EURASIP Journal on Image
and Video Processing

RESEARCH Open Access

Coverless information hiding based on the generation of anime characters

Yi Cao[1], Zhili Zhou[1*], Q. M. Jonathan Wu[2], Chengsheng Yuan[1] and Xingming Sun[1*]

* Correspondence: zhou_zhili@163.com; sunnudt@163.com
[1]Jiangsu Engineering Center of Network Monitoring, Engineering Research Center of Digital Forensics, Ministry of Education, School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China
Full list of author information is available at the end of the article

Abstract

To fundamentally resist the steganalysis, coverless information hiding has been proposed, and it has become a research hotspot in the field of covert communication. However, the current methods not only require a huge image database, but also have a very low hidden capacity, making it difficult to apply practically. In order to solve the above problems, we propose a coverless information hiding method based on the generation of anime characters, which first converts the secret information into an attribute label set of the anime characters, and then uses the label set as a driver to directly generate anime characters by using the generative adversarial networks (GANs). The experimental results show that compared with the current methods, the hidden capacity of the proposed method is improved by nearly 60 times, and it also has good performance in image quality and robustness.

Keywords: Coverless information hiding, Image generation, Attribute label, Hiding capacity

1 Introduction

Traditional information hiding methods mainly take advantage of the redundancy of carrier and modify it according to agreed rules to embed secret information into the carrier in an invisible way [1–5]. However, as long as the carrier is modified, the modification traces will be left, and it is possible for steganalysis algorithms to detect the existence of hidden behavior successfully. In order to make the information hiding methods fundamentally resistant to steganalysis [6], scholars in the field of information hiding have proposed the concept of coverless information hiding (CIH) [7]. Compared with the traditional methods, CIH methods directly generate or retrieve the stego-carriers based on the secret information without modification.

The existing CIH methods include image selection methods, semi-creative methods based on texture synthesis, and creative methods based on generative adversarial networks (GANs) [8]. Image selection methods need to establish a large-scale natural image database in advance, and then retrieve the natural images that can express secret information as stego-images. Although the image selection methods directly transmit secret information with natural images, which can fundamentally resist the detection

Springer Open

of various steganalysis algorithms, their hiding capacity is very limited. Semi-creative methods based on image sample synthesis do not need to establish a natural image database in advance. They can synthesize an arbitrary size stego-image according to agreed rules, so that it has a large hidden capacity. However, because there are quilting between the samples, there is also the possibility of detection. Moreover, in this case, the stego-image has no actual semantics, which is easy to arouse the suspicion of attackers and has low practicability. Although there are some creative methods based on GANs for CIH, most of them are used to hide numbers and specific images, which cannot be applied to conceal any untrained secret information.

In order to generate a stego-image that can express arbitrary secret information, this paper proposes a CIH method based on the generation of anime characters. With the development of deep learning methods [9–11], especially GANs, the automatic generation of anime characters has achieved good results. Not only can they maintain the consistency of statistical characteristics with the training image set, but they also achieve the degree of visual effect that the fake can be confused with the real. Figure 1 is an example of anime characters generated automatically by GANs [12]. Besides, with the development of GANs, there are many codes and web pages on the Internet that can generate anime images. This makes it easy for everyone to generate anime images. Therefore, when sharing a stego-image, we can directly indicate that it is the generated anime image. For example, we shared some stego-images in Wechat Moments, with the following text, “I have created anime images myself, so happy!” In this case, compared with computer-generated natural images, anime character images are more resistant to the computer and visual detection [13].

This paper directly generates an anime character that can express secret information. First, it converts secret information into a collection of attribute labels for anime characters, such as hairstyle, hair color, eye color, etc. Then, with the set of attribute labels as the constraint condition, use a generative network of anime characters based on GANs [12] to generate the image set that conforms to the constraint condition. After

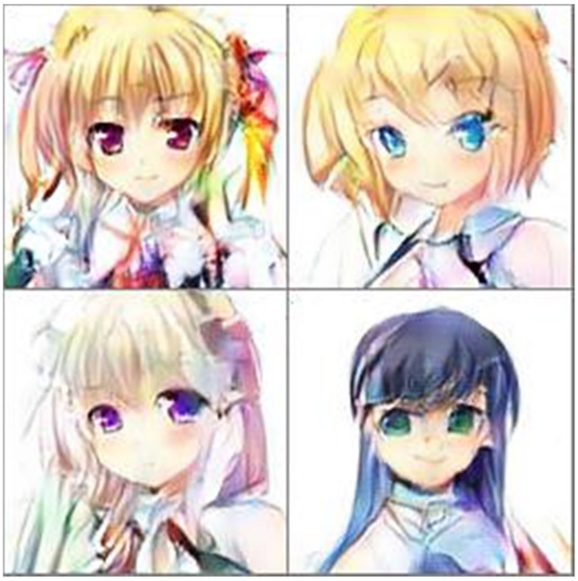


Fig. 1 An example of anime characters generated automatically by GANs

that, the quality of the generated image is evaluated, and the anime characters with good quality are selected as the stego-images. Finally, the receiver extracts the attribute labels expressing secret information according to the corresponding method, and then obtains the secret information. Compared with the existing methods, this paper proposes an idea of generating specific anime characters based on secret information to realize CIH. Its main contributions can be summarized as the following three points:

(1) This paper uses the attributes of anime characters to represent secret information. Compared with image selection methods, it can significantly improve the hiding capacity and has high practical application value. For example, the hiding capacity of this method is about 60 times that of the method in the literature [14].
(2) In this paper, according to the attributes of anime characters, the GAN is adopted to generate stego-images directly. Its statistical characteristics are consistent with the training set and without any modification. Compared with the semi-creative CIH methods based on texture synthesis, it has higher security.
(3) There is no necessary connection between the secret information and the anime character generation network. Compared with the existing GAN-based methods of CIH, the proposed method can transmit arbitrary secret information.

2 Relative works

2.1 Image selection methods

Image selection methods rely on image retrieval [15]. Fridrich et al. [16] first proposed the idea of information hiding based on carrier selection, which, according to agreed rules, retrieves specific natural images from the pre-established image database to express secret information. Subsequently, literature [7, 17] proposed a CIH method to transmit secret information by image hash sequence. After that, to improve the hiding capacity, literature [18–22] selected different features and secret information to establish a mapping to realize CIH. Literature [23] first used gray gradient co-occurrence matrix to encode the image, and then used the mapping relationship between image and a random number to represent the payload information. Literature [24] uses a set of sub-image blocks at specific locations of natural images to splice them into secret images that need to be transmitted, so as to achieve approximate transmission of secret images. Literature [25] proposed a dynamic content selection framework applied to CIH, which dynamically selects natural images to represent and transmit secret messages according to certain mapping rules constructed between secret messages and user identity. In [14], discrete cosine transformation (DCT) coefficients are used to represent secret information. All the above CIH methods employed the low-level features to represent secret information. Although they can effectively resist the steganalysis, they suffer from the robustness problem, and their hiding capacity is very low. Thus, it is hard to apply them in real-world scenarios.

2.2 Semi-creative methods based on texture synthesis

Semi-creative methods mean that the secret information can directly generate the stego-carrier according to agreed rules without specifying the original carrier in advance. And the stego-carrier generally belongs to a specific type, such as texture images. Usually, it is necessary to build a basic sample database in advance, then select the appropriate samples from the database according to secret information, and synthesize a relatively natural large stego-image according to agreed rules. Otori et al. [26] used LBP code to establish the mapping relationship between binary data and pixel points, and then find suitable texture samples from the database according to secret information to synthesize a stego-image. But the hiding capacity of this method is low and there is some error. To realize information hiding with large capacity and no error code, Wu et al. [27] used similarity ranking of different texture samples to express secret information. This method preserves all texture samples so that attackers can reconstruct the original samples and obtain secret information through quilting between texture samples. After that, to improve security and hide capacity, literature [28–32] proposed a series of improved algorithms.

2.3 Creative methods based on GANs

Liu [33, 34] et al. conducted experiments in the MNIST data set and used labels "1~9" to represent secret information, and then used these labels as constraints to generate simulated handwritten images. This method not only has lower hiding capacity, but also can clearly see the category label of secret information encoding and has lower security. Duan [35] et al. used an image with completely unrelated semantics to transmit secret images. Although this method has a large hiding capacity and has no relation between the secret image and the stego-image, it must retrain the model every time it communicates, and the model must be shared with the receiver to complete the communication task. In addition, the secret image and the stego-image are in the same generated image database, and there is a one-to-one relationship. Therefore, there are security risks. Liu et al. [36] proposed a CIH method based on image repair technology and Cardan Grille Mask (CGK). However, this method needs to share CGK in the communication process, which also has some security risks. Moreover, because secret information is written in the damaged part of the image, the image repair effect is not very good.

3 Proposed CIH method

The framework of the proposed CIH method is shown in Fig. 2, which mainly includes the sender and the receiver.

According to the main functions, it can be divided into the following three modules: secret information and label set conversion module (LSTM), location index module, and secret image generation module. In this paper, the attribute labels of anime characters are used to represent secret information. The sender first converts the secret information into the corresponding attribute labels, and then generates anime characters that can express secret information according to the attribute labels at a specific index position. After receiving the stego-image containing secret, the receiver first extracts the attribute labels of the anime characters at the index position and then converts it into secret information. Next, the specific implementation process of each module is introduced.

3.1 Convert secret information into labels set

As shown in Fig. 3, this paper uses the attribute labels of anime characters to represent secret information, so the transformation of secret information and labels set is crucial.

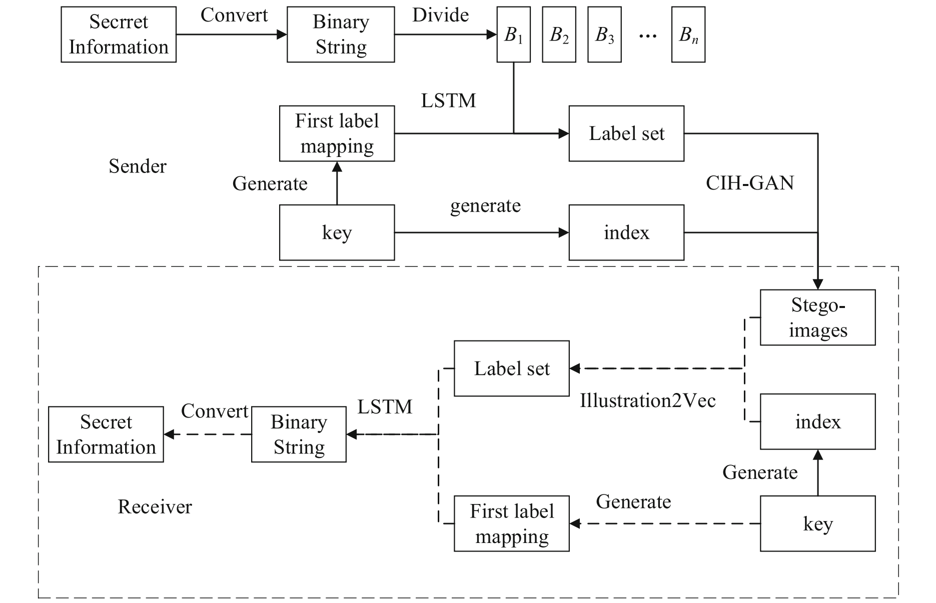


Fig. 2 The framework of the proposed method

This paper uses Illustration2Vec [37], a network used to predict the attribute labels of anime characters, to carry out label extraction. For a given image, Illustration2Vec can predict the probability of 512 attributes. In this paper, we mainly select the attributes with a high probability of occurrence, including 5 hairstyles, 13 hair colors, 10 eye colors, and several other attributes such as “blush,” “smile,” “open mouth,” and “ribbon.” In this paper, long short-term memory network (LSTM) [38] is used to convert secret information and labels set. In the field of natural semantic processing, LSTM can generate high-quality text content, which can predict the probability of the next output content in the case of existing partial input. This paper mainly uses this function of LSTM to transform secret information and image attribute labels.

The labels set format described in this paper for each anime characters can be expressed as {hairstyle (2 bit), hair color (3 bit), eye color (3 bit), other attributes 1 (2 bit), other attributes 2 (2 bit), ..., other attributes n (2bit)}. The payload of each attribute depends on the number of labels for the attribute. That is, if an attribute represents *m*-

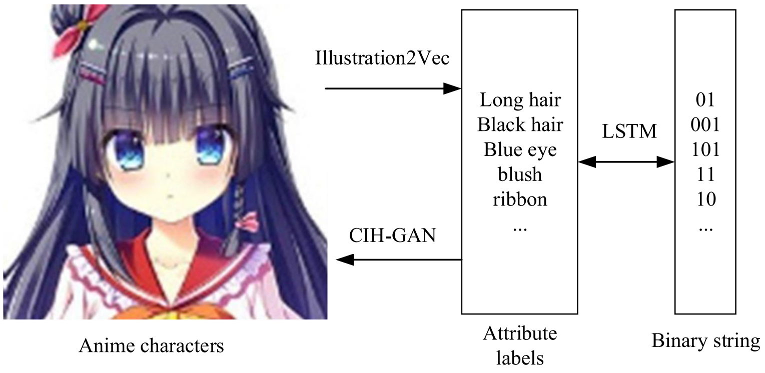


Fig. 3 Secret information representation

bit binary information, the labels of the attribute is at least 2^m kinds. In addition, the label format is not static, and the communication parties can modify it by themselves.

Before the transformation, this paper optimizes and trains the LSTM network. First, from Getchu (www.getchu.com), a lot of anime characters were crawled. Then, the image was preprocessed, and about 27,000 high-quality anime characters were taken as the original data set. The LSTM model is then trained with the obtained label document to obtain the label set generation model.

As shown in Fig. 4, the specific process of converting secret information into attribute tags is described as follows:

Step 1: Convert the secret information into a binary string, then divide it according to the label format to obtain the secret information set $S = \{s_1, s_2, s_3, \ldots, s_t\}$;
Step 2: Generate the first attribute mapping through a pseudo-random transformation function $M = f_M(\text{Key})$ according to the Key shared by both parties, that is, the mapping M of hairstyle and 2 bit binary information, and obtain the first label $l_1$in the label set through query M;
Step 3: Take the first attribute label l_1 as input and predict the next label through the LSTM network. In this paper, we select the corresponding attribute labels based on the secret message fragment. Taking l_2 as an example, its corresponding attribute for the hair color represents 3-bit secret information. The probability of the next attribute generated by LSTM with l_1 as input can be expressed as $p(l_2| l_1)$, because l_2 need to represent 3-bit secret information, so the first eight of the probability rankings are selected as candidate sets, then select the label based on the secret message s_2;
Step 4: Similarly, the probability of the predicted nth attribute can be expressed as $p(l_n| l_1, l_2, \ldots, l_{n-1})$. Then, select the attribute labels based on the secret information.

Step 5: Repeat Step 4 until the combination of attributes representing an anime characters is completed, and skip to Step 1 to continue to generate the set of attributes describing the next anime characters. Finally, get the label collection. $L = \{l_1, l_2, l_3, \ldots, l_t\}$.

The process of converting attribute label collection $L = \{l_1, l_2, l_3, \ldots, l_t\}$ into secret information is shown below:

Step 1: According to the Key shared by both parties, generate the first attribute mapping through a pseudo-random transformation function $M = f_M(\text{Key})$ and obtain the first secret information fragment s_1 through query M.

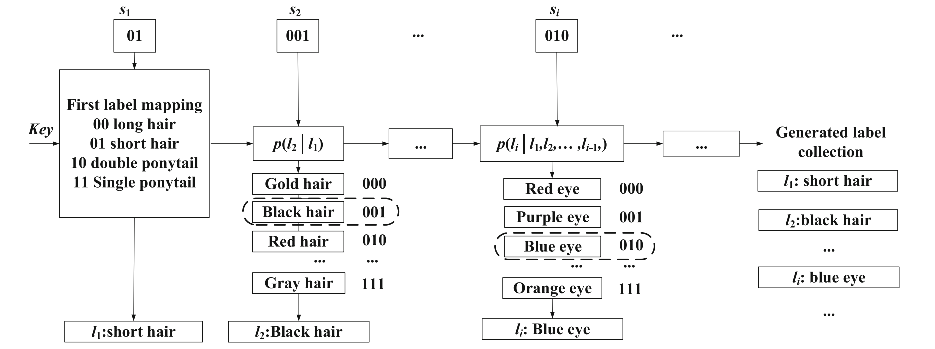


Fig. 4 LSTM conversion example

Step 2: Take the first attribute label l_1 as input, obtain the candidate set of label l_2 through LSTM network, and obtain the corresponding secret information fragment s_2 according to the actual l_2.

Step 3: Obtain the secret information set $S = \{s_1, s_2, s_3, \ldots, s_t\}$.

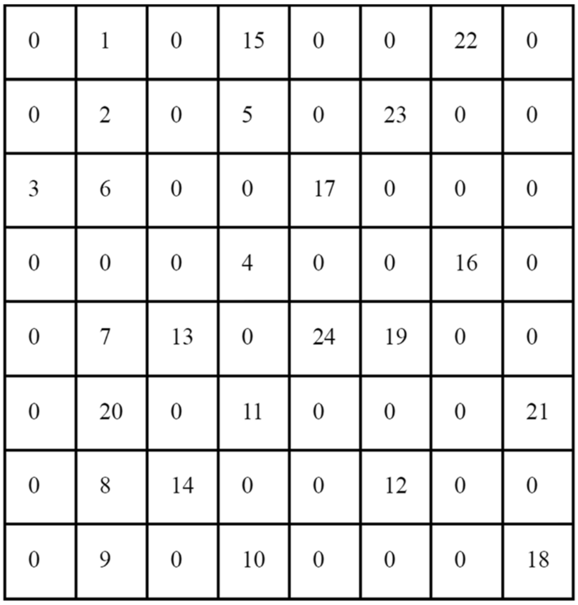
3.2 Position index

In this paper, $N \times N$ smaller anime characters are combined into a stego-image. That is, each row and column of the stego-image has an anime character, and the size of the stego-image can be adjusted according to actual needs. Considering the security of the algorithm, it is not that all the anime characters in the stego-images express secret information. We used the index shown in Fig. 5 to determine which locations of the anime characters expressed secret information.

Where 0 indicates that the anime character at this position does not transmit secret information, and other numbers indicate that the anime character at this position contains secret information. Generally speaking, the original position index of $N \times N$ image is denoted as $I_0 = \{i_1, i_2, \ldots, i_{N \times N}\}$. During the communication, both parties generate the index sequence $I = \{i'_1, i'_2, \ldots, i'_t\}, t \le N \times N$of the current communication according to pseudo-random transformation function$I = f_I(I_0, key)$. In Fig. 5, “1” represents the position of ″i'_1”, “2” represents the position of ″i'_2,” and so on. That is, the value indicates the extraction sequence of secret information. We first extract the secret information at position 1, then extract the information at position 2, and so on.

3.3 Generation of stego-images

As shown in Fig. 1, the current GAN-based anime character generation technology can automatically generate outstanding anime character according to the labels. Therefore, based on literature [12], this paper realizes the anime character generative network



0	1	0	15	0	0	22	0
0	2	0	5	0	23	0	0
3	6	0	0	17	0	0	0
0	0	0	4	0	0	16	0
0	7	13	0	24	19	0	0
0	20	0	11	0	0	0	21
0	8	14	0	0	12	0	0
0	9	0	10	0	0	0	18

Fig. 5 An example of an index

applied to the CIH, which is mainly constrained by the labels set corresponding to secret information and generates animation images representing secret information at the index position.

The purpose of CIH is to realize the hidden transmission of messages, so it is necessary to ensure that the receiver can extract the secret information accurately. In this paper, a post-verification module was added based on the network of literature [12] to evaluate and select the quality of the generated images, and the anime characters collected from Getchu were used for training. Its main function is to use Illustration2Vec to extract labels after the generation of anime character transmitting secret information. If the corresponding attribute labels cannot be extracted completely, the generated anime character should be optimized until the corresponding attribute labels can be extracted correctly. At the same time, the post-verification module will also evaluate the image quality, and select the anime character with good quality to transmit secret messages based on ensuring the correct extraction.

3.4 Information hiding

The steganography process is the generation process of anime characters, the specific process is shown below.

Step 1: Convert the secret information into a binary string, segment the secret information sequence $S = \{s_1, s_2, s_3, \ldots, s_t\}$ according to the label structure, and obtain the first attribute mapping M and location index $I = \{i'_1, i'_2, \ldots, i'_t\}$ according to the Key;
Step 2: Convert secret information sequence into anime character attribute label sequence $L = \{l_1, l_2, l_3, \ldots, l_t\}$ through the LSTM model;
Step 3: Use the stego-image generation network, generate the anime character expressing secret information at the index position of the stego-image, and randomly generate the anime character at other positions.
Step 4: Send the generated stego-image to the receiver in a pre-agreed way.

3.5 Information extraction

The extraction process is to extract attribute labels in anime character. The specific process is as follows:

Step 1: Obtain the first property mapping M and location index $I = \{i'_1, i'_2, \ldots, i'_t\}$ according to the *Key*;
Step 2: Use Illustration2Vec to extract the corresponding attribute label combination $L = \{l_1, l_2, l_3, \ldots, l_t\}$.
Step 3: Convert anime character attribute label sequence into secret information sequence $S = \{s_1, s_2, s_3, \ldots, s_t\}$ through the LSTM model;
Step 4: Convert the binary bit information into secret information.

4 Experimental results and discussion

The environment of our experiments is given as follows. System: Ubuntu 16.04 LTS, RAM: 48 GB DDR4, CPU: i5-8500 3.0 GHz, GPU: NVIDIA GTX 1080Ti; Software platform: python 3.6. The experiments are implemented based on the code of [4]. The experimental results and analysis focus on three aspects: image quality evaluation, hiding capacity, robustness, and security.

4.1 Image clarity evaluation

Image clarity is an essential index for evaluating image quality and has important significance in the field of image pattern recognition. This paper uses the attribute labels of anime character to represent secret information. In order to ensure that the receiver extracts the attribute labels correctly and avoids the suspicion of the attacker, the clarity of the generated stego-images must be consistent with the images in the training set. If the stego-image is blurry, it is difficult to ensure that the receiver can extract the attribute labels correctly. Therefore, the clarity of the stego-image is an important indicator for evaluating the proposed method. In order to visually show the difference in clarity between the generated image and the original image, while considering the influence of image edge information, noise, and energy on image clarity, we selected the following five image clarity indicators for comparison.

(a) Tenengrad gradient function [39]: it uses Sobel operator to extract the gradient values in the horizontal and vertical directions, and mainly evaluates the clarity through the edge information. The sharper the edges of the image, the clearer the image.
(b) Variance function [39]: it is more sensitive to noise. The purer the image, the smaller the function value.
(c) Vollath function [40]: it is similar to the variance function, but it is better when the noise is significant.
(d) Sum of Modulus of gray Difference (SMD) [41]: it uses the energy gradient function as the evaluation function of clarity. The more high-frequency components in the image, the clearer the image.
(e) Entropy function [41]: when the image energy is constant, the larger the image entropy, the clearer the image.

The results are shown in Table 1. According to the evaluation results, the clarity measurement value of the generated image is close to that of the original image, with little deviation. As shown in Fig. 6, Fig. 6a is the original image, and Fig. 6b is the generated image according to the attribute labels in Fig. 6a. Obviously, the original image and the generated image have the same set of labels, {long hair, black hair, blue eyes, blush, ribbon}. In general, the generated image has the same clarity as the image in the training set and can express secret information correctly.

4.2 Hiding capacity

This paper uses the attribute labels of anime character to represent secret information, which has a higher hiding capacity compared with the existing CIH methods. Take Fig. 7 as an example, the secret information expressed is “National Double First-class construction university and a high-level construction university in Jiangsu province.” Among them, each anime character expresses 14-bit secret information, and 64 anime characters all

Table 1 Image quality evaluation

Method	Original	Generated	Distinction
Tenengrad gradient [39]	34.26	34.50	0.7%
Variance [39]	1674.91	1515.72	− 9.5%
Vollath [40]	1512.79	1415.13	− 6.45%
SMD [41]	2215.99	2336.70	5.44%
Entropy [41]	4.83	5.21	1.62%

express secret information. That is, the transmission of secret messages up to 896 bit in a stego-image. Its capacity is compared to the current CIH methods, as shown in Table 2.

In this paper, $N \times N$ smaller anime characters are combined into a stego-image. If $N = 1$, each stego-image can express 14 bits of information. Although the capacity is similar to the existing methods, the proposed method does not require the establishment of a huge image database in advance, and the time to generate a stego-image is much shorter than to retrieve a stego-image. Therefore, the proposed method has better efficiency under the same capacity. Because in the implementation of GAN-based anime characters generation, 8*8 output is more common, we set N to 8. Compared with the cover selection methods, this paper has a great improvement in the hiding capacity. Compared with the current best method, the capacity of this paper is about 60 times of its capacity. Secondly, the capacity of the proposed method can be adjusted according to the actual situation, that is, the size of N can be determined according to the actual needs. Assuming that the secret information to be sent is C bits, then $N \geq \lceil \sqrt{C/14} \rceil$. Finally, the same secret information can be represented by different secret images, which improves the flexibility and security of the algorithm.

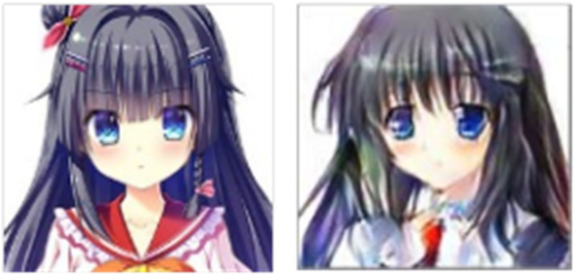
4.3 Robustness

Robustness is an important factor in evaluating the performance of coverless information hiding, which determines whether the receiver can correctly extract secret messages. Several kinds of attacks applied to the stego-images are listed below.

(a) Rotational attack, with angles of 10°, 30°, and 50°, respectively

(b) Scaling, with scaling ratios of 0.3, 0.5, 0.75 and 1.5, respectively

(c) Gaussian noise. The mean value is 0 and variance is 0.001, 0.005 and 0.1, respectively.



a. original image **b**. generated image

Fig. 6 **a** Original image. **b** Generated image

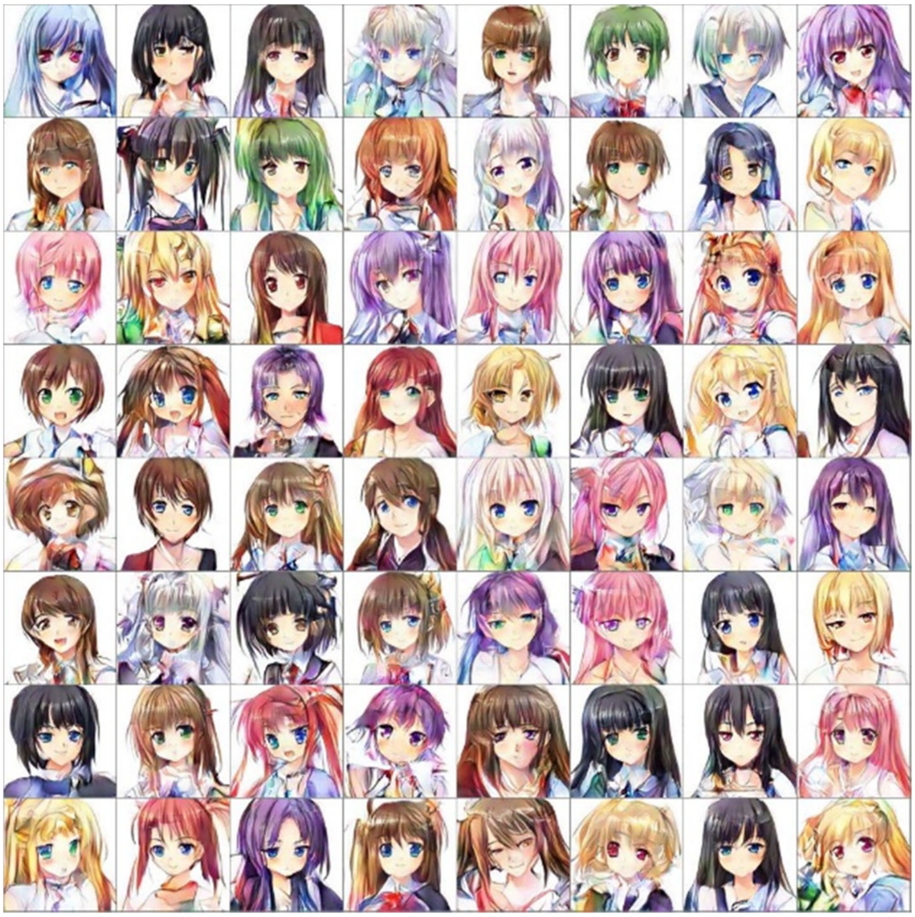


Fig. 7 An example of stego-image

(d) salt and pepper noise. The mean value of noise is 0, and the variance is 0.001, 0.005, and 0.1, respectively

(e) Speckle noise. The mean value of noise is 0, and the variance is 0. 01, 0.05 and 0.1, respectively

(f) Median filtering. Template sizes are 3 × 3, 5 × 5, 7 × 7, respectively

(g) Mean filtering. Template sizes are 3 × 3, 5 × 5, 7 × 7, respectively

(h) gaussian filtering. Template sizes are 3 × 3, 5 × 5, 7 × 7, respectively

In this paper, bit error rate (BER) is introduced to measure the robustness of the algorithm in the communication process.

$$BER = \frac{\sum_{1=1}^{m} p_i \oplus q_i}{m} \tag{1}$$

Where p_i represents the correct binary information, q_i represents the extracted binary information, and m represents the total number of binary information fragments. The test results are shown in Table 3. Although it is slightly inferior to the method [14], it is focused on robustness. But they are better than the methods [19] [20]. The purpose of this paper is to increase the hidden capacity of the CIH methods as much as possible based on ensuring certain robustness.

Table 2 Hiding capacity

Method	Capacity (bits $\cdot$ *carrier*$^{-1}$)
Literature [7]	8
Literature [19]	8
Literature [14]	15
Literature [20]	18
Proposed method (1*1)	14
Proposed method (8*8)	896

4.4 Anti-steganalysis and security

The original intention of CIH is to completely resist the detection of steganalysis algorithm. The most basic purpose of steganalysis is to divide the input image into stego-image and normal image. Generally, as long as the carrier is modified, the modification traces will be left, and it is possible for steganalysis algorithms to detect the existence of hidden behavior successfully. However, in theory, for the proposed CIH method, the stego-image and the randomly generated image are completely the same under the steganalysis algorithm and cannot be distinguished. In order to verify this theory, we used

Table 3 Robustness test results (BER)

Attack		Literature [14]	Literature [19]	Literature [20]	Proposed
Rotational	10°	0.164	1	0.7894	0.0937
	30°	0.1116	0.9681	0.8307	0.1190
	50°	0.1288	1	0.792	0.1676
Scaling	0.3	0.0086	1	0.8204	0.8992
	0.5	0	1	0.7364	0.5892
	0.75	0	1	0.5943	0.2354
	1.5	0	0.9894	0.3928	0.0582
	3	0	1	0.2984	0.0505
Gaussian noise	σ(0.001)	0.0301	0.9896	0.8088	0.1548
	σ(0.005)	0.0172	1	0.8165	0.4680
	σ(0.1)	0.0086	0.9896	0.8662	0.9638
Salt noise	σ(0.001)	0	0.8617	0.3359	0.1609
	σ(0.005)	0	0.9787	0.5065	0.4904
Speckle noise	σ(0.01)	0.0086	1	0.6951	0.0972
	σ(0.05)	0.0086	1	0.8798	0.2341
	σ(0.1)	0.0258	1	0.9367	0.9107
Median filter	(3 × 3)	0	1	0.6822	0.1813
	(5 × 5)	0.0086	1	0.6951	0.3486
	(7 × 7)	0.0172	1	0.8088	0.4699
Mean filter	(3 × 3)	0	1	0.739	0.2424
	(5 × 5)	0	1	0.8488	0.1861
	(7 × 7)	0	1	0.876	0.7024
Gaussian filter	(3 × 3)	0	1	0.686	0.1743
	(5 × 5)	0	1	0.7558	0.3051
	(7 × 7)	0	1	0.9031	0.4984

Table 4 Steganalysis results

Stego-image size	Accuracy
1*1	0.00%
8*8	0.03%

the most popular Xu-Net [42] with the pre-trained model to perform steganalysis on 1000 stego-images. The results are shown in Table 4.

Obviously, the proposed method can well resist the detection of algorithm. Besides, the proposed method provides multiple protection for secret information. First of all, we determined the first attribute mapping and location index by using the secret key agreed by both parties in advance, to ensure that it is difficult for attackers to obtain the accurate mapping relationship and the location of anime character expressing secret information. Meanwhile, for different users, the stego-images corresponding to the same secret information and the stego-images obtained by the same users at different times are all different. Therefore, it is difficult for attackers to decipher secret messages.

5 Conclusion

This paper proposed a new idea for CIH. Driven by secret information and constrained by attribute labels, it directly generates anime character with high quality to transmit secret information. Compared with the current cover selection methods, proposed method has a great improvement in capacity. However, there is a gap in robustness compared with the current robust coverless information hiding methods. The next step is to improve the robustness of the method by optimizing the generation model. This paper provides a more practical solution for the development of coverless information hiding, that is, to express secret information in the process of generating target images according to attributes, which has certain guiding significance for the development of coverless information hiding.

Abbreviations

GANs: Generative adversarial networks; CIH: Coverless information hiding; DCT: Discrete cosine transformation; LBP: Local binary patterns; CGK: Cardan Grille Mask; LSTM: Long short-term memory network; BER: Bit error rate

Acknowledgements
Thanks to all those who have suggested and given guidance for this manuscript.
Availability of data and materials
Please contact corresponding author for data requests.

Authors' contributions

YC was a major contributor in writing the manuscript. Other authors provided guidance on the ideas and experiments of the manuscript. All authors read and approved the final manuscript.

Funding
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 grants U1836208, U1536206, U1836110, 61602253, 61672294, 61972205, 61972207; 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; and by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

Competing interests

The authors declare that they have no competing interests.

Author details
[1]Jiangsu Engineering Center of Network Monitoring, Engineering Research Center of Digital Forensics, Ministry of Education, School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China. [2]Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada.

Received: 20 March 2020 Accepted: 17 August 2020
Published online: 03 September 2020

References

1. R. Meng, G. Steven, J. Wang, X. Sun, A fusion steganographic algorithm based on faster R-CNN. Comput Mater Continua **55**(1), 001–016 (2018)
2. Y. Zhang, X. Luo, Y. Guo, C. Qin, F. Liu. Multiple robustness enhancements for image adaptive steganography in lossy channels. IEEE Transactions on Circuits and Systems for Video Technology, 2019, Published online (Early Access), DIO:10.1109/TCSVT.2019.2923980.
3. K.A. Kingsley, A.M. Barmawi, Improving data hiding capacity in code based steganography using multiple embedding. J Inform Hiding Multimedia Signal Processing **11**(1), 14–43 (2020)
4. C. Qin, W. Zhang, F. Cao, X. Zhang, C. Chang, Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection. Signal Process. **153**, 109–122 (2018)
5. M.I. Moussa, E.M. Badr, S. Almotairi, A data hiding algorithm based on DNA and elliptic curve cryptosystems. J Inform Hiding Multimedia Signal Processing **10**(3), 458–469 (2019)
6. T. Qiao, X. Luo, T. Wu, M Xu, Z Qian. Adaptive steganalysis based on statistical model of quantized DCT coefficients for JPEG images. IEEE Transactions on Dependable and Secure Computing, Published online (Early Access), DIO: https://doi.org/10.1109/TDSC.2019.2962672.
7. Z. Zhou, Q. Wu, C. Yang, X. Sun, Z. Pan, Coverless image steganography based on histograms of oriented gradients-based hashing algorithm. J Internet Technol **18**(5), 1177–1184 (2017)
8. I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, Y. Bengio, Generative adversarial nets. In: Advances in neural information processing systems, 2672–2680 (2014)
9. Y. Yang, Q. Wu, X. Feng, A. Thangarajah, Recomputation of dense layers for the performance improvement of DCNN. IEEE Trans. Pattern Anal. Mach. Intell.. https://doi.org/10.1109/TPAMI.2019.2917685
10. C. Yuan, Z. Xia, X. Sun, Q. Wu, Online. DOI (2019). https://doi.org/10.1109/TCDS.2019.2920364
11. C Yuan, Z Xia, L Jiang, Y Cao, Q Wu, X Sun, Fingerprint liveness detection using an improved CNN with image scale equalization, IEEE Access, 2019, 7: 26953-26966.
12. Y. Jin, J. Zhang, M. Li, Y. Tian, H. Zhu, Z. Fang. Towards the automatic anime characters creation with generative adversarial networks. arXiv preprint arXiv:1708.05509, 2017.
13. J. Wang, T. Li, X. Luo, Y. Shi, S. Jha, Identifying computer generated images based on quaternion central moments in color quaternion wavelet domain. IEEE Trans Circuits Systems Video Technol **29**(9), 2775–2785 (2018)
14. X. Zhang, F. Peng, M. Long, Robust coverless image steganography based on DCT and LDA topic classification. IEEE Transactions on Multimedia **20**(12), 3223–3238 (2018)
15. Z. Zhou, Q. Wu, Y.Yang, X. Sun. Region-level visual consistency verification for large-scale partial-duplicate image search. ACM Transactions on Multimedia Computing, Communications, and Applications. 2020, DOI: doi.org/https://doi.org/10.1145/3383582.2020
16. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications (Cambridge University Press, 2009)
17. Z. Zhou, H. Sun, R. Harit, X. Chen, X. Sun. Coverless image steganography without embedding. In: Int Confer Cloud Comput Security. Springer, Cham. 2015: 123-132.
18. Z. Zhou, Y. Cao, M. Wang, E. Fan, Q. Wu, Faster-RCNN based robust coverless information hiding system in cloud environment. IEEE Access **7**, 179891–179897 (2019)
19. C. Yuan, Z. Xia, X. Sun, Coverless image steganography based on SIFT and BOF. J Internet Technol **18**(2), 435–442 (2017)
20. S. Zheng, L. Wang, B. Ling, D. Hu, Coverless information hiding based on robust image hashing. In: International Conference on Intelligent Computing, Liverpool, UK, 536–547 (2017)
21. Y. Cao, Z. Zhou, X. Sun, C. Gao, Coverless information hiding based on the molecular structure images of material. Comput Materials Continua **54**(2), 197–207 (2018)
22. L. Zou, J. Sun, M. Gao, W. Wan, B.B. Gupta, A novel coverless information hiding method based on the average pixel value of the sub-images. Multimed. Tools Appl., 1–16 (2018)
23. J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, Y. Jia, A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix. IETE Tech. Rev., 1–11 (2018)
24. Z. Zhou, Y. Mu, Q. Wu, Coverless image steganography using partial-duplicate image retrieval. Soft. Comput. **23**(13), 4927–4938 (2019)
25. Y. Cao, Z. Zhou, C. Yang, X. Sun, Dynamic content selection framework applied to coverless information hiding. J Internet Technol **19**(4), 1179–1186 (2018)
26. H. Otori, S. Kuriyama, Texture synthesis for mobile data communications. IEEE Comput. Graph. Appl. **29**(6), 74–81 (2009)
27. K. Wu, C. Wang, Steganography using reversible texture synthesis. IEEE Trans. Image Process. **24**(1), 130–139 (2014)
28. H. Zhou, K. Chen, W. Zhang, Z. Qian, N. Yu, Targeted attack and security enhancement on texture synthesis based steganography. J. Vis. Commun. Image Represent. **54**, 100–107 (2018)
29. Z. Qian, H. Zhou, W. Zhang, X. Zhang, Robust Steganography Using Texture Synthesis. In: Advances in Intelligent Information Hiding and Multimedia Signal Processing, Taiwan, 25–33 (2016)
30. L. Pan, Z. Qian, X. Zhang, Steganography by constructing texture images. J. Appl. Sci., 625–632 (2016) (In Chinese)
31. Z. Qian, L. Pan, N. Huang, X. Zhang, Constructive steganography by tangles. KSII Transactions on Internet & Information Systems, 12(8) (2018)
32. Z. Qian, N. Huang, S. Li, X. Zhang, Constructive steganography using texture synthesis. IETE Tech. Rev., 1–9 (2018)
33. M. Liu, M. Zhang, J. Liu, Y. Zhang, Y. Ke. Coverless information hiding based on generative adversarial networks. arXiv preprint arXiv:1712.06951, 2017.
34. M. Liu, M. Zhang, J. Liu, P. Gao, Y. Zhang, Coverless information hiding based on generative adversarial networks. J. Appl. Sci. **36**(2), 371–382 (2018) (In Chinese)
35. X. Duan, H. Song, C. Qin, M.K. Khan, Coverless steganography for digital images based on a generative model. Comput Materials Continua **55**(3), 483–493 (2018)

36. J. Liu, T. Zhou, Z. Zhang, Y. Ke, Y. Lei, M. Zhang, X. Yang. Digital cardan grille: a modern approach for information hiding. arXiv preprint arXiv:1803.09219, 2018.
37. M. Saito, Y. Matsui. Illustration2vec: a semantic vector representation of illustrations. SIGGRAPH Asia 2015 Technical Briefs. ACM, 2015: 5.
38. Z. Yang, X. Guo, Z. Chen, Y. Huang, Y. Zhang, RNN-stega: Linguistic steganography based on recurrent neural networks. IEEE Trans Inform Forensics Security **14**(5), 1280–1295 (2019)
39. S. Qin, Research and improvement of digital image clarity evaluation function. Microcomputer Appl **30**(1), 32–37 (2011) (In Chinese)
40. Y. Wang, Y. Tan, J. Tian, A new kind of sharpness-evaluation-function of image. J Wuhan Univ Technol **3**, 124–126 (2007) (In Chinese)
41. Z. Li, X. Li, L. Ma, Y. Hu, L. Tang, Research on clarity evaluation method oriented to no-reference image. Remote Sensing Technol Application **26**(2), 239–246 (2011) (In Chinese)
42. G. Xu, H. Wu, Y. Shi, Structural design of convolutional neural networks for steganalysis. IEEE Signal Proc Lett **23**(5), 708–712 (2016)

Publisher's Note

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