Generative Image Steganography Based on GANs

Yaojie Wang[1,2](✉), Xiaoyuan Yang[1,2], and Hengkang Jin[1,3]

[1] Engineering University of PAP, Xi'an 710086, China
wangyaojie0313@163.com
[2] Key Laboratory of Network and Information Security of PAP,
Xi'an 710086, China
[3] Unified Communications and Next Generation Network Systems Laboratory,
Xi'an 710086, China

Abstract. According to the embedding method of secret information, steganography can be divided into: cover modification, selection and synthesis. In view of the problem that the cover modification will leave the modification trace, the cover selection is difficult and the load is too low, this paper proposes a generative image steganography scheme based on GANs, which combines with cover synthesis. Based on GAN, the scheme uses secret information as the driver and directly generates encrypted images for transmission, which can effectively resist the detection of steganalysis algorithms. The security of the scheme is based on the key of the encryption algorithm. Even if the attacker obtains the transmitted information, only the meaningless result will be obtained without the key. Experiments were carried out on the data set of CelebA, and the results verified the feasibility and security of the scheme.

Keywords: Information hiding · Cover synthesis · Generative adversarial networks · Security

1 Introduction

In Fridrich's groundbreaking work of modern steganography [1], steganographic channel is divided into three categories, cover selection, modification and synthesis. cover modification is the most common method of traditional information hiding, but it is inevitable to leave some traces of modification on the cover, which makes it difficult to resist the detection based on statistical analysis algorithm. Cover selection method does not modify the cover image, thereby avoiding the threat of the existing steganalysis technology. This method cannot be applied to practical applications because of its low payload [2]. Compared with the former two methods, the cover synthesis method is more suitable. However, this method is only a theoretical conception, rather than a practical steganography, because it is difficult to obtain multiple natural samples [3].

Fortunately, a data-based sampling technique, generative adversarial networks (GANs) [4] have become a new research hot spot in artificial intelligence. The biggest advantage and feature of GANs is the ability to sample real space and generate samples driven by noise, which provides the possibility for cover synthesis. Based on GANs,

W. Han et al. (Eds.): CTCIS 2019, CCIS 1149, pp. 1–15, 2020.
https://doi.org/10.1007/978-981-15-3418-8_1

this paper combines symmetric encryption and information hiding, and proposes a generative image steganography scheme. We do not make any modifications to the generated image, which can resist steganographic analysis detection. At the same time, a key-based coordinate encryption algorithm is proposed, which accords with the Kerckhoffs principle [5]. It enhances the ability to resist steganalysis and expands new ideas for the development of information hiding and cryptography.

The remainder of this letter is organized as follows: We detail the development and improvement of machine learning in steganography. Section. 3 shows how to build generative image steganography by GANs. Experiment results are demonstrated in Sect. 4. Section 5 concludes this research and details our future work.

2 Improvement of Generative Model in Steganography

In recent years, some researchers have tried to introduce the theory of confrontation into the field of information security. PassGAN [6] was introduced into the code-deciphering work, and the password generative method based on machine learning was used to replace the artificially formulated password rules, which made obvious progress. Biggo et al. [7] introduced the idea of confrontation into network attack and defense, and the concept of confrontation model was proposed, especially for the improvement of vulnerability repair. In terms of information hiding, some researchers have introduced the generation of confrontation networks into steganography, but the main method they use is still based on the framework of carrier modification. The representative schemes are as follows:

(1) SGAN & SSGAN

Volkhonskiy et al. [8] proposed the SGAN scheme, which first combined GAN with steganography, adding a message embedding module on the basis of original GAN. Different from the traditional method, the generated image is used as the carrier to embed the information. At the same time, an additional steganographic analysis discriminator is trained to ensure that the generated image of the generator cannot be distinguished from the encrypted image after embedded information, so that the steganographic security is further improved. The scheme structure is shown in Fig. 1 below:

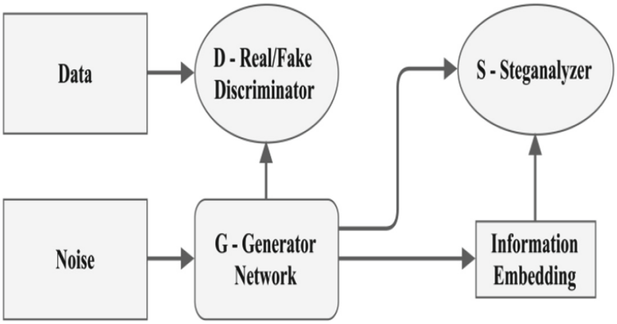


Fig. 1. The structure of SGAN

Similar to [8], Shi et al. [9] introduce WGAN [10] to increase convergence speed and achieve more stable image quality. At the same time, GNCNN was used as the steganographic analysis module to improve the safety of steganography. Wang et al. [11] improved the framework and reconstructed the discriminator of original GAN. The generated image is first embedded into the secret information, and then input into the discriminator for discriminating, forcing the generated image to be more suitable for embedding information while ensuring image quality.

The basic idea of the above solution is to introduce a simple LSB modification module to the GAN confrontation training to achieve steganography. On the one hand, the advantages of generating model in GAN are utilized to ensure that the generated carrier images meet the statistical characteristics of natural images. On the other hand, an additional steganographic discriminator and message embedding module are added to ensure that the generated vector image is effective against steganalysis. Therefore, these schemes can generate image carriers that meet specific steganographic security, but the general performance against steganographic analysis is poor and cannot effectively resist the detection of other steganalysis methods.

(2) ASDL-GAN

Tang et al. [12] proposed the automatic Steganographic Distortion Learning (ASDL) for the first time based on the additive distortion cost function. They use machine learning to obtain the probability matrix P of image pixel modification, then use the STC method to embed secret information. This scheme is called ASDL-GAN.

The scheme utilizes the adversarial network to improve the performance of the generator G, and the probabilistic matrix P is obtained by sampling the generator G to implement steganography. The discriminator D distinguishes both the encrypted carrier and the original carrier. The basic structure is shown in Fig. 2 below:

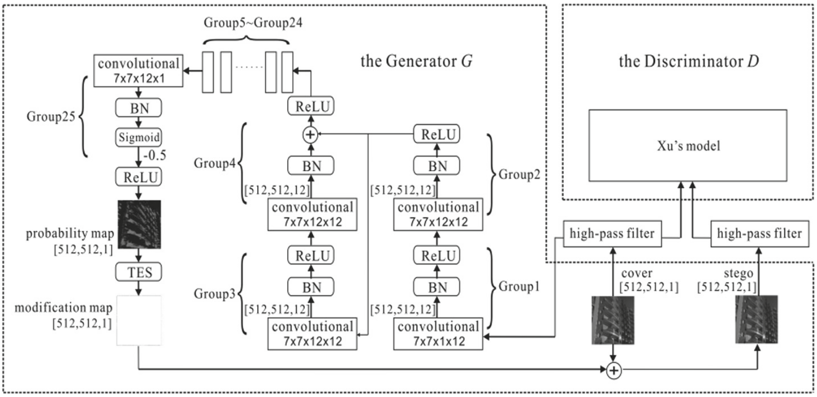


Fig. 2. The structure of ASDL-GAN

To learn the probability matrix P, they propose a miniature network TES as the activation function of the probability matrix. To further improve the security of ASDL-GAN, Yang et al. [13] proposed UT-SCA-GAN (U-net, Tanh-simulator function, Selection Channel Awareness). They use the Tanh-simulator function instead of the TES activation function to improve efficiency, using U-net as the basic structure of the generator. To resist SCA steganalysis, the scheme also introduces the absolute values of 30 high-pass filters in the rich model as auxiliary conditions. The basic framework is shown in Fig. 3:

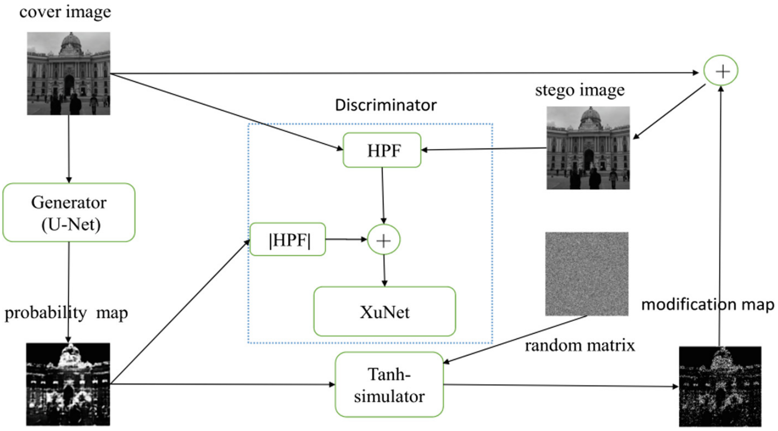


Fig. 3. The structure of UT-SCA-GAN

The main method of these representative schemes is still to embed secret information based on carrier modification. They do not fundamentally satisfy the statistical characteristics of the original image. That is to say, the transmitted encrypted carrier still has traces of modification, which makes it difficult to resist the detection of the steganographic algorithm.

For further study the application of adversarial training in steganography,we propose a novel method—generative image steganography based on GANs. Its feasibility and safety have been verified through experiments, and This paper has the following contributions:

1. According to the idea of carrier synthesis, the concept of generative image steganography is innovatively proposed, and no modification is made to the generated carrier information, which can fundamentally resist the detection of steganographic analysis.
2. Combining "two points, one line" mathematical principle, a coordinate encryption algorithm is proposed, which combines symmetric encryption and information hiding, and satisfies the Kerckhoffs' principle. Ideally, without shared keys, the extraction of secret information is equivalent to brute force cracking.

3 Generative Image Steganography

According to the characteristics of ACGAN [14] which can generate specific label messages, this paper proposes a GAN-based generative image steganography scheme, which directly generates secret cryptographic carriers driven by secret messages, and combines symmetric encryption with steganography to further improve security. The specific program framework is shown in Fig. 4.

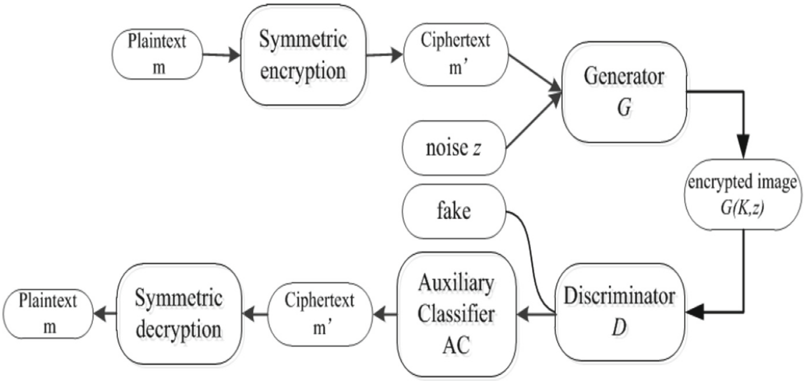


Fig. 4. The structure of the proposed scheme

The scheme consists of encryption algorithm and steganography algorithm. The encryption algorithm can be represented by coordinates, which can be encrypted and decrypted according to the "two points and one line" mathematical principle. Meanwhile, it can expand the dimension according to different security levels. This paper takes two-dimensional plane as an example to introduce the principle of the algorithm. The GAN-based steganographic algorithm replaces the category label with secret information as the driver, directly generates encrypted images for transmission, then the receiver extracts the embedded secret information through the discriminator, thereby realizing generative image steganography.

3.1 Symmetric Encryption Algorithm

First introduce the mathematical algorithm of the symmetric algorithm as shown below:

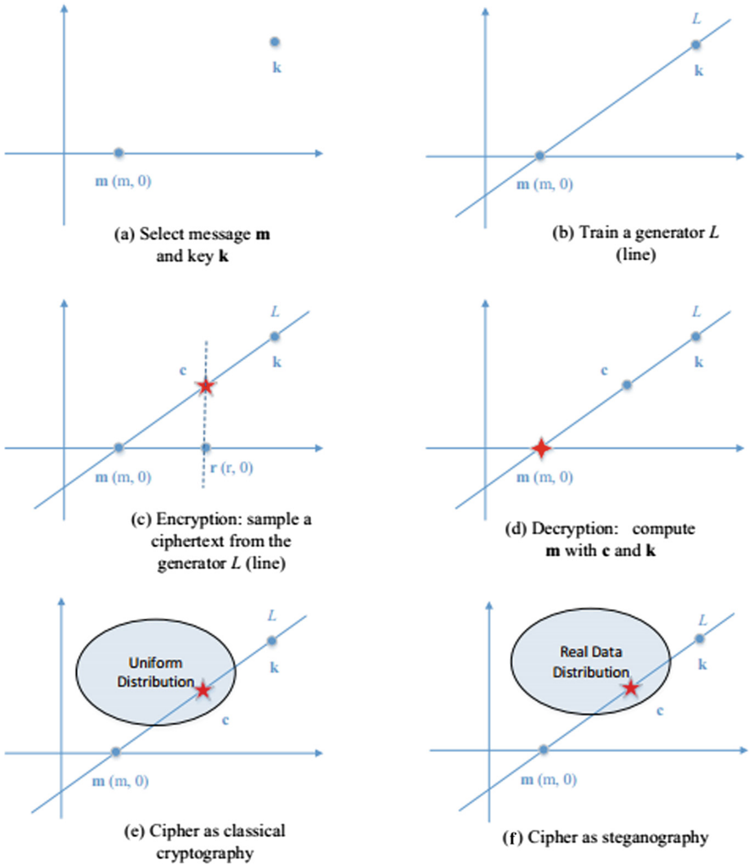
$$m' = E(m, K) \tag{1}$$

$$m = D(m', K) \tag{2}$$

Where m is the plain text, K is the shared key, and m$'$ is the encrypted ciphertext, that is, the encrypted information. $E(.)$ denotes an encryption algorithm and $D(.)$ denotes a decryption algorithm. In this scheme, both $E(.)$ and $D(.)$ are equivalent, both of which are represented by $L(.)$.

From a simple point of view, we take the two-dimensional plane as an example to introduce the structure of the algorithm. Suppose that a coordinate point (m,0) on the X-axis in the plane coordinate represents a secret information m. The Shared key *k*(kx, ky) may be any point on the plane except for points on the X-axis, as shown in Fig. 5(a). Two points m and k define a unique straight line L(m, k) as shown in Fig. 5(b). In this case, L can be considered as the simplest ciphertext generator,which can generate different ciphertexts according to different samples. The sender selects a random number r, then sample a point *c*(cx,cy) according to the line, which can be regarded as the corresponding ciphertext, as shown in Fig. 5(c). The receiver extracts the ciphertext c from the encrypted image. According to the mathematical principle of "two points and one line", it's easy for receiver to get the m by intersection of the L(c, k) and the X-axis as shown in Fig. 5(d).

We continue to expand this idea. The symmetric encryption of this paper is different from the classical cryptography. Under the same key condition, the ciphertext is not unique. This is also a groundbreaking work, which is worthy of further study. If the ciphertext follow a uniform distribution, this cipher (encryption algorithm) is a classical cryptography shown in Fig. 5(e). If the ciphertext follow a real data distribution, this cipher (steganography algorithm) is a generative steganography, as shown in Fig. 5(f).



(a) Select message **m** and key **k**

(b) Train a generator *L* (line)

(c) Encryption: sample a ciphertext from the generator *L* (line)

(d) Decryption: compute **m** with **c** and **k**

(e) Cipher as classical cryptography

(f) Cipher as steganography

Fig. 5. Symmetric encryption algorithm

In this simple encryption scheme above, this scheme can only resist low-level Ciphtext-only attack. However, cryptographers can easily find the key by using statistical methods such as frequency analysis. Therefore, we can increase the dimension, increase the amount of calculation, and limit the frequency of use, such as changing the key periodically.

3.2 Image Steganography Algorithm

Before we apply the proposed scheme, we need to train ACGAN first. Since each generated sample in ACGAN has a corresponding category label, ACGAN's input consists of z and $C \sim P_C$, so generator G uses both z and C to generate the image $X_{fake} = G(C, z)$. Discriminator D outputs the probability distribution P(S|X) of the real data and the category label's probability distribution P(C|X) = D(X). The loss function has two parts: the likelihood log L_S of the real data and logarithmic L_C of correct category:

$$L_S = E[logP(S = real|X_{real})] + E[logP(S = fake|X_{fake})] \tag{3}$$

$$L_C = E[logP(C = c|X_{real})] + E[logP(C = c|X_{fake})] \tag{4}$$

Training discriminator D ultimately maximizes $L_S + L_C$, while training generator G targets $L_S - L_C$ to be minimal. ACGAN's characterization for z is independent of category label C. In training ACGAN, we use the same parameters so that the receiver and sender can get the same generator, and the above information is completely confidential.

Considering that the generator of ACGAN can be combined with noise z and category label C as drivers, which can directly generate specific image samples, and label $C(C_1, C_2, C_3, \cdots)$ can be composed of multiple sub-labels. Combined with the idea of carrier synthesis, the category label C is replaced with secret information m', and directly generate an encrypted image on the basis of ACGAN. This method realizes generative image steganography, which avoids the modification of the carrier. The detailed hiding and extraction process is as follows:

In the hiding process, we first encode the coordinate information m' that needs to be hidden into the corresponding sub-label, and combine the sub-label into label group G (m′). Then, we combine the label group G(m′) and random noise Z as the driver and input them into ACGAN, so that we can generate the encrypted image $G(m',z)$ of the specified category by the generator and realize the generated image steganography. The hidden process is shown in Fig. 6:

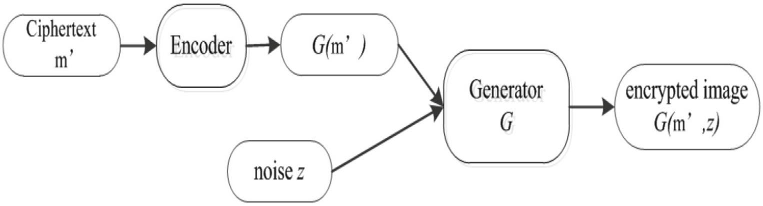


Fig. 6. The structure of the hidden algorithm

In the extraction process, after receiving the encrypted image, the receiver takes a reverse operation to extract information. First, we input the encrypted image into discriminator D in the ACGAN, but D can not directly output the secret information, the output is the likelihood logarithm of image category. Next, the probability of each category in the encrypted image is output by the softmax function [15]. Then, the probability of the image category is converted into a corresponding category label. Finally, we decode the obtained category labels, thereby obtaining embedded coordinate information to achieve information extraction. The extraction process is shown in Fig. 7.

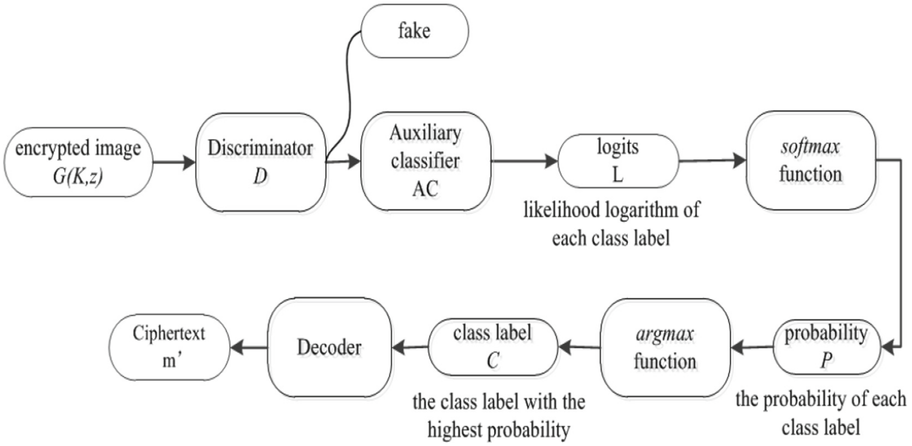


Fig. 7. The structure of extraction algorithm

4 Experiment and Analysis

The ACGAN network training for sender and receiver is as follows: the random noise z is uniformly distributed on (−1,1), the real sample data set is CelebA celebrity face set, and the number of training steps is 10,000. The experimental environment is shown in Table 1. The secret information to be hidden is 10 articles randomly selected from the People's Daily official website.

The optimizer in ACGAN uses a momentum-based optimization method with a learning rate of 0.0002. At each training, the weight of the discriminator D is updated once, the weight of the generator G is updated twice, and the weight of the auxiliary classifier AC is updated once.

The generator consists of four deconvolutional layers. The 3×3 filters are used in each layer. The discriminator consists of four convolutional layers and four deconvolutional layers. The auxiliary classifier consists of four convolutional layers and one fully connected layer [16].

Table 1. Experimental environment

Software platform	Tensorflow v0.12	
Hardware environment	CPU	i7-8250U 3.2 GHz
	RAM	16 GB DDR3 1600 MHz
	GPU	NVIDIA 1080

4.1 Message Hiding and Extraction

In order to verify the feasibility of the proposed scheme, this paper only takes the two-dimensional plane space as an example. First, the code table dictionary can be built to cover 3755 Chinese characters in the national level font library. In addition, national secondary Chinese characters and some common phrases and special symbols should be covered as much as possible. Based on the mnist handwritten digit set with 0–9 total 10 category labels, this method selects 10000 category label combinations to construct a code table dictionary, that is, every 4 numbers are grouped (each number can be selected from 10 numbers)), a total of 10000 groups, each group corresponding to a Chinese character word or phrase, to construct a one-to-one mapping code table dictionary, while the mapping dictionary can be randomly established by the program to establish a corresponding relationship and add a plus or minus sign before the category label to ensure the randomness of the dictionary, As shown in Table 2. In order to increase the difficulty of deciphering, the mapping dictionary should be replaced periodically or the mapping relationship should be changed to reduce the frequency of use of the same mapping dictionary.

Table 2. Examples of the dictionary

Chinese character or phrase	Category label combination
福建 (Fujian)	−0021
火箭军 (Rocket army)	3024
运-20大型运输机 (Yun-20 large transport aircraft)	−0322
...	...

In the plane coordinates, the random selection message m is: 终南山 (Zhongnanshan). We can Find the category label combination in the code table dictionary is −1100, and the corresponding m coordinate is (−10.000, 0); assuming that the receiver and the sender share the key K coordinate (1.000, 11.000) in advance, the sampling generator L(m,k) is: y = x + 10, and the sampling is performed at random to obtain the sampling point m' coordinate (−3.124, 6.876), which is the delivery message to be hidden.

In this experiment, the input label setting vector length is 40, and the message m' (−3.124, 6.876) to be hidden is encoded (the first and 21st bits are positive and negative signs, and 1/0 is positive/negative signs respectively; 2nd Bits to the 20th place represent the x coordinate; the 22nd to 40th bits represent the y coordinate), and the obtained secret information $\phi(\mathrm{m}')$ is as follows:

$$\phi(m') = \begin{Bmatrix} \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ \boxed{0} & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{Bmatrix} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \textbf{X-axis cod-} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \textbf{Y-axis} \end{array}$$

According to the label mapping dictionary on the CelebA dataset, it corresponds to three labels: “pico opening”, “smile”, “dark”.

As we have described, GS-GAN can generate multi-label samples by entering multiple tags in the generator, so you can use the trained generator to generate a dense image with labels. The experimental results are shown in Fig. 8. The “no-label” image is the process of input noise generation; the “+ pico-port” image is generated by the same noise and the “pico-port” label; Then add labels in order. In this manner, the last image is generated by the same noise z and 3 different labels.

Every time we train GS-GAN network 400 times in the experiment, we carry out a test that generates secret image by secret message K and extracts secret message from encrypted image.

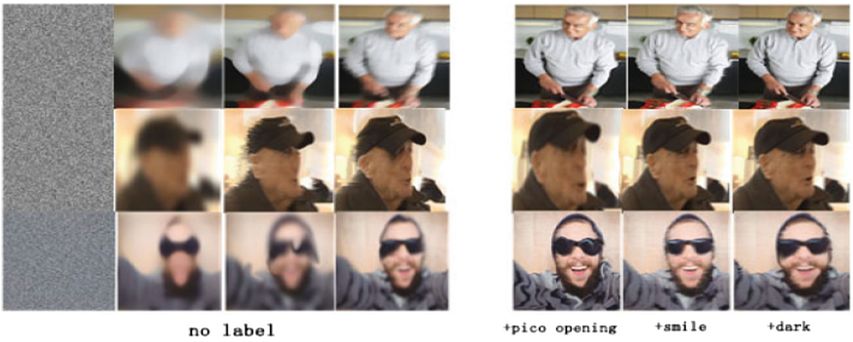


Fig. 8. The generated encrypted pictures

The error rate of extracting information is shown in Fig. 9. After 6,000 trainings, the extracted information error rate is less than 0.07, and only the error correction code is added at the time of encoding to ensure the correctness of the decoding. It can therefore also be seen that the proposed solution allows for errors in the communication process without affecting the correct delivery of the communication information.

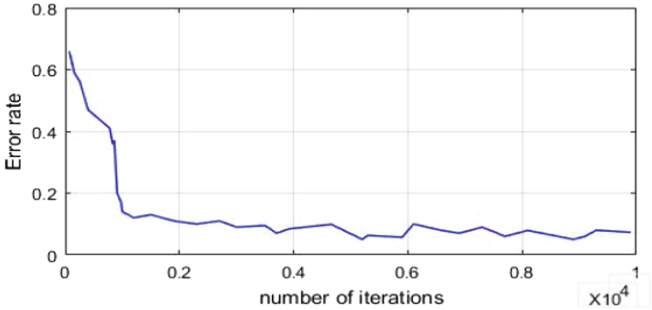
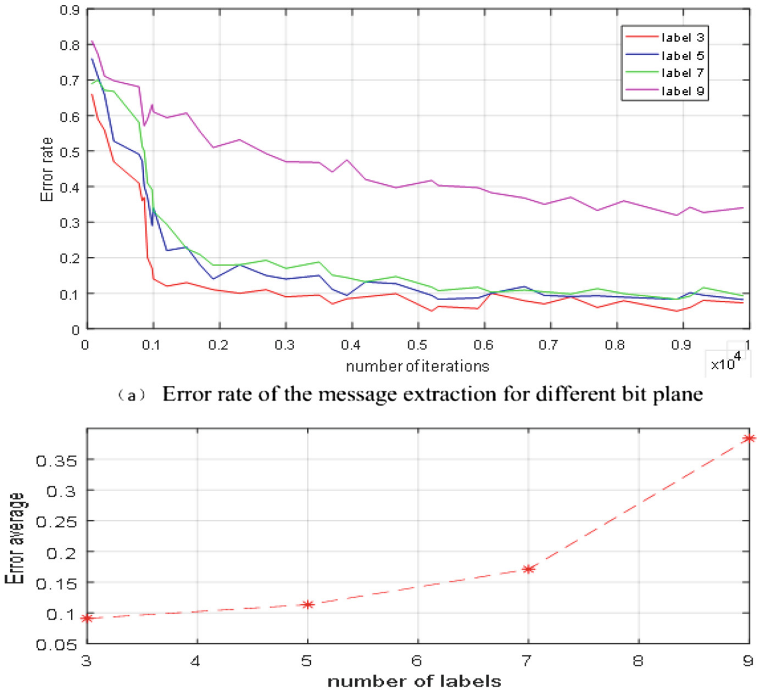


Fig. 9. The number of error class labels extracted

In order to further verify the scheme, we increase the amount of embedded information under the same conditions, that is, increase the number of labels in the dense image. As shown in Fig. 10(a), the number of labels is 3, 5, 7, and 9, respectively. As the number of labels increases, the error rate of extracting information increases with the same number of trainings. Figure 10(b) shows the average error rate of information extracted with different number of tags after 8000 training sessions. The error rate of the extracted information decreases as the number of labels decreases. When the number of labels is ≤ 7, after 8000 trainings, the error rate of the extracted information is less than 0.09. We can add error correction code to ensure the correctness of decoding.



（a） Error rate of the message extraction for different bit plane

（b） Average Error rate the message extraction

Fig. 10. Error rate of the message extraction

It can be seen from the experiment that we can generate the corresponding encrypted image according to the specified label information, and correctly extract the selected label from it. When the number of labels does not exceed a certain threshold, the transmission error rate of the scheme can be effectively reduced, and no modification to the carrier is needed, and the detection of the steganalysis algorithm can be more effectively resisted.

4.2 Hiding Capacity

According to Sect. 3.1, each encrypted image has 10 label images. The corresponding hiding capacity is tested by changing the different word segmentation methods in the code dictionary. We conducted hidden capacity test experiments according to 3 different word segmentation methods. The experimental results are shown in Table 3.

1. We don't use the words segmentation in the dictionary but directly divide the text information into single Chinese character. In the hidden experiment, each word corresponds to a label image. That is,each encrypted image is composed of 10 label images, so the hidden capacity of each encrypted image is 10 words. Since no words segmentation dictionary is used, the number of phrases in the dictionary and the average word length are zero.
2. Select words with an average length of 2 to establish a dictionary (100 phrases, average length is 2). This dictionary not only includes label images corresponding to the common words, but also the label image corresponding to the words of different lengths. According to the principle of forward maximum matching, if the secret information contains the phrase in the mapping dictionary, the words are divided into the phrase, otherwise it is divided into a minor phrase or word, and so on. Randomly select 10 text segments, the experimental results show that the average hidden capacity of each image is 17.42 words.
3. Similarly to method 2, a dictionary is established for words with an average length of 3 (100 phrases, average length is 3). We also adopted the principle of forward maximum matching. The experimental results show that the average hiding capacity of each image was 30.11 words.

Table 3. Experimental results for the hiding capacity test

Average words length of dictionary (Chinese characters/words)	Words numbers of phrases dictionary	The capacity of literature [17] 's method (Chinese characters/image)	The capacity of our method (Chinese characters/encrypted-image)
0	0	1.00	10.00
2	100	1.57	17.42
3	100	1.86	30.11

The experimental results show that establishing a reasonable code dictionary and increasing the average length of the words in the dictionary can improve the information hiding capacity. Theoretically, the hidden capacity of a single label image is the number of Chinese characters in the dictionary. The average information hiding capacity of multiple images is the average length of secret information fragments after word segmentation:

$$\overline{C} = \frac{\sum_{i=1}^{n} C_i}{n} \tag{5}$$

Where: n is the number of secret information fragments, C_i is the length of the i-th secret information fragment.

It can be seen from Table 3 that the scheme of this paper has a large improvement in the hidden capacity. The reason is that each label image corresponds to one keyword, and the average length of the text information corresponding to the encrypted image containing multiple label images is greatly increased, making the capacity of hidden information. Each of the encrypted images in [17] corresponds to one high-frequency keyword, resulting in a relatively small amount of hidden information.

4.3 Security

The security of this paper is based on two aspects: First, a simple and easy encryption algorithm is proposed. According to the two-point and one-line mathematical principle, under the premise of no key, the single point cannot determine the straight line L(m, K), that is, brute force cracking is not feasible. That is to say, the security of the system depends on the confidentiality of the key used, not the confidentiality of the algorithm itself, in accordance with the Kerckhoffs criterion. At the same time, the spatial dimension can be expanded according to different confidential levels. When the security level is high, the spatial dimension is increased, so that the possibility of attacking the attacker is greatly increased, but the encryption and decryption operation still maintains a linear relationship, and the calculation amount is small and the encryption efficiency is high. Under the premise of regularly changing the key, the algorithm is easy to implement and difficult to decipher. Secondly, the secret image of hidden secret information is directly generated by ACGAN, and no modification is made to the carrier information, which greatly increases the anti-stealth analysis. Ability. Compared with the traditional methods of encryption and information hiding, the method proposed in this paper is more difficult to cause the suspicion of attackers, and it can cover secret communication more concealedly.

It is assumed that the attacker suspects that the transmitted image contains secret information, but since it does not have the same GS-GAN model as the communication parties, it is difficult to extract secret information from the dense image by the discriminator. Even if the hidden content is intercepted, only the meaningless result will be obtained without the key, thereby ensuring the security of the covert communication.

5 Conclusion and Future Work

This paper proposes a generative image steganography scheme (GS-GAN), which uses the latest technology of GAN to innovatively realize the new concept of “generative image steganography”. At the same time, the combination of symmetric encryption and information hiding has opened up new ideas for the development of information security. On the one hand, the information that needs to be hidden is used as the driver to directly generate the dense image for transmission, and the embedded carrier is not modified, which conforms to the idea of carrier synthesis, and can effectively resist the detection of the steganographic analysis algorithm based on statistics; on the other hand, the security is based on Receiving the shared key of both parties, even if the hidden content is intercepted, only the meaningless result will be obtained without the key, thereby ensuring the security of the covert communication. We used the CelebA dataset to evaluate the performance of the GS-GAN scheme. Theoretical analysis and experimental results show the feasibility and safety of the proposed method.

How to improve the structure of the discriminant model D and improve the ACGAN extraction process is the key research direction of our next step.

Acknowledgment. This work was supported by National Key R&D Program of China (Grant No. 2017YFB0802000), National Natural Science Foundation of China (Grant Nos. 61379152, 61403417)

References

1. Fridrich, J., Kodovsky, J.: Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur. **7**(3), 868–882 (2012)
2. Fridrich, J.: Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge (2010)
3. Holub, V., Fridrich, J., Denemark, T.: Universal distortion function for steganography in an arbitrary domain. EURASIP J. Inf. Secur. **2014**(1), 1 (2014)
4. Goodfellow, I., Pouget- Abadie, J., Mirza, M.: Generative Adversarial Networks[DB/OL], 10 June 2014. http://arxiv.org/abs/1406.2661
5. Ke, Y., Zhang, M.Q., Liu, J., et al.: Generative steganography with Kerckhoffs’ principle. Multimed. Tools Appl. **78**, 13805–13818 (2018)
6. Hitaj, B., Gasti, P., Ateniese, G., Perez-Cruz, F.: PassGAN: a deep learning approach for password guessing. In: Deng, R.H., Gauthier-Umaña, V., Ochoa, M., Yung, M. (eds.) ACNS 2019. LNCS, vol. 11464, pp. 217–237. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21568-2_11
7. Biggio, B., et al.: Evasion attacks against machine learning at test time. In: Blockeel, H., Kersting, K., Nijssen, S., Železný, F. (eds.) ECML PKDD 2013. LNCS (LNAI), vol. 8190, pp. 387–402. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40994-3_25
8. Volkhonskiy, D., Nazarov, I., Borisenko, B., et al.: Steganographic generative adversarial networks (2017)
9. Shi, H., Dong, J., Wang, W., Qian, Y., Zhang, X.: SSGAN: secure steganography based on generative adversarial networks. In: Zeng, B., Huang, Q., El Saddik, A., Li, H., Jiang, S., Fan, X. (eds.) PCM 2017. LNCS, vol. 10735, pp. 534–544. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-77380-3_51

10. Arjovsky, M., Chintala, S., Bottou, L.: Wasserstein GAN (2017)
11. Wang, Y., Yang, X., Liu, J.: Information hiding scheme based on generating confrontation network. J. Comput. Appl. **38**(10), 2923–2928 (2018)
12. Tang, W., Tan, S., Li, B., et al.: Automatic steganographic distortion learning using a generative adversarial network. IEEE Sig. Process. Lett. **24**, 1547–1551 (2017)
13. Yang, J., Liu, K., Kang, X., et al.: Spatial image steganography based on generative adversarial network. https://arxiv.org/abs/1804.07939
14. Odena, A., Olah, C., Shlens, J.: Conditional image synthesis with auxiliary classifier GANs (2016)
15. Lücke, J., Sahani, M.: Generalized softmax networks for non-linear component extraction. In: de Sá, J.M., Alexandre, L.A., Duch, W., Mandic, D. (eds.) ICANN 2007. LNCS, vol. 4668, pp. 657–667. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74690-4_67
16. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. In: International Conference on Neural Information Processing Systems (2012)
17. Zhou, Z.L., Cao, Y., Sun, X.M.: Coverless information hiding based on bag-of-words model of image. J. Appl. Sci. **34**(5), 527–536 (2016)