3.1. Image Text Semantic Association. Many complex images can be generated according to the semantic association. Recently, researchers have studied coverless steganography technology based on semantic. The experimental results show that the steganography algorithm based on semantic generation [37] has a high embedding rate and the communication efficiency can be significantly improved. Moreover, taking advantage of the semantics of images to express secret information, the steganography capacity of coverless steganography can also be improved to a certain extent [38]. For this reason, this paper adopts the idea of semantic association, and the principle of construction is shown in Figure 2. The upper part of the whole image is expressed as a hot picture, with its semantics limited to 1-2 characters, and it is randomly presented in the coverless hidden part of the template in the form of answers. The lower part is the hidden part of coverless information, which utilizes text icons as the main body to map secret

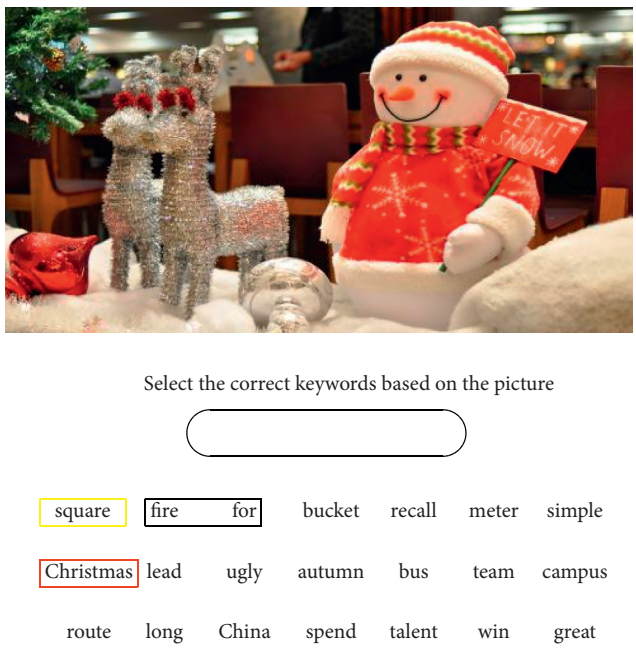

Figure 2: Generated carrier image. The generated image consists of a hotspot image, three rows and seven columns of text icons, some text guidance, and details.

information. Furthermore, the upper and lower parts can be connected by guessing riddles. The realization of the whole program is mainly divided into two parts. The first part is to determine the carrier theme and image content. In the second part, the convolutional neural network—Alex-Net—is trained by transfer learning. And the trained network is used to classify the icon portion of the carrier template. Then, the coverless mapping relationship is constructed to achieve information hiding.

3.2. Image Generation and Coverless Image Information Hiding. As shown in Figure 2, our coverless image steganography includes the upper, the middle, and the lower, which correspond to the hot news image, the text guidance, and the small icons, respectively. The three parts are roughly composed of the following modules: the preset template, some small icons, and the hot news image are spliced into secret carrier image according to the construction principle, the hot news image is in the top half of the carrier, and those small icons are in the bottom half; the image in the upper half of the carrier and the icons in the lower half can be connected by image and text semantics and the semantic matching can be realized between image semantics and interpretation.

The focus of the algorithm is to select appropriate construction principles so that the constructed image by applying the construction principle as a constraint is reasonable in content and logic. Firstly, in this algorithm, the web crawler technology is used to crawl hot news headlines and images on the front page of the theme website, and the keywords are extracted by utilizing the word segmentation tool. Secondly, the text label is constructed by using 21 60×60 icons to form a text template with 3 rows and 7 columns. These text icons have 1024 categories; that is, 10-bit binary information can be represented by a single icon. This includes hot keywords that are crawled, such as the word "Christmas" (in the red box) in the template. In addition, the first two positions except for the first text icon as the flag bit (in the black box) are selected, which is used to store the length of the secret information and the position information of the semantic answer. The first text icon (in the yellow box) is used as the coverless watermark. The calculation process is as follows: after determining the 200-bit binary sequence T, the 200-bit binary sequence T is divided into 20 segments by 10 bits, and each 10-bit segment is converted into a decimal, denoted as $T = \{T1, T2, T3, \ldots, T20\}$; then, the arithmetic average of T is calculated. According to the value, the text icon is placed in the first position of the text template and embedded as a watermark. Finally, the transfer learning feature of the Alex-Net network is used to complete the classification of the text icons; then, the text icons are connected in a certain order according to the secret information. The last part is the fixed elements in the template, mainly including some text guidance and details to improve the template.

The interestingness of the template is considerably significant. The data mining method is used to automatically excavate people's behavior habits from the social platform as the construction principle. The construction principle can be updated in accordance with the hotspot information, and it will improve the security of the stego image when it is transmitted in the public channel of the social platform, which is extremely important. According to this idea, before and after Christmas, the template shown in Figure 2 is used to achieve coverless steganography. Moreover, when the secret information is spread on public channels such as social platforms, the possibility of being attacked by a third party can be greatly reduced. Meanwhile, the security of the hidden communication system has also been improved to a certain extent.

3.3. Establishment of Dataset. In essence, the lower part of the image is the key to achieve steganography. The one-to-one mapping relationship between the secret information and the image library is constructed through the text icons of this paper. There are 1024 60×60 high-frequency English word icons in the image library with a single icon corresponding to a 10-bit binary sequence. Each English icon is regarded as a category, named number "1–1024."

The accuracy of icon recognition by convolutional neural networks directly determines the success of the extraction of secret information in this paper. Therefore, the problem of recognition rate must be considered when building a dataset for training convolutional neural networks in this paper. In order to improve recognition accuracy, the idea of adversarial samples is introduced when transferring the training network [39]. The adversarial sample is to make the model make wrong judgments by simply modifying the target, but these changes are visually minimal and basically

imperceptible. As shown in Figure 3, the convolutional neural network classified the original image as the Alps, but after adding Gaussian noise with an intensity of 0.07 to the image, the network incorrectly classified it as a dog with a probability of 99.99%. The main reason for this phenomenon is that the model training process relies on some unstable features of the image, and the addition of certain disturbances just changes these features, making the model misclassify. The possible disturbances are added to the original sample set to form training data. In this way, these errors will be fitted by the network during the learning process, which is regarded as the correct classification. Therefore, the adversarial sample can be effectively resisted.

Attack methods such as noise adding, smoothing, filtering, and scaling are often used by attackers. From this perspective, we select corresponding adversarial samples training to resist these commonly used attack methods. For example, the adversarial samples corresponding to noise adding are generally resistant to channel transmission problems. Therefore, common noise (salt and pepper noise, Gaussian noise) is selected for training in this paper. Similarly, the smoothed samples are selected for training to suppress noise, which will improve the recognition rate and resistance to the attack. In addition, attackers often interfere and destroy the target according to the frequency of a certain band, so this paper selects the image to be filtered (mean filtering and median filtering) for training. Furthermore, image scaling will increase the smoothness and clarity of the image. In order to improve information security, this paper also uses the images that are generated after the scaling attack as training samples.

Based on the above description, common image attacks are summarized in Table 1.

In the process of transmission, the images are inevitably destroyed by various attacks, so improving robustness is the key to steganography. For this reason, the dataset established in this paper not only contains 1024 types of text icons in the image library but also expands the images of these 1024 types of icons after common various attacks as adversarial samples. In this paper, each text icon and its adversarial sample will form a dataset. The adversarial samples are obtained from the original icons through common image attack processing, such as noise adding, smoothing, filtering, and scaling. Take the icon as an example (as shown in Figure 4).

As indicated from Table 1, the mean value of white Gaussian noise is zero, the variance increases from 0.01 to 0.5, and the step size is 0.02. With the increase of the variance, the noise intensity will increase. The mean value of salt and pepper noise is zero, the intensity is increased from 0.01 to 0.05, and the step size is 0.01. Under actual circumstances, when the noise intensity exceeds 0.7, the icon contents will fail to be classified, which is not in line with the actual situation. Image smoothing is actually low-pass filtering, and the smoothing process will result in blurry image edges. In this training, a linear smoothing method is used to smooth the images disturbed by zero-mean random Gaussian noise. In addition, it should be noted that the amount of disturbance is determined. If excessive noise samples are added to the adversarial samples, the training network will be overfitted, which is not conducive to the detection of icon contents [40]. Therefore, in order not to destroy the image content, the added disturbance should be kept within a reasonable attack range.

The filters mainly refer to mean filters and median filters. The attack size parameters range from 1×1 to 9×9, and 2×2 is specified as the unit interval. The quality factor of JPEG compression changes from 1 to 99 with the unit interval of 1. Each category contains 65 pictures, of which 0.7 is the training set, and the rest is the validation set. The entire training dataset of this paper includes 66,560 images.

4. Proposed Coverless Image Information Hiding Scheme

The proposed scheme includes information hiding and information extracting. Information hiding algorithm based on image text semantic association is described in the following.

4.1. Information Hiding. The specific steps of the entire hidden process are shown as follows: taking the single carrier images in this paper as an example, if the secret information is too long, multiple carrier images can be constructed according to the same rules and transmitted in the form of the image set. It is worth noting that each image in the image set should be reserved with a capacity of 10 bits as the flag bit so that the secret information can be extracted in order. The flow chart of the coverless steganography algorithm is shown in Figure 5.

Step 1: convert the information to be hidden into a binary bit stream S, and obtain the binary sequence length L.

Step 2: determine the subject of the cover images, and obtain the number of subject characters N and the image P.

Step 3: randomly select 2 positions from 3 rows and 7 columns to place the image semantic theme, and record the position POS = {POS1, POS2} in sequence.

Step 4: successively connect the secret information length L, the position of semantic answers POS, and the secret information S. If the secret information length is less than 200 bits, it will randomly compensate 0 or 1 afterwards until 200 bits, which is marked as T.

Step 5: divide the binary sequence T into 20 segments by 10 bits and record as $T = \{T1, T2, T3, \ldots, T20\}$. The corresponding English icons are retrieved in the established coverless image library.

Step 6: calculate the coverless watermark W according to the value of T, and map to an icon placed on the first of the template.

Step 7: splice the image P, English icons, and other templates in accordance with puzzle rules to obtain the carrier image X.

4.2. Information Extraction. The secret information extraction process is known as the hidden inverse process. At

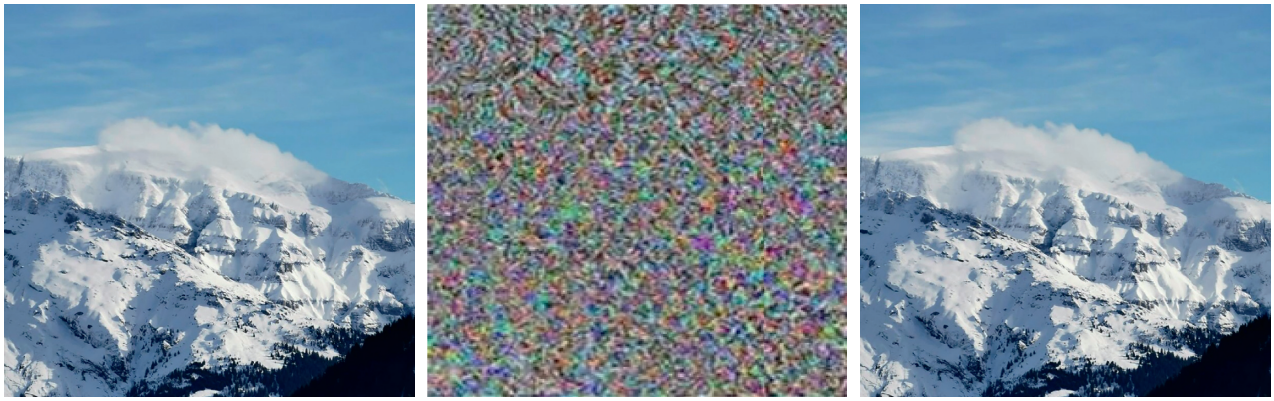

Figure 3: Before and after adding adversarial samples.

Table 1: The kind of image attacks used in the paper.

Attack	The specific parameters
JPEG compression	The quality factors Q: 50%, 70%, 90%
Gauss noise	The mean μ: 0, the variances σ: 0.1, 0.5
Salt and pepper noise	The mean μ: 0, the variances σ: 0.01, 0.05
Mean filtering	The window size: 3×3, 5×5, 7×7
Median filtering	The window size: 3×3, 5×5, 7×7
Scaling	The scaling ratios: 0.3, 0.5, 0.75, 1.5, 3
Smoothing	None

this time, the entire image is logical in content; only by using the trained network to identify, the secret information can be extracted. In the entire system, the established image library is known and completely confidential for both the sender and receiver. Furthermore, the neural network can also be retrained to update the image library. It is stipulated in the paper that the image set is composed in a certain order. If the secret information is too long, the extraction of multiple carriers is also based on a certain order. The specific steps for extracting secret information are as follows:

Step 1: receive image X and calculate the image watermark to judge whether it is replaced. If the watermark is replaced, no extraction is performed.

Step 2: preprocess the image, and cut the text icons part of the information hiding according to the template.

Step 3: use the Alex-Net to classify the text icons and obtain the secret information T.

Step 4: read the POS information and length L of the front bit of the T sequence in proper order.

Step 5: obtain secret information S.

5. Experimental Results and Analysis

The experiments are done by a personal computer with a configuration: Windows 10 Single GPU: NIVID GTX1050 and MATLAB 2018a. The experimental results and analysis include the following four parts. Considering that robustness is the most important influencing factor, besides the experimental comparison with the literature [41, 42], we also discussed the impact of different carrier-free methods on robustness in Section 5.1. It is noted that the datasets used in literature [41, 42] are unknown, so it could not reproduce the experiment and use the original author's results.

5.1. Analysis of Robustness. In the process of transmission, the images are damaged by various attacks inevitably, such as JPEG compression and filtering attack. How to resist these attacks, in other words, how to improve the robustness, is the key to steganography. In this paper, we used the same attack methods to conduct robustness experiments comparison with literature [41, 42]. The image attacks are shown in Tables 2 and 3.

Robustness is also an important performance index for image information hiding, and it represents the capability of resisting image attacks. The robustness measurement index can be expressed by the bit error rate BER, which refers to the bit error rate of the secret information extracted by the stego images through the algorithm under the third-party attacks. The BER calculation formula is defined as follows:

$$\mathrm{BER} = \frac{\mathrm{Bc}}{\mathrm{Bt}}, \tag{1}$$

where Bc is the number of error bits in the information obtained by the receiver through decoding and Bt is the total number of bits in the information sent by the sender.

In the robustness comparison experiment, each time a 100-bit information stream will be generated randomly. According to the classification method of the Alex-Net network training set, each icon corresponds to a 10-bit binary sequence. The test is performed 10 times under each parameter, and then the average value can be calculated. The structured coverless steganography in this paper is based on Alex-Net recognition. Therefore, the robustness of the algorithm is directly determined by the accuracy of network classification detection. Under different attack indexes, the BER of the structured coverless steganography algorithm in this paper is shown in the following tables.

5.1.1. Robustness Comparison. In order to fully prove the robustness of our method, a large number of experiments are

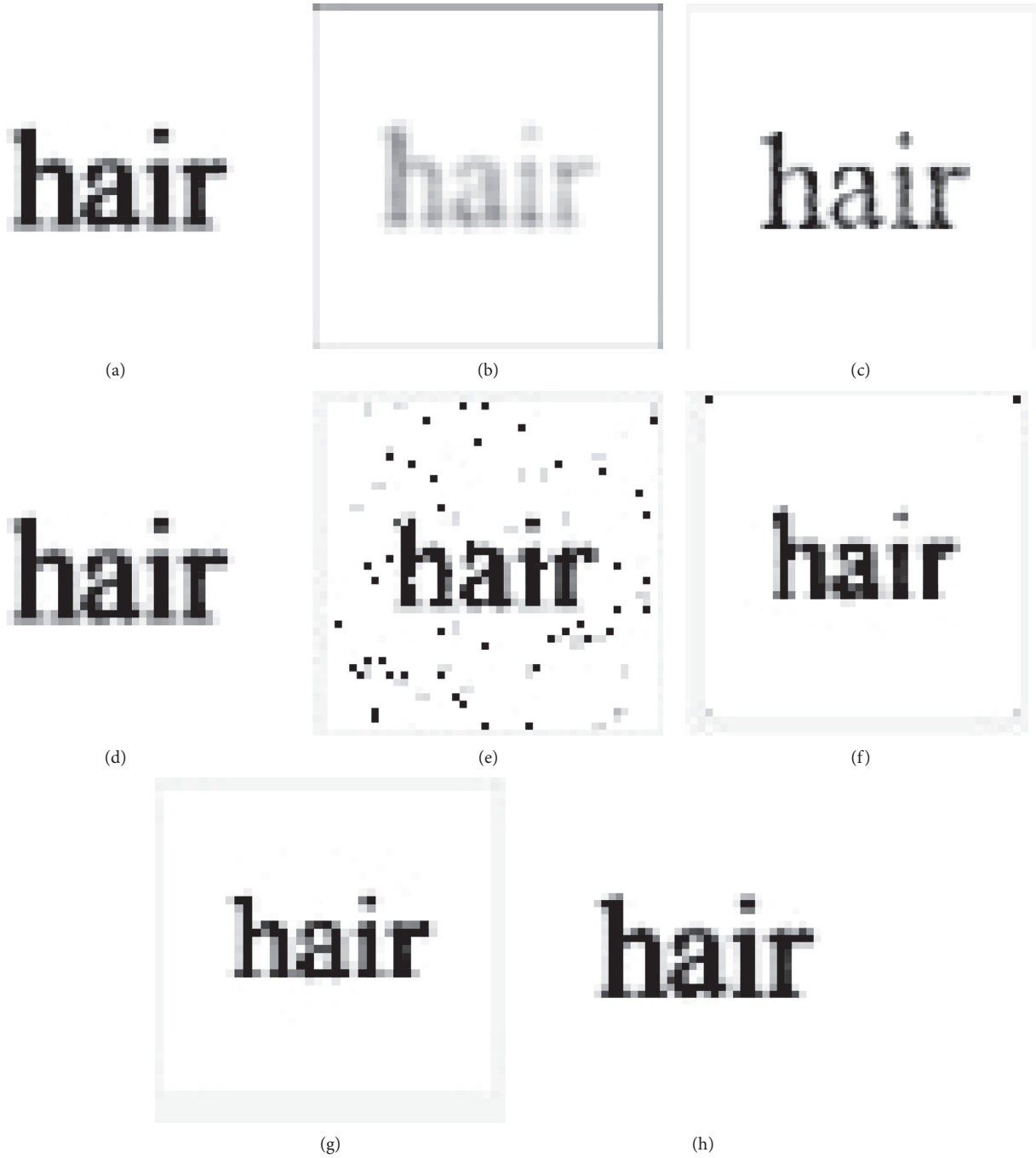

Figure 4: Adversarial samples diagram. (a) Original icon. (b) Mean filtering. The window size is 3×3. (c) Gauss noise. The mean μ is 0, and the variance σ is 0.5. (d) Image smoothing. (e) Salt and pepper noise. The mean μ is 0, and the variance σ is 0.05. (f) Median filtering. The window size is 3×3. (g) Scaling. The scaling ratio is 0.75. (h) JPEG compression. The quality factors Q: 70%.

conducted in this paper to compare with the CSD (chaotic sequences and image DCT algorithm) [41] and CBZS (chaos based zero-steganography) [42] algorithm. It is worth noting that some algorithm names in Tables 2 and 3 are abbreviated for ease of display.

The image attacks we used in the experiment are shown in Table 1 in Section 3.3. In terms of specific attacks, the robustness of most attacks in this paper is significantly better than the other two algorithms. Especially in compression, filtering, and noise attacks, the proposed method is much higher than the two other algorithms, which further proves that the proposed method is scalable and extensive.

The bit error rates under noise attacks used in the experiment are shown in Figures 6 and 7.

Noise attack is one of the critical parts of robustness testing. The typical noise during the image processing includes salt and pepper noise and additive white Gaussian noise. In the experiment, the parameters were set as follows:

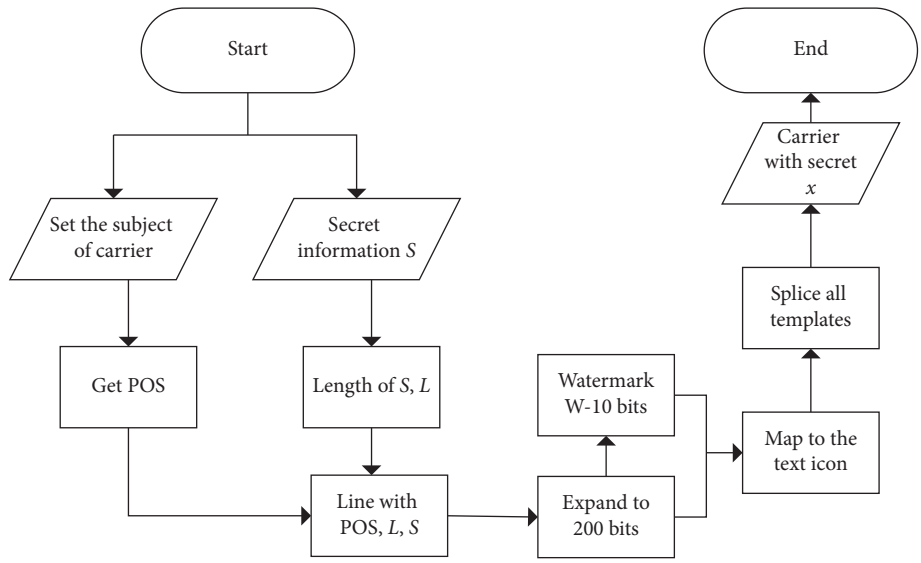

Figure 5: The flow chart of splicing image through coverless steganography algorithm.

Table 2: Comparison of ability to resist the JPEG compression attack among the CSD, CBZS, and the proposed algorithm (BER).

Compression quality	CBZS	CSD	Proposed algorithm
90	0.048	0.002	0
70	0.08	0.009	0
50	0.098	0.017	0

Table 3: Comparison of the ability to resist the mean filter attack among the CBZS, CSD, and the proposed algorithm (BER).

Size	CBZS	CSD	Proposed algorithm
3×3	0.0020	0.02	0.017
5×5	0.0034	0.035	0.032
7×7	0.0080	0.051	0.049

the mean μ of selected Gaussian white noise is 0, the normalized variance σ^2 varies from 0 to 1 with a step of 0.1. The salt and pepper noise intensity I ranges from 0.1 to 1.0 with an increment of 0.1.

The experimental results show that the robustness of our method is significantly better. When the Gaussian noise variance $\sigma^2 < 0.6$ or the salt and pepper noise intensity $D < 0.5$, the bit error rate under the algorithm is always 0. Once the noise intensity exceeds the threshold, the bit error rate will be suddenly increased to a higher level. However, in practical applications, it is impossible for the noise intensity to reach such a high level; the image at this time is completely meaningless. Therefore, the structured coverless steganography algorithm designed in this paper has powerful robustness.

Comparison of the ability to resist the JPEG compression attack among the CSD, CBZS, and the proposed algorithm is shown in Table 2. JPEG compression is a commonly used image compression method. Its compression principle is that, in the transform domain of the image, the high-frequency part of the image is filtered out to achieve

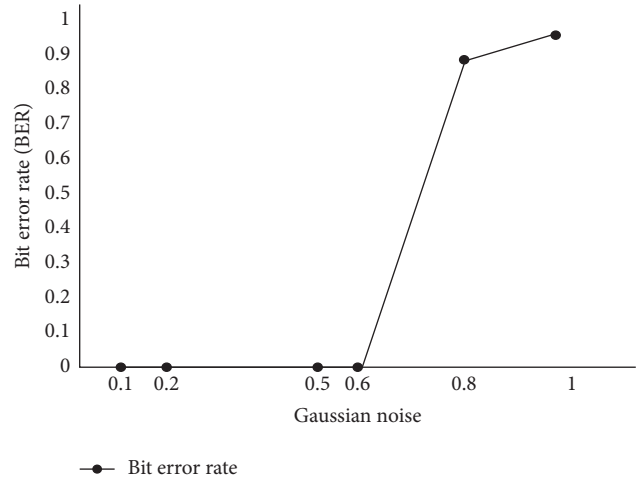

Figure 6: BER comparison under Gaussian noise attack.

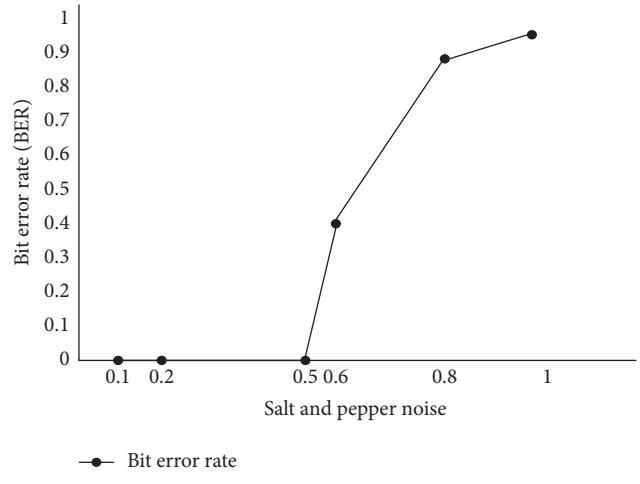

Figure 7: BER comparison under salt and pepper noise attack.

compression. In the experiment, the parameters were set as the quality factors Q: 50%, 70%, and 90%. When the compression quality of the algorithm is changed with an increment of 10, with the reduction of the compression quality value, the degree of compression can be increased. When the compression quality value is 90, the image is closest to the original image.

The experimental results show that the robustness of our method is significantly better than the two other algorithms. It is found that when the compression quality is changed, the bit error rate of the algorithm in this paper is always 0, which is not disturbed by the compression attack. The above analysis shows that our method is more robust than the other two methods and featured with clear advantages.

Comparison of the ability to resist the mean filter attack among the CBZS, CSD, and the proposed algorithm is shown in Table 3. Image filtering is to suppress the image noise while ensuring the image details as much as possible. According to the classification of noise, it is also divided into the time domain and frequency domain for processing. In this paper, the mean filter in the time domain was selected for testing. In the experiment, the parameters were set as follows: the convolution sizes are $3 \times 3, 5 \times 5, 7 \times 7$.

The experimental results show that the bit error rate under the mean filter attack is higher. Although our method gets the lower performance the same as literature [41, 42] under the mean filter attack, our approach has shown some advantages in other cases.

5.1.2. The Effect of Different Carrier-Free Methods on Robustness. We compared the robustness of the method proposed in this paper with different carrier-free methods. It is worth noting that the experimental method refers to literature [44]. The experimental results of the method in this paper are mainly compared with Pixel [45], SIFT + Hash [46], SIFT + BOF [47], and DCT + LDA [48]. The results are presented in Table 4. According to the results in the following table, our method has obvious advantages over the performance of other methods against noise attacks. Among the four traditional methods, Pixel and DCT + LDA perform better, while the other two models using the Hash algorithm perform poorly, with an error rate of over 80%. This is an inevitable result of using the Hash function: as long as the input image is slightly altered with a little noise, the output depending on the Hash algorithm will change so much that the original message cannot be properly decoded. In the comparison of experimental results, it can be seen that, under JPEG compression, Gaussian noise, salt and pepper noise, and other attacks, the method proposed in this paper can reach the optimal level, and even the decoding error rate is 0 under JPEG attack. The present method still has a good performance in some attacks while the traditional method has a poor performance. Finally, the method in this paper has the lowest error rate. It is shown that the proposed method is superior to the other traditional information hiding methods in terms of robustness.

$$C = \frac{B}{D} \times 100\% \quad (2)$$

5.2. Security Analysis. The algorithm proposed in this paper provides multiple protection for secret information.

5.2.1. The Privacy of Steganography. For the ways to hide information, instead of modifying the content or structure of the image, we transmit the fun images that have nothing to do with the secret information. In short, our method embeds the secret information into the stego image without any modification. Therefore, our method can fundamentally resist the existing steganalysis tools.

5.2.2. The Privacy of Images. In our paper, using the preset template, some small icons and a hot news image are spliced into secret carrier images according to the construction principle, which is fully reasonable and interesting in content, in line with people's sharing and communication habits on social platforms. In addition, by setting the invisible watermark, the error codes caused by the malicious replacement of text icons can be prevented, which will make the entire algorithm more secure. The relevant experimental results can be seen in Section 5.1. It can be seen as a major scheme to improve steganography safety.

To sum up, even if the image is spread on social platforms, the algorithm proposed in this paper also has high security.

5.3. Analysis of Capacity. For the coverless steganography algorithm, the hiding capacity of a single image is determined by the size of the image library. For example, to represent an 8-bit binary number, 2^8 images should be included in the constructed image library. The size of stego for the structured coverless steganography proposed in this paper is 512×512, including 21 60×60 text icons. Each image can be hidden up to 180-bit binary sequence except for part of the image theme and zone bits, instead of the image library of 2^{180} images, whose length can already be used for key transmission with a higher security level. Moreover, the construction strategy of this paper only needs to change the image theme. It can be transmitted in the form of a set of pictures: the single transmission capacity of 10 structured images is 10×180 bits, about 120 Chinese characters, whose capacity can be used for actual covert communication. It can be represented by the data embedding rate.where C is the data embedding rate, B is the length of the hidden information, and D is the size of the cover image.

According to the analysis of the test results, it is found that after the carrier is compressed by JPEG, the reduction in image quality has no effect on the recognition of the text icons. Therefore, the image can be compressed on the premise of ensuring the image content. In this paper, the embedding rate and the single maximum capacity are greatly improved, compared with other coverless algorithms [15, 16, 43]. In addition to our method, we also selected Pixel, SIFT_Hash, DCT_LDA, and SIFT_BOF, and so forth. The capacity data is shown in Table 5. Compared with several

Table 4: Robustness comparison of different carrier-free methods (error rate) (%).

Attack	SIFT_Hash	SIFG + BOW + HASH	Pixel	DCT + LDA	Our method
JPEG compression (10)	84.77	99.61	0.78	1.17	0.00
JPEG compression (30)	84.77	99.61	0.78	1.17	0.00
JPEG compression (50)	84.77	99.61	0.78	1.17	0.00
JPEG compression (70)	84.77	99.61	0.78	1.17	0.00
JPEG compression (90)	84.77	99.61	0.78	1.17	0.00
Mean filter (3×3)	99.61	100.00	0.00	0.00	0.017
Mean filter (5×5)	99.22	100.00	0.00	0.00	0.032
Mean filter (7×7)	99.61	100.00	0.00	1.17	0.049
Gauss noise (0.001)	73.83	99.61	0.00	0.78	0.00
Gauss noise (0.005)	73.83	99.61	0.00	0.78	0.00
Gauss noise (0.1)	73.83	99.22	0.00	0.78	0.00
Original	0.00	0.00	0.00	0.00	0.00
Salt and pepper (0.001)	83.59	100.00	0.39	0.78	0.00
Salt and pepper (0.005)	95.70	99.61	0.39	1.17	0.00
Salt and pepper (0.1)	100.00	99.61	4.30	7.03	0.00

coverless steganography methods proposed in recent years, it can be seen from the table that our method has a higher relative capacity and can deliver more information with fewer pixels.

5.4. PSNR and SSIM Measures. The results of the peak signal-to-noise ratio and the structural similarity index measure are good to show the imperceptibility of the presented method, used to compare differences between the original images and the changed form of them. In this section, the performance of our proposed method is compared with schemes like [49], [50], and [51].

PSNR is calculated by the following equation:

$$10\,\mathrm{PSNR} = \log_{10}\left(\frac{\mathrm{MAX}_1^2}{\mathrm{MSE}}\right), \tag{3}$$

where MAX_1 is the value of the possible pixel in the cover images. MSE is the mean square error and it is defined by

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - \mathrm{St}(i,j)]^2, \tag{4}$$

where C and St are cover image and stego image, respectively. m and n are the sizes of the cover image.

Table 6 depicts the comparison of SSIM and PSNR values between our scheme and other schemes. Although the PSNR value of our method is not the best among the four methods, it can still show good invisibility. In addition, we use coverless steganography in this paper, which does not modify the original carrier. Therefore, the stego image generated in this paper has not changed compared with the original carrier image. So, the structural similarity index at this time is 1, which can well show the imperceptibility to the readers.

Table 7 depicts BER and PSNR values of the secret extracted from the attacked stego. For Gaussian noise, noise with a mean of 0 and variance of 0.01 is added to the stego images. The results of the table show that the proposed method has good performance in the imperceptibility.

Table 5: Comparison of capacity with other algorithms.

Algorithm	Cover size	Embedding rate
Pixel	512×512	3.82×10^{-5}
SIFT_Hash	512×512	6.86×10^{-5}
DCT_LDA	512×512	5.7×10^{-5}
SIFT_BOF	512×512	3.82×10^{-5}
Ours	512×512	1.1×10^{-3}

Table 6: Comparison of the proposed method with other schemes.

Scheme	PSNR (dB)	SSIM
Literature [49]	53.25	0.9851
Literature [50]	51.37	0.9984
Literature [51]	69.59	0.9999
Ours	61.50	1.0

Table 7: BER and PSNR values of the secret extracted from the attacked stego.

Scheme	BER	PSNR (dB)
Literature [49]	0.0334	21.359
Literature [50]	0.0364	20.037
Literature [51]	0.0233	28.761
Ours	0.0151	29.527

6. Conclusion

This paper presents a method of coverless image steganography based on the image and text semantic. The essence of the method is that the text icons can be used to express the hiding information and the Alex-Net network is used to establish the one-to-one mapping relationship between the icons and the secret sequences. The adversarial training samples are used to improve the recognition of the neural network, thereby improving the robustness of the algorithm. In addition, the rules of structured cover are rationally designed in this paper. On the whole, the payload and the robustness performance can be effectively improved. At the same time, some experiments have been designed to

test the algorithm performance in MATLAB 2018a environment. Experimental and theoretical results show that the proposed algorithm in this paper not only has more powerful robustness against common image attacks but also improves the hiding capacity. Meanwhile, it can resist steganography analysis and demonstrate higher security.

In the hidden strategy proposed in this paper, the selection of preset templates and the construction of semantic association methods are not automatically extracted from social platforms. In future work, the method of data mining method can be adopted, which can automatically excavate the social behavior habits of users on the Internet from social platforms. Then, theme images and association rules can be automatically generated. Furthermore, while deep learning is combined with image semantics, the algorithm design can be improved, and the hidden capacity of a single image will be further increased.

Data Availability

The software code and data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. U1736121) and Wuhan Maritime Communication Research Institute (Grant no. KCJJ2019-2).

References

[1] X. Chen, H. Sun, Y. Tobe et al., "Coverless information hiding method based on the Chinese mathematical expression," *International Conference on Cloud Computing and Security*, pp. 133–143, Springer, Berlin, Germany, 2015.

[2] 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, Article ID 105375, 2020.

[3] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, and A. K. Sangaiah, "New cubic reference table based image steganography," *Multimedia Tools and Applications*, vol. 77, no. 8, pp. 10033–10050, 2018.

[4] Z. Zhou, H. Sun, R. Harit et al., "Coverless image steganography without embedding," in *International Conference on Cloud Computing and Security*, pp. 123–132, Springer International Publishing, Cham, Switzerland, 2015.

[5] X. Chen, S. Chen, and Y. Wu, "Coverless information hiding method based on the Chinese character encoding," *Journal of Internet Technology*, vol. 18, no. 2, pp. 313–320, 2017.

[6] Y. Cao, Z. Zhou, C. Yang et al., "Dynamic content selection framework applied to coverless information hiding," *Journal of Internet Technology*, vol. 19, pp. 1179–1186, 2018b.

[7] Z. Qian, L. Pan, S. Li et al., "Steganography by constructing marbling texture," *International Conference on Cloud Computing and Security*, pp. 428–439, Springer, Cham, Switzerland, 2018.

[8] Information Technology—Information and Data Security, "Researchers at Hunan University of Finance & Economics have reported new data on information and data security (coverless image steganography: a survey)," *Computers, Networks & Communications*, 2020.

[9] S. Sun and Q. Miao, "Research on semi-structured text information extraction algorithm based on improved HMM," *Electronic Science and Technology*, vol. 27, no. 10, pp. 111–114+118, 2014.

[10] H. Song, *Coverless Information Hiding Based on Generative Model*, Henan Normal University, Xinxiang, China, 2018.

[11] Y. Liu, Y. Pan, R. Xia, D. Liu, and J. Yin, "FP-CNNH: a fast image hashing algorithm based on deep convolutional neural network," *Computer Science*, vol. 43, no. 9, pp. 39–46+51, 2016.

[12] S. Zheng, L. Wang, B. Ling et al., "Coverless information hiding based on robust image hashing," *International Conference on Intelligent Computing*, pp. 536–547, Springer, Cham, Switzerland, 2017.

[13] Z. Wang, *Research on Coverless Information Hiding Algorithm*, Xidian University, Xi'an, China, 2019.

[14] Y. Cao, Z. Zhou, Y. Zhou et al., "Information hiding based on cartoon images," in *Proceedings of the China Information Hiding Workshop*, Jilin, China, July 2019.

[15] J. Wu, Y. Jia, and Y. Liu, "Coverless information hiding algorithm based on image coding and stitching," in *Proceedings of the 14th China Information Hiding Workshop*, Guangzhou, China, March 2018.

[16] J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, and Y. Jia, "A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix," *IETE Technical Review*, vol. 35, pp. 1–11, 2018.

[17] Z. Zhou, M. J. Wu, and X. Sun, "Encoding multiple contextual clues for partial-duplicate image retrieval," *Pattern Recognition Letters*, vol. 109, pp. 18–26, 2018.

[18] L. Zou, J. Sun, M. Gao et al., "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools and Applications*, vol. 78, no. 7, 2019.

[19] Z. Qian, N. Huang, S. Li, and X. Zheng, "Constructive steganography using texture synthesis," *IETE Technical Review*, vol. 35, no. sup1, 2018.

[20] L. Zhao and H. Li, "Research on modified information hiding technology based on carrier," *Science and Technology Information*, vol. 15, no. 24, pp. 4–6, 2017.

[21] X. Zhang, *Behavior Steganography in Social Network*, Springer International Publishing, Cham, Switzerland, 2017.

[22] X. Chen and S. Chen, "Text coverless information hiding based on compound and selection of words," *Soft Computing*, vol. 23, no. 15, 2019.

[23] Z. Zhou, Y. Mu, N. Zhao, Q. M. Jonathan Wu, and C.-N. Yang, "Coverless information hiding method based on multi-keywords," *Cloud Computing and Security*, Springer International Publishing, Cham, Switzerland, 2016.

[24] J. Wu, Z. Kang, Y. Liu et al., "A coverless information hiding method based on image classification," *Journal of Hunan University (Natural Science Edition)*, vol. 46, no. 12, pp. 25–32, 2019.

[25] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, vol. 60, pp. 1097–1105, 2012.

[26] D. Zhou, "Animal picture classification based on AlexNet network," *Journal of Guizhou University (Natural Science Edition)*, vol. 36, no. 6, pp. 73–77, 2019.

[27] J. Cao, H. Cui, and Q. Zhang, "Classification of ancient murals based on feature fusion with AlexNet model," *Journal of Image and Graphics of China*, vol. 25, no. 1, pp. 92–101, 2020.

[28] X. Xu, "A new deep learning model based on improved AlexNet for radiation source target recognition," *International Association of Applied Science and Engineering*, vol. 5, pp. 7–11, 2018.

[29] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *International Conference on Learning Representations*, https://arxiv.org/abs/1409.1556, 2015.

[30] C. Szegedy, W. Liu, Y. Jia et al., "Going deeper with convolution," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1–9, Boston, MA, USA, 2015.

[31] K. He, X. Zhang, S. Ren et al., "Deep residual learning for image recognition," pp. 770–778, 2016, https://arxiv.org/abs/1512.03385.

[32] G. Wang and C. Niu, "Stochastic gradient descent algorithm based on convolution neural network," *Computer Engineering and Design*, vol. 39, no. 2, pp. 442–462, 2018.

[33] M. Zhong, J. LeBien, and M. Aide, "Multispecies bioacoustic classification using transfer learning of deep convolutional neural networks with pseudo-labeling," *Applied Acoustics*, vol. 166, Article ID 107375, 2020.

[34] W. Li, L. Duan, D. Xu, and I. W. Tsang, "Learning with augmented features for supervised and semi-supervised heterogeneous domain adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, pp. 1134–1148, 2014.

[35] J. Nam, W. Fu, S. Kim et al., "Heterogeneous defect prediction," *IEEE Transactions on Software Engineering*, vol. 44, no. 9, pp. 874–896, 2017.

[36] J. Zhou, S. Pan, I. Tsang et al., *Hybrid Heterogeneous Transfer Learning through Deep Learning*, AAAI Press, New Orleans, LA, USA, 2014.

[37] H. Aujla, M. J. C. Crump, M. T. Cook, and R. K. Jamieson, "The Semantic Librarian: a search engine built from vector-space models of semantics," *Behavior Research Methods*, vol. 51, no. 6, 2019.

[38] Y. Liu and Song, *Information Carrier's Text Information Hiding Technology*, Nanjing University of Aeronautics and Astronautics, Jiangsu, China, 2017.

[39] S. Ma, X. Zhao, and Y. Liu, "Adaptive spatial steganography based on adversarial examples," *Multimedia Tools and Applications*, vol. 78, no. 22, 2019.

[40] X. Song, X. Wu, S. Gao et al., "Simulation Study on Handwritten numeral recognition based on deep neural network," *Science Technology and Engineering*, vol. 19, no. 5, pp. 193–196, 2019.

[41] M. Bilal, S. Imtiaz, W. Abdul, S. Ghouzali, and S. Asif, "Chaos based zero-steganography algorithm," *Multimedia Tools and Applications*, vol. 72, no. 2, pp. 1073–1092, 2014.

[42] J. Wu, X. Fei, and N. Wang, "Zero-steganography algorithm research based on chaotic sequences and image DCT transform," *Electronic Measurement Technology*, vol. 40, no. 5, pp. 174–179, 2017.

[43] Y. Wang and B. Wu, "A coding scheme base on deep learning in coverless information hiding," in *Proceedings of the China Information Hiding Workshop*, Jilin, China, July 2019.

[44] Y. Wang and B. Wu, "An intelligent mapping relation search method for information hiding without carrier," *Chinese Journal of Information Security*, vol. 5, no. 3, pp. 48–61, 2020.

[45] Z. Zhou, H. Sun, R. Harit et al., "Coverless image steganography without embedding," *Cloud Computing and Security*, pp. 123–132, Springer International Publishing, Cham, Switzerland, 2015.

[46] Y. Cao, Z. Zhou, X. Sun et al., "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[47] Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Computing*, vol. 23, no. 13, pp. 4927–4938, 2019.

[48] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223–3238, 2018.

[49] A. Sukumar and V. Subramaniyaswamy, "A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage," *Multimedia Tools and Applications*, vol. 79, pp. 10825–10849, 2020.

[50] M. Valandar and M. Barani, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools and Applications*, vol. 78, pp. 9971–9989, 2019.

[51] M. Subhedar and V. Mankar, "Secure image steganography using framelet transform and bidiagonal SVD," *Multimedia Tools and Applications*, vol. 79, pp. 1865–1886, 2020.