Received May 15, 2019, accepted May 29, 2019, date of publication June 5, 2019, date of current version July 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920956

A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things

RUOHAN MENG[1,2], QI CUI[1,2], ZHILI ZHOU[1,2], ZHANGJIE FU[1,2] AND XINGMING SUN[1,2]
[1]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2]Jiangsu Engineering Centre of Network Monitoring, Nanjing 210044, China

Corresponding authors: Xingming Sun (sunnudt@163.com) and Zhilli Zhou (zhou_zhili@163.com)

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

ABSTRACT With the wide application of the Internet of Things (IoT), the risk of data leakage and theft in IoT is gradually increasing since communication channel is public in data transmission. Thus, the IoT security has become a major problem in information security. Steganography is one of the key methods to solve the problems of personal privacy disclosure and covert communication. In order to make sure secure communications, this paper proposes a novel steganography algorithm based on image-to-image translation by adding steganography module and steganalysis module to CycleGAN, adapting to the covert communication and privacy preserving of the IoT. Steganalysis network is used to improve the anti-detection ability of stego image. Moreover, cycle consistent in CycleGAN can guarantee the quality of the generated image. Through the proposed scheme, the stego image can resist steganalysis by monitors to some extent and remain intact. The experimental results show that this method has a better performance than the state-of-the-art approach.

INDEX TERMS Internet of Things (IoT), steganography, CycleGAN, image-to-image translation.

I. INTRODUCTION

Nowadays, Internet of Things (IoT) technologies have been widely used in industrial control, military investigation, identification technology, pervasive computing, etc [2]. The architecture of the IoT can be generally divided into three componets: cloud, device terminal and mobile terminal. Through the communication between mobile terminal and cloud, an instruction is sent to device terminal through the cloud, thereby realizing the connection between the things and the network [3]. In this situation, high-performance servers are usually required to provide public service computing [3]. Meanwhile, in order to effectively control the network congestion problem in IoT, the emergency packets are applied and improved [4]–[7]. In addition, for multiple cloud platforms and terminal devices, there are lots of service quality data, which may exist the leakage of important data [8]. Moreover, because IoT devices are close to users' lifes, such as video surveillance, vehicle localization, smart bracelet and so on, the most of data is about user privacy. It is possible that sensitive data is more vulnerable to disclosure and monitor. Therefore, security and privacy get a large number of concerns [9]–[11], and privacy-perserving challenges faced by IoT system are major problems to be solved.

In order to secure communication between device and the cloud or application programs, information hiding technologies can be applied to approach the concealment and security of communication besides encrypting the transmitted message. The scheme of covert commutation is urgently needed to guarantee the privacy or essential data protection and resist the potential monitor. Steganography scheme refers to a covert communication mode that embeds secret information imperceptibly into carrier and transmits it publicly. By hiding secret information in the public communication media, such

The associate editor coordinating the review of this manuscript and approving it for publication was Patrick Hung.

as image, text, video, audio, etc., it can obtain the secret carrier called stego. In the process of stego transmission, it is a challenge that finding anomalies by the monitor, so that secret information can be covertly transmitted. Therefore, researchers are adopting the steganography approaches to the IoT in attempt to secure communication. Kim *et al.* [12] proposed an anti-reverse-engineering dynamic tamper detection scheme in IoT applications, which realized image information hiding. Li *et al.* [13] proposed a steganography method for IoT using a Maximum Matching Degree sifting algorithm. This method mainly chooses a better cover image which is the most suitable image to embed secret messages by preprocessing. In addition, Chen *et al.* [14] applied a information hiding algorithm to mobile platforms. They introduced an improved image steganography method for secure data transmission from a computer to a mobile phone. In their method, messages could be hidden in an image on the computer using a password, and users can download the image from the computer to a mobile phone. The decoder program will extract hidden information through Java programs on the mobile phone. Later, Shirali-Shahreza *et al.* [15], [16] proposed text and image-based MMS steganography and secret information exchange through abbreviated short message to realize the covert transmission. With the computational power of edge computing in IoT, Cui *et al.* [17] proposed an scheme of foreground object generation by GAN. Thus, the stego for covert communication shall have the ability of undetectable where the ability plays a key role in the steganography approach. At the same time, we need to ensure that there is no perceptible difference between cover and stego, which means that the anti-descent mechanism of stego image quality.

CycleGAN learns a mapping $G : X \rightarrow Y$ from source domain X to target domain Y to perform image transfer [1], that is, to transfer the image style from source domain X to target domain Y. It contains two mappings: $G : X \rightarrow Y$, $F : Y \rightarrow X$. CycleGAN consists of two discriminators and two generators. Each mapping process includes a discriminator and a generator to realize the style migration of images from source domain X to target domain Y. Another mapping implements the style migration of images from target domain Y to source domain X. Because the texture of image has changed in the process of style transfer, and the two mapping processes are a cyclic process, this paper proposes to add secret information in the process of style transfer, which makes a high anti-detection of steganalysis. This paper extends the structure of CycleGAN by adding an information hiding module and a steganalysis module. Secret information is embedded in the process of image-to-image translations, and steganalysis is used to judge and supervise the generated stego image and transferred image, which will achieve secure covert communication under the monitor. The cycle-consistency loss of CycleGAN ensures no obvious abnormality between the style transferred images and stego images. For the extracting terminal, secret information is extracted by the corresponding extraction algorithm.

The main contributions of our work are as follows:

1) The proposed steganography approach makes the anti-detection process of stego images more explicit and effective than embedding on the images trained from scratch. The reason is that the training objective and direction of the stego images are shifted to image-to-image translations.
2) Compared with embedding secret information from scratch in the image generation process of GAN, this method introduces cycle-consistent adversarial training pattern for steganography process, and defines the embedding distortion, so as to improve the quality of stego images.
3) This method is suitable for covert communication of the IoT, that is to communicate secret message covertly over terminals, which makes communication of the IoT platform more covert and secure.

The rest of the paper is organized as follows. In Section II, we introduce the models, technologies and research status related to the proposed method. The basic idea of the proposed scheme is outlined in Section III. Extensive experiments are performed with the contrast results in Section IV to demonstrate the performance of the method proposed in the paper. Conclusions are presented in Section V.

II. RELATED WORKS

A. GENERATIVE ADVERSARIAL NETWORKS

Deep learning has been widely used in classification, object and face detection, forensics and so on [18]–[21]. With the development of deep learning, various algorithms based on CNN have also been proposed and improved. In 2014, Goodfellow *et al.* [22] firstly proposed GAN model to simulate the distribution of generating relatively real computer images to natural images. It contains two basic sub-structures, generator and discriminator. The generator generates images using a convolutional operation through a random input noise. Then the generated image and the real image are fed into the discriminator to classify. Through supervised learning of the features extracted on the real image and the generated image, the discriminator judges whether the distribution of the generated image and the real image satisfies the minimum value of the maximum difference on KL-divergence. The generator will modify the generated image according to the optimal direction of the discriminator until the discriminator can not recognize the generated image correctly at a specific threshold. On the basis of GAN, a series of improved GANs have been further developed. Mirza *et al.* [23] proposed Conditional GAN, which improved the unsupervised generation process to a supervised process. They added constraints to the generator of GAN model, thus providing the given direction for the generation process. WGAN (Wasserstein GAN) proposed by Arjovsky *et al.* [24] solved the problem of instability in the training process of GAN, and proposed effective methods to ensure the diversity of generated samples. On the basis of WGAN, Berthelot *et al.* [25] proposed BEGAN, adding an auto-encoder to the discriminator.

The construction of the encoder was the same as that of the generator with different weights. The proposed model effectively controlled the balance between generator and discriminator, as well as the balance between the diversity and quality of generated samples. Ma *et al.* [26] proposed that DA-GAN is used for instance-level image conversion by translating a text description into an image.

B. IMAGE-TO-IMAGE TRANSLATION

Hertzmann *et al.* [27] proposed that non-parametric texture model for translating an image to another image by image analogies method. Due to the antagonistic characteristics of GAN, it is very suitable to generate natural images. Isola *et al.* [28] put forward the ''pix2pix'' framework by modifying conditional adversarial networks. The framework added a U-Net structure to the generator. In addition, on the basis of adversarial loss, L_1 loss was added to measure the variation between real image and generated image, making it suitable for image-to-image translation, so as to generate the image of the corresponding domain according to the input image. Wang *et al.* [29] realized the generation of high-resolution images on the basis of pix2pix. The SingleGAN proposed by Yu *et al.* [30] was based on multiple GAN. It implemented multi-domain image-to-image translations by using a single generator. In the field of Unpaired Image-to-Image Translation [31]–[33], Zhu *et al.* [1] proposed CycleGAN using cycle-consistent adversarial networks to achieve unpaired image-to-image translation. By transforming the images of different domains into each other, the converted images could also be restored to the pre-converted images. Anoosheh *et al.* [34] proposed RoDayGAN by modifying the image translation model and using the known 6-DOF position of the closest day image, the night driving image was converted into a more meaningful day driving image.

C. STEGANOGRAPHY

Image steganography algorithms use redundant information of the cover image to hide secret information, which is difficult to be detected by the monitor. It is achieved that transmitting secret information over the public transmission of the stego image. In the early days, the most widely used method is the least significant bit (LSB) replacement. Information hiding is accomplished by embedding secret information directly into the least significant bit of image pixels. Although the LSB algorithm has large hiding capacity and is easy to extract and operate, its robustness and anti-detectability is not strong. In order to improve the robustness of stego images, boosted steganography scheme (BSS) was proposed by Sajedi and Jamzad [35]. It had a preprocessing stage to select a cover image from a database before applying steganography methods. And the experimental results showed that the scheme could significantly improve the steganography security. Content adaptive algorithms are mainly designed based on the theory of minimizing distortion, such as S-UNIWARD [36], WOW [37], HUGO [38] and so on. This kind of algorithm calculates the image distortion after embedding secret messages by defining a distortion cost function and gives the recommended value that each unit can be embedded. The stego image is completed after hiding the secret message over the unit suitable for embedding.

Due to deep neural network can extract the deep features of images, the information hiding algorithm based on deep learning has developed to a certain extent. Baluja [39] proposed to use neural networks to find the appropriate location to embed secret images in the cover images. By training an encoder network to embed secret images, they could be dispersed in every bit of the image unit, rather than embed in one bit of a unit. At the same time, the model also trained a decoder network, which could extract secret images from the stego images. Meng *et al.* [40] proposed the use of object detection method to select the object area in cover images as the safe area for steganography. They proved that the security of steganography was increased by hiding secret information in a secure well-textured region. Meng *et al.* [41] proposed that combining coverless information hiding and steganography in [40], so as to increase the payloads. Zhang *et al.* [42] proposed a steganographic algorithm to invalidate steganalysis networks based on deep learning. This method used the gradient in the training process of the deep learning model to add specific noise to the cover image to obtain the enhanced cover image so that it could ''mislead'' the classification of the deep learning (make the stego image recognized as cover image). Then the traditional adaptive steganography framework was used to realize information embedding on the enhanced cover image.

In addition, the application of information hiding in GAN has been extensively studied due to the similarity of confrontation characteristics between the generator and discriminator in GAN and steganography and steganalysis in information hiding [43]. Volkhonskiy *et al.* [44] proposed a GAN-based steganography model named SGAN in 2017. On the basis of GAN, this model added a new discriminator named steganalysis, which was used to discriminate on the generated stego images during training process to make the final generated stego images can resist steganalysis. On the basis of SGAN, Shi *et al.* [45] proposed an improved steganographic model SSGAN based on GAN model, whose model structure was similar to that of SGAN. WGAN (Wasserstein GAN) [24] was adopted in SSGAN to replace DCGAN [46]. It achieved faster training speed and higher image quality. In addition, the steganalysis was replaced by GNCNN [47]. Through the confrontation between GNCNN and generator, the image generated by GAN was more suitable for steganography. When CycleGAN was proposed, although the problem of unpaired image-to-image translation was solved, there were also some problems. Chu *et al.* [48] pointed out that CycleGAN could hide part of the input data and then restored the hidden data at the time of output, which could be used for information hiding. Tang *et al.* [49] proposed the ADV-EMB steganographic scheme, which adjusted the cost of image modification according to the gradient

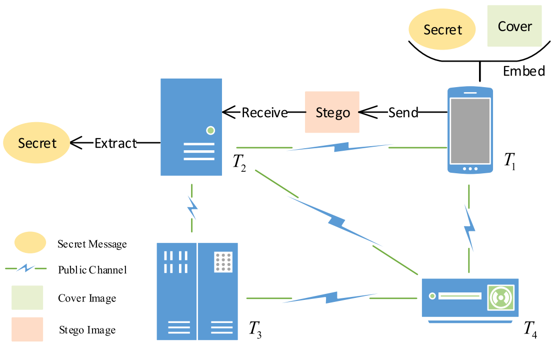

FIGURE 1. An instance of covert communication between terminals in the IoT.

returned by the target CNN steganalyzer, so as to hide secret message and deceive CNN-based steganalysis at the same time.

III. THE PROPOSED S-CYCLEGAN STEGANOGRAPHIC SCHEME

In this section, we propose a novel steganographic scheme, called S-CycleGAN. As illustrated in Figure 1, an instance of covert communication between terminals in the IoT with public channel is presented. Here, T_1, T_2, T_3 and T_4 are terminals in the IoT. The covert communication exists on T_1 and T_2. T_1 hides secret messages in a cover image by the proposed steganography algorithm, and sends the stego image with secret messages to T_2. T_2 extracts secret messages by extraction algorithm. The steganographic scheme adds steganography module and steganalysis module based on CycleGAN.

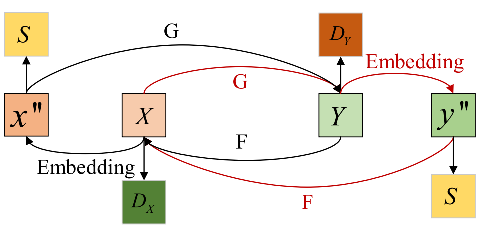

FIGURE 2. The structure of S-CycleGAN.

As illustrated in Figure 2, our model includes two cycles $Embedding : (G : X \rightarrow Y) \rightarrow y'', F : y'' \rightarrow X$ and $Embedding : (F : Y \rightarrow X) \rightarrow x'', G : x'' \rightarrow Y$. Among them, X and Y represent two domains respectively, x'' and y'' represent stego images. In addition, there are three discriminators D_X, D_Y and S, where the functions of D_X and D_Y are same as those of D_X and D_Y in CycleGAN. D_X and D_Y are used to distinguish the generated image from the target domain image. S is the increased steganalysis module, which is used to distinguish stego images from generated images. Through the confrontation between steganalysis and generator, the concealment and robustness of the steganographic image are improved.

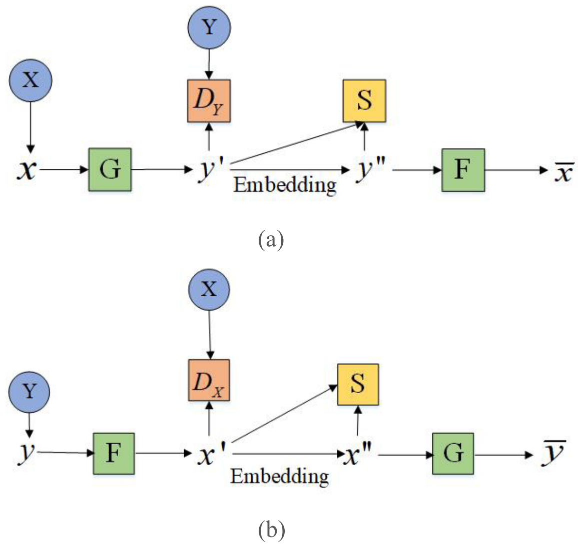

FIGURE 3. The detailed processes of S-CycleGAN, (a) is the transformation and steganography process from X domain to Y domain, (b) is the transformation and steganography process from Y domain to X domain.

In the proposed scheme, we hope to carry out information hiding in the process of translating the image from X-domain into the style image of the Y-domain, so as to achieve high-quality image transformation and the stego image can resist steganalysis at the same time. The scheme that includes three phases, as shown in Figure 3(a). In the first stage, the X-domain image is transformed into the Y-domain style image by generator G, that is, y'. The real image $y(y \in Y)$ and the generated image y' are distinguished by D_Y. If the difference can be judged, the generator will adjust the distribution of the generated image until it can fool D_Y. The second stage is the steganography of secret messages. By using the LSB matching steganography algorithm to embed the secret messages into the generated image y', the stego image is obtained as y''. The inputs of steganalysis S are the stego images as fake images and the generated images as real images. Steganalysis S aims to maximize the difference between the stego image and the generated image. When S distinguishes stego image and generated image, generator will adjust the distribution of y' until it can fool S after it being embedded secret messages. Thus, a high quality stego image that can resist steganalysis is obtained. In the third stage, the stego image can be reconstructed to the input image of the generator G by generator F, that is, the generated $\bar{x}$ and x are as similar as possible. The transformation and steganography process from Y-domain to X-domain is similar to the transformation and steganography process from X-domain to Y-domain, as shown in Figure 3(b).

In the beginning of training process, converting the image x from domain A into the image y' that the image style is the style in domain B, and y' is fed to the discriminator of CycleGAN. Then, the random binary string with length of $3 \times H \times W$ (payload $= 1$), where H and W denotes the height and width of the pixels in y' is embedded in y' and output y'' to simulate the process of embedding the secret message.

Algorithm 1 The Embedding Algorithm Applied in the Proposed S-CycleGAN

Input: The Image x belong to domain X and the secret message M_{secret}
Output: The stego y'' belong to domain Y

Transfering by the trained *Model:* $x \rightarrow y'$
Embedding the M_{secret} into y':
for $i \leftarrow 1$ *to* *lenth*(M_{secret}) **do**
  if $LSB(y'(i)) == LSB(M_{secret}(i))$ **then**
    pass
  else if $y'(i) == 0$ **then**
    $y'(i) += 1$
  else if $y'(i) == 255$ **then**
    $y'(i) -= 1$
  else
    $y'(i) += randomInt\ (0, 1)$
return y' *as* y''

After the steganalysis discriminates y'', the updated gradients are transmitted to the generator. Repeat the process until the training is completed.

In the scenario of implementing the trained model, we will get the stego by carring out Algorithm 1. In the proposed method, we mainly design adversarial loss, cycle consistency loss and full objective function.

A. ADVERSARIAL LOSS SETTING

For cyclic *Embedding* : $(G : X \rightarrow Y) \rightarrow y'', F : y'' \rightarrow X$, their discriminators are D_Y and S. We design adversarial loss as shown in Formula (1).

$$\begin{aligned} &L_{GAN}\left(G, S, D_Y, X, Y\right) \\ &= \partial\left(\left(E_{y\sim P_{data}(y)}\left[\log D_Y(y)\right]\right) + E_{x\sim P_{data}(x)}\left[1 - D_Y\left(G\left(x\right)\right)\right]\right) \\ &\quad + \left(1-\partial\right) E_{x\sim P_{data}(x)}\left[\log S\left(G\left(x\right)\right)\right. \\ &\quad + \left.\log\left(1 - S\left(Emb\left(G\left(x\right)\right)\right)\right)\right] \rightarrow \min_{G}\max_{D_Y}\max_{S} \end{aligned} \tag{1}$$

Among them, $P_{data}(y)$ and $P_{data}(x)$ denote the distributions of real images in Y-domain and X-domain, D_Y and S are discriminator and steganalysis module respectively, and $Emb\left(G\left(x\right)\right)$ is the stego image after embedding secret information into the generated image. The purpose of generator G is to make the distribution of generated image $G\left(x\right)$ as close as possible to that of image in Y domain. $D_Y(G(x))$ means that the discriminator D_Y is to distinguish the difference between the generated image $G\left(x\right)$ and the real image y in the Y domain. The purpose of discriminator S is to judge the difference between the distribution of stego image $Emb\left(G\left(x\right)\right)$ and that of generated image $G\left(x\right)$ as far as possible. The discriminator D_Y and steganalysis S are trained to maximize them. ∂ is the weighting term.

For cyclic *Embedding* : $(F : Y \rightarrow X) \rightarrow x'', G : x'' \rightarrow Y$, their discriminators are D_X and S. We design adversarial loss as shown in Formula (2).

$$\begin{aligned} &L_{GAN}\left(F, S, D_X, X, Y\right) \\ &= \partial\left(\left(E_{x\sim P_{data}(x)}\left[\log D_X(x)\right]\right) + E_{y\sim P_{data}(y)}\left[1 - D_X\left(F\left(y\right)\right)\right]\right) \\ &\quad + \left(1-\partial\right) E_{y\sim P_{data}(y)}\left[\log S\left(F\left(y\right)\right)\right. \\ &\quad + \left.\log\left(1 - S\left(Emb\left(F\left(y\right)\right)\right)\right)\right] \rightarrow \min_{F}\max_{D_X}\max_{S} \end{aligned} \tag{2}$$

where F is the generator to make the distribution of generated image $F\left(y\right)$ as close as possible to that of image in X domain. D_X and S denote the discriminator and steanalysis module respectively. $Emb\left(F\left(y\right)\right)$ is the stego image embedded with the secret message.

B. CYCLE CONSISTENCY LOSS FOR STEGANOGRAPHY

There are two cycles in our model. One cycle is to transform the X-domain style image into the Y-domain style image, and then hide the messages to get the stego image y''. Next, y'' is reconstructed to X-domain style image through generator F, that is, $\bar{x}$. That is, cycle: Embedding: (G: X-Y)-y'' , F: y''-X. Another cycle is to transform the Y-domain style image into the X-domain style image by generator F, that is, x', and then hide the messages from x' to get the stego image x''. Next generator G is aimed to reconstructed x'' into the image with the same distribution as the input image of generator F, that is, $\bar{y}$. The difference with CycleGAN is that we reconstructed the stego image to the input image instead of reconstructing the generated image directly. Cycle consistency loss shows as Formula (3). For image x transferring from X-domain to Y-domain, G and F should satisfy backward cycle consistency: $x \rightarrow G(x) \rightarrow Emb(G(x)) \rightarrow F(Emb(G(x))) \approx y$. For image y from Y-domain, the cycle consistency is $y \rightarrow F(y) \rightarrow Emb(F(y)) \rightarrow G(Emb(F(y))) \approx y$.

$$\begin{aligned} L_{cyc}(G, F) = &E_{x\sim P_{data}(x)}\left[\| F\left(Emb\left(G\left(x\right)\right)\right) - x \|_1\right] \\ &+ E_{y\sim P_{data}(y)}\left[\| G\left(Emb\left(F\left(y\right)\right)\right) - y \|_1\right] \end{aligned} \tag{3}$$

C. FULL OBJECTIVE FUNCTION

The full object function is shown in Formula (4). It contains two cycles of adversarial losses those are $L_{GAN}(G, S, D_Y, X, Y)$ and $L_{GAN}(F, S, D_X, X, Y)$ and a cycle consistency loss that is $L_{cyc}(G, F)$.

$$\begin{aligned} L\left(G, F, S, D_X, D_Y\right) = &L_{GAN}\left(G, S, D_Y, X, Y\right) \\ &+ L_{GAN}\left(F, S, D_X, X, Y\right) + \lambda L_{cyc}(G, F) \end{aligned} \tag{4}$$

IV. EXPERIMENTS

In order to evaluate the performance of the proposed S-CycleGAN scheme, we conducted the following experiments.

1) Adding steganalysis and steganographic module to CycleGAN, that is, the proposed method S-CycleGAN.

The S-CycleGAN model is trained to generate stego images. It will be showed in Section IV-B.

2) SGAN [44] is used as the one of baselines. We use the same datasets of S-CycleGAN to generate the stego images for SGAN. It will be reported in Section IV-B.
3) Using the Freìchet Inception Distance (FID) [50] and Inception score (IS) [51] to evaluate the image quality of two sets of stego images generated by two steganographic algorithms. It will be demonstrated in Section IV-C.
4) We add S-UNIWARD steganography which embeds the message directly into translated image by CycleGAN as the other baseline for steganalysis. The datasets are the same as S-CycleGAN model's datasets. Steganalysis algorithms SPA and SRM are used to analyze the three groups of stego images obtained by SGAN, S-CycleGAN and CycleGAN with S-UNIWARD steganographic algorithms, so as to compare the concealment of these stego images. It will be demonstrated in Section IV-D.
5) The instance of implementing the process of embedding and extraction with the real secret messages is shown in Section IV-E.

The common settings, hardware environment and notations in the experiments will be described in Section IV-A.

A. SETTING

1) IMAGE SET

To evaluate the proposed methods, we conducted experiments on the datasets in CycleGAN [1]. Among them, the data sets Horse2Zebra and Apple2Orange are sampled from LSVRC2012 (ImageNet) dataset. To simulate secret data embedding during the variation of landscape images, we chose Summer2Winter dataset for translation. Meanwhile, we select to train on the Photo2Monet dataset to implement the embedding of secret information in the style transfer process. The details of each dataset are shown in Table 1. We select the image in training set for training. At the same time, when testing performance, we select the image in the test set.

TABLE 1. Number of images in each data set.

	Training set	Test set
Apple2Orange	2014	514
Horse2Zebra	2401	260
Summer2Winter	2193	547
Photo2Monet	7359	872

2) HARDWARE ENVIRONMENT

All experiments in this paper are performed on NVIDIA 1080Ti GeForce GPU and Intel i7-6900K CPU. The employed framework is TensorFlow with Python.

3) NOTATIONS

In the experiments, the name of the dataset indicates the transformed style of S-CycleGAN or the target class of SGAN.

B. TRAINING PROCESS AND RESULTS

By default, the learning rate is set to 0.0002 with update parameters $\beta_1 = 0.5$, $\beta_2 = 0.999$ in the training process of S-CycleGAN and SGAN. We choose Adam as the optimization function with momentum of 0.5. The weight of the regulation term in S-CycleGAN is set to 10. Refer to the setting of CycleGAN, generative network consists of 9 residual blocks with instance normalization [52] for data normalization during style transferring. In S-CycleGAN, Instance Normalization is not set up in the first layer of the discriminant networks and stegannalysis networks, and leacky Relu with 0.2 is added in the next three layers. In addition, the steganalysis network refers to Xu-Net [53]. After data feeding, the high-pass convolutional kernel is added to extract weak embedded features, and the extracted features are used for steganalysis. In the training process, we will simulate secret information as random binary codes of the same scale as the pixels of the input image. The output stego images are derived from the generated images with size of 256×256. Then the embedded binary code length is $256 \times 256 \times 3$, i.e. the payload is 1.

Some experimental results are shown in Figure 4. Stego images generated on apple, orange, horse, zebra, summer, winter, monet and photo datasets by steganography algorithm S-CycleGAN and SGAN, respectively. Through the display and comparison of some experimental results, we can clearly see that stego images generated by S-CycleGAN are of much higher image quality than those generated by SGAN.

C. EVALUATING STEGO QUALITY

We selected different evaluation metrics to evaluate the image quality. First, we select the classification model Inception V3 [59] on ImageNet [60], and use Inception Score (IS) as the quantitative evaluation index. By computing the KL-divergence between the distributions of the target class and the generated class, the IS measures the distance between the two probability distributions. The larger the value of IS, the smaller the discrepancy representing this distribution, then the quality of the generated image is better. However, there are some limitations of IS [54]. Due to the sensitivity to weights in the neural network and the high dependence on the category of samples, IS has certain restrictions on the evaluation of generated images.

The experimental results are shown in Table 2 and Figure 5. Besides the horse data set, the IS value of stego image generated by S-CycleGAN IS higher than that of stego image generated by SGAN. In particular, the IS value of the image generated by S-CycleGAN is 2.6 times higher than that of the image generated by SGAN in the comparison experiment of Monet data set. It shows that the image distribution generated by the method of S-CycleGAN proposed in this paper is

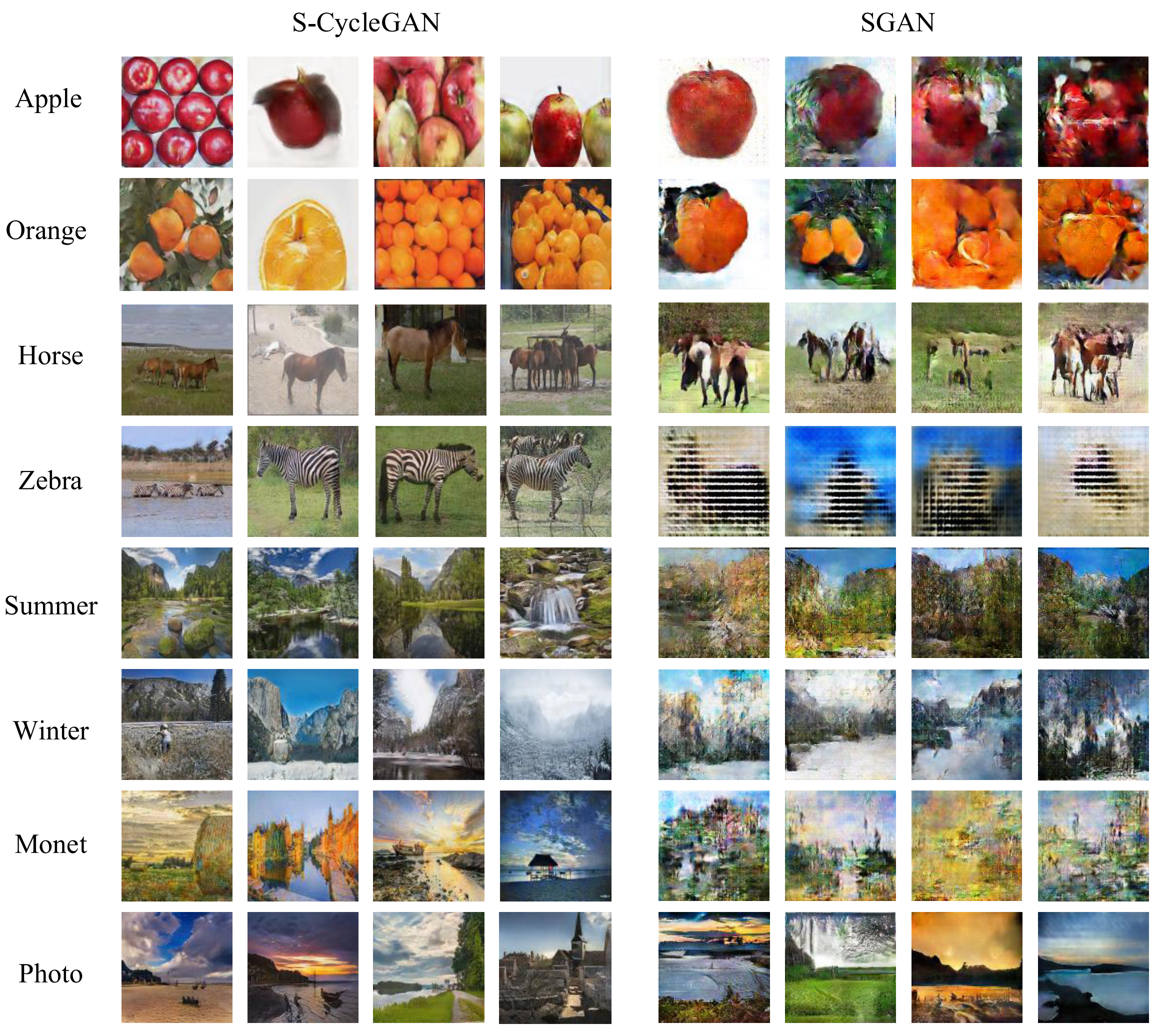

FIGURE 4. The comparison of two sets of stego images by S-CycleGAN steganography and SGAN steganography algorithm.

TABLE 2. Inception score of the generated stego images by S-CycleGAN and SGAN.

	S-CycleGAN	SGAN
Apple	5.22	3.88
Orange	4.63	4.33
Horse	3.66	4.45
Zebra	1.58	1.45
Monet	5.44	2.11
Photo	3.75	3.06
Summer	2.48	2.03
Winter	2.51	2.00
Average	3.66	2.91

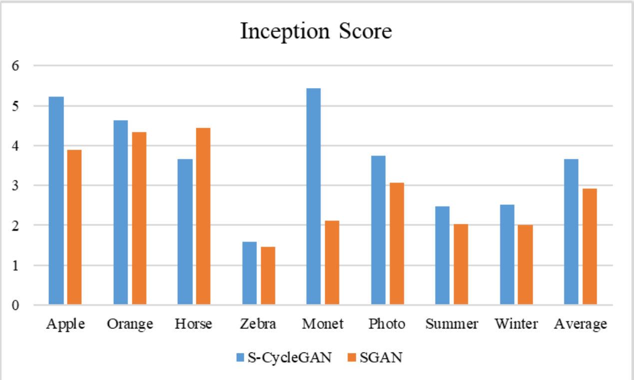

FIGURE 5. The comparison of stego images generated by S-CycleGAN and SGAN in IS evaluationS-.

closer to the natural distribution than that of SGAN, and the diversity effect of S-CycleGAN is better.

To solve the limitation of IS in the evaluation of image quality, FID is used as another evaluation metric for all generated data. FID calculates the Wasserstein-2 distance between the generated data and the real data using Inception-v3 measurement. A lower FID value indicates a closer distance between the two distributions, which indicates the better image quality. FID is more robust to noise than IS. In addition, FID shows a closer approximation to the human vision system [50]. Therefore, we believe that FID shows the quality of generated images more effectively.

TABLE 3. Fréchet inception distance of the generated stego images by S-CycleGAN and SGAN.

	S-CycleGAN	SGAN
Apple	112.78	267.36
Orange	135.30	313.63
Horse	51.54	112.41
Zebra	44.33	308.15
Monet	53.03	203.36
Photo	54.62	59.75
Summer	50.02	131.82
Winter	58.77	157.41
Average	70.05	194.24

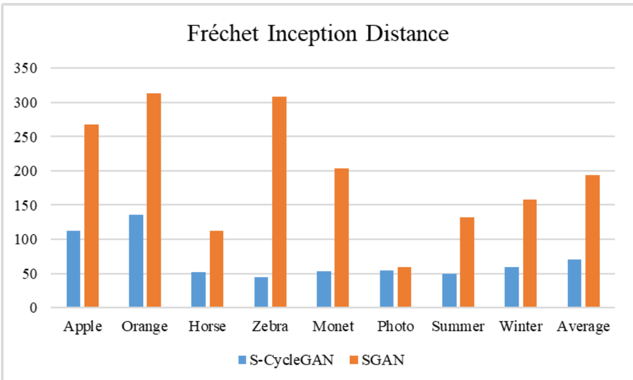

FIGURE 6. The comparison of stego images generated by S-CycleGAN and SGAN in FID evaluation.

The comparative experiment results of FID are shown in Table 3 and Figure 6. The images generated by S-CycleGAN are all higher than those generated by SGAN under the evaluation standard of FID. The maximum FID value of stego image generated by S-CycleGAN can be approximately 7 times that of the FID value of stego image generated by SGAN. The FID experiment further proves that the quality of generated stego image of S-CycleGAN proposed in this paper is better than that of SGAN.

Due to the high efficiency of CycleGAN in domain transfer, S-CycleGAN has advantages when the training set is insufficient. Compared with SGAN, the image quality of S-CycleGAN is obviously better, such as zebra, horse, apple and orange. SGAN cannot effectively simulate the real data distribution when the training data is insufficient. In the case of training with sufficient training samples, although SGAN can generate images with high image quality, the image integrity of the image content is low, and it is easy to be perceived as computer-generated images.

D. EVALUATING PERFORMANCE ON STEGANALYSIS

At first, sample pair analysis (SPA) [55], a steganalysis method targeting at LSB stego steganography, is used to estimate the performance of stego. Secondly, we use Spatial Rich Model (SRM) [56] which is widely used to perform steganalysis. Meanwhile, Ensemble Classifiers [56] are used as the classifier. We use the trained model, which is provided from [57], as the pre-trained model for classification,. The model is trained on the BOSSBase v1.01 [58] dataset, whose number of images is 10,000, and the training set and test set account for 70% and 30% respectively. The high anti-detection rate of stego image by steganalysis reflects the concealment of secret information.

TABLE 4. The anti-detection rate of sample pair analysis.

	S-CycleGAN	SGAN	CycleGAN+S-UNIWARD
Apple	0.996	0.919	0.970
Orange	1.000	0.995	0.968
Horse	1.000	0.955	0.993
Zebra	0.997	0.956	0.975
Monet	1.000	0.855	0.993
Photo	1.000	0.950	0.975
Summer	1.000	0.891	0.991
Winter	1.000	0.895	0.996
Average	0.999	0.927	0.983

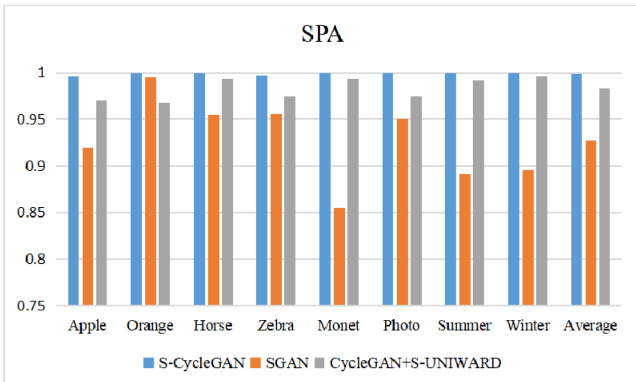

FIGURE 7. The comparison of anti-detection rate of stego images generated by S-CycleGAN, SGAN and CycleGAN with S-UNIWARD in SPA.

In order to compare the performance of the proposed method, we add S-UNIWARD steganography with payload of 1 which embeds the message directly into translated image as comparison. Table 4 and Figure 7 show the results of SPA steganalysis algorithm on the stego images obtained by S-CycleGAN, SGAN and CycleGAN with S-UNIWARD algorithm. The results are the anti-detection rate of stego images. As can be seen from Table 4 and Figure 7, stego images generated by S-CycleGAN can escape SPA detection with the highest accuracy. Moreover, the results on S-CycleGAN are significantly better than those on SGAN, and the results on S-CycleGAN are slight better than those on CycleGAN with S-UNIWARD. The data with an anti-detection rate of 1 in the detection result indicates that stego images can completely resist SPA detection, which proves that the cycle-consistent loss of S-CycleGAN in training can help maximize the tolerance of cover image modification.

In addition to the SPA steganalysis, we use a more typical steganalysis algorithm SRM. The algorithm contains a variety

TABLE 5. The anti-detection rate of spatial rich model steganalysis.

	S-CycleGAN	SGAN	CycleGAN+S-UNIWARD
Apple	0.50	0.04	0.12
Orange	0.38	0.01	0.04
Horse	0.87	0.13	0.60
Zebra	0.97	0.42	0.75
Monet	0.66	0.61	0.18
Photo	0.99	0.06	0.48
Summer	0.97	0.24	0.68
Winter	0.99	0.34	0.60
Average	0.791	0.231	0.431

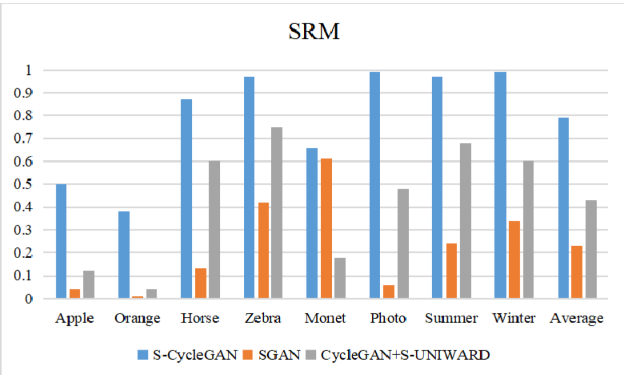

FIGURE 8. The comparison of anti-detection rate of stego images generated by S-CycleGAN, SGAN and CycleGAN with S-UNIWARD in SRM.

of spatial high-pass filtersthose are used to filter the image, so as to obtain rich residual image. The cooccurrence matrix is calculated according to the residual image as the steganalysis feature of the stego image. Table 5 and Figure 8 show the steganalysis results of SRM steganalysis algorithm on the three group of stego images. By analyzing the data, we can see that the anti-detection rate of the stego images generated by the proposed S-CycleGAN is higher than that of the stego images obtained by the SGAN and CycleGAN with S-UNIWARD. has The average anti-detection rate of the stego image generated by SGAN algorithm is 0.231. The average anti-detection result of CycleGAN with S-UNIWARD 0.431. But steganography algorithm S-CycleGAN generated stego image anti-detection rate is up to 0.99, the lowest is 0.38, the average anti-detection rate is 0.791. The average anti-detection rate of stego images generated by S-CycleGAN is 3.4 times and 1.8 times higher than those of stego images generated by SGAN and CycleGAN with S-UNIWARD. Thus, the stego images generated by S-CycleGAN are more suitable for steganography than those generated by SGAN and CycleGAN with S-UNIWARD.

E. EMBEDDING AND EXTRACTION

When an image is input, the transferred image is generated according to the pre-trained model, and secret information is embedded in the process by LSB Matching algorithm. For stego images, secret information can be obtained by

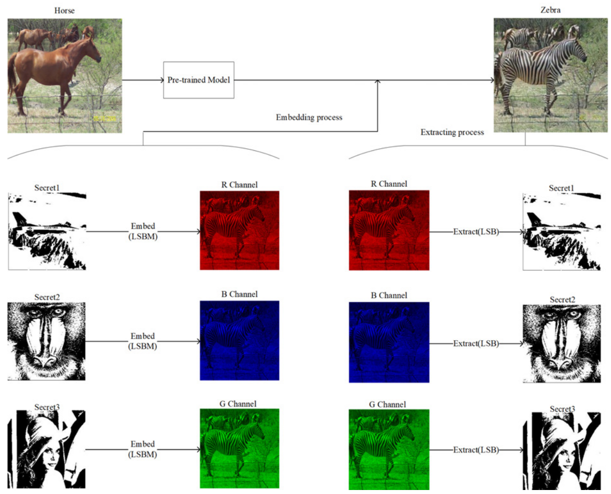

FIGURE 9. The illustration of the embedding process and the extraction process.

extracting each minimum effective bit. Figure 9 shows an specific procedure of the transmission of the secret message and shows the results of extraction.

V. CONCLUSIONS

In this paper, we proposed a novel approach named S-CycleGAN to embed secret messages in the process of image-to-image translation. This approach mainly adds steganography module and steganalysis module on the basis of CycleGAN. Steganalysis module is used to counteract the generated stego images, which makes the generated stego images more secure. By the facilitation of cycle consistency loss, the stego images generated by the proposed method will be close to the cover images effectively. Through the analysis of several experimental data, it is proved that the proposed S-CycleGAN not only guarantees the quality of stego images, but also makes the stego images more resistant to detection, and realizes the concealment and security in the transmission process. The method is adapted to solve the security of IoT communication and realize the secret communication between terminals.

REFERENCES

[1] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *Proc. IEEE Int. Conf. Comput. Vis.*, Oct. 2017, pp. 2242–2251.

[2] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, "SIGMM: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2019. doi: 10.1109/TII.2018.2799907.

[3] A. Kamilaris and A. Pitsillides, "Mobile phone computing and the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 885–898, Dec. 2016.

[4] T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[5] S. Moeller, A. Sridharan, B. Krishnamachari, and O. Gnawali, "Backpressure routing made practical," in *Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops*, Mar. 2010, pp. 1–2.

[6] R. Laufer, T. Salonidis, H. Lundgren, and P. Le Guyadec, "A cross-layer backpressure architecture for wireless multihop networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 2, pp. 363–376, Apr. 2014.

[7] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.

[8] Y. Xu, L. Qi, W. Dou, and J. Yu, "Privacy-preserving and scalable service recommendation based on SimHash in a distributed cloud environment," *Complexity*, vol. 2017, Art. no. 3437854, Nov. 2017. doi: 10.1155/2017/3437854.

[9] L. Qi, R. Wang, C. Hu, S. Li, Q. He, and X. Xu, "Time-aware distributed service recommendation with privacy-preservation," *Inf. Sci.*, vol. 480, pp. 354–364, Apr. 2018.

[10] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang, and R. Bie, "A secure and verifiable access control scheme for big data storage in clouds," *IEEE Trans. Big data*, vol. 4, no. 3, pp. 341–355, Sep. 2018.

[11] L. Qi, S. Meng, X. Zhang, R. Wang, X. Xu, Z. Zhou, and W. Dou, "An exception handling approach for privacy-preserving service recommendation failure in a cloud environment," *Sensors*, vol. 18, no. 7, p. 2037, 2018.

[12] S. R. Kim, J. N. Kim, S. T. Kim, S. Shin, and J. H. Yi, "Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications," *J. Supercomputing*, vol. 74, no. 9, pp. 4261–4280, 2018.

[13] H. Li, L. Hu, J. Chu, L. Chi, and H. Li, "The maximum matching degree sifting algorithm for steganography pretreatment applied to IoT," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18203–18221, 2018.

[14] Y.-F. Chen, T. Li, D.-N. Gao, X.-Q. Hu, X.-P. Zhang, and J. Liu, "A secure mobile communication approach based on information hiding," in *Proc. 2nd Asia Pacific Conf. Mobile Technol., Appl. Syst.*, Guangzhou, China, Nov. 2005, p. 5. doi: 10.1109/MTAS.2005.243754.

[15] M. Shirali-Shahreza, "Steganography in MMS," in *Proc. IEEE Int. Multitopic Conf.*, Dec. 2007, pp. 1–4.

[16] M. Shirali-Shahreza and M. H. Shirali-Shahreza, "Text steganography in SMS," in *Proc. Int. Conf. Converg. Inf. Technol. (ICCIT)*, Nov. 2007, pp. 2260–2265.

[17] Q. Cui, Z. Zhou, Z. Fu, R. Meng, X. Sun, and Q. M. J. Wu, "Image steganography based on foreground object generation by generative adversarial networks in mobile edge computing with Internet of Things," *IEEE Access*, to be published. doi: 10.1109/ACCESS.2019.2913895.

[18] R. Gurusamy and V. Subramaniam, "A machine learning approach for MRI brain tumor classification," *Comput., Mater. Continua*, vol. 53, no. 2, pp. 91–108, 2017.

[19] C. Li, Y. Jiang, and M. Cheslyar, "Embedding image through generated intermediate medium using deep convolutional generative adversarial network," *Comput., Mater. Continua*, vol. 56, no. 2, pp. 313–324, 2018.

[20] C. Yuan, X. Li, Q. Wu, J. Li, and X. Sun, "Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis," *Comput., Mater. Continua*, vol. 53, no. 4, pp. 357–371, 2017.

[21] Q. Cui, S. Mcintosh, and H. Sun, "Identifying materials of photographic images and photorealistic computer generated graphics based on deep cnns," *Comput. Mater. Continua*, vol. 55, no. 2, pp. 229–241, 2018.

[22] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. Adv. Neural Inf. Process. Syst.*, 2014, pp. 2672–2680.

[23] M. Mirza and S. Osindero, "Conditional generative adversarial nets," 2014, *arXiv:1411.1784*. [Online]. Available: https://arxiv.org/abs/1411.1784

[24] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein GAN," 2017, *arXiv:1701.07875*. [Online]. Available: https://arxiv.org/abs/1701.07875

[25] D. Berthelot, T. Schumm, and L. Metz, "Began: Boundary equilibrium generative adversarial networks," 2017, *arXiv:1703.10717*. [Online]. Available: https://arxiv.org/abs/1703.10717

[26] S. Ma, J. Fu, C. W. Chen, and T. Mei, "DA-GAN: Instance-level image translation by deep attention generative adversarial networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 5657–5666.

[27] A. Hertzmann, C. E. Jacobs, N. Oliver, B. Curless, and D. H. Salesin, "Image analogies," in *Proc. 28th Annu. Conf. Comput. Graph. Interact. Techn.*, 2001, pp. 327–340.

[28] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, "Image-to-image translation with conditional adversarial networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jul. 2017, pp. 1125–1134.

[29] T.-C. Wang, M.-Y. Liu, J.-Y. Zhu, A. Tao, J. Kautz, and B. Catanzaro, "High-resolution image synthesis and semantic manipulation with conditional GANs," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 8798–8807.

[30] X. Yu, X. Cai, Z. Ying, T. Li, and G. Li, "SingleGAN: Image-to-image translation by a single-generator network using multiple generative adversarial learning," 2018, *arXiv:1810.04991*. [Online]. Available: https://arxiv.org/abs/1810.04991

[31] A. Anoosheh, E. Agustsson, R. Timofte, and L. Van Gool, "ComboGAN: Unrestrained scalability for image domain translation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2018, pp. 783–790.

[32] Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, and J. Choo, "StarGAN: Unified generative adversarial networks for multi-domain image-to-image translation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 8789–8797.

[33] A. Ignatov, N. Kobyshev, R. Timofte, K. Vanhoey, and L. Van Gool, "WESPE: Weakly supervised photo enhancer for digital cameras," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2018, pp. 691–700.

[34] A. Anoosheh, T. Sattler, R. Timofte, M. Pollefeys, and L. Van Gool, "Night-to-day image translation for retrieval-based localization," 2018, *arXiv:1809.09767*. [Online]. Available: https://arxiv.org/abs/1809.09767

[35] H. Sajedi and M. Jamzad, "BSS: Boosted steganography scheme with cover image preprocessing," *Expert Syst. Appl.*, vol. 37, no. 12, pp. 7703–7710, 2010.

[36] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 2014, p. 1, Jan. 2014. doi: 10.1186/1687-417X-2014-1.

[37] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, vol. 2, Dec. 2012, pp. 234–239.

[38] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, Berlin, Germany, 2010, pp. 161–177.

[39] S. Baluja, "Hiding images in plain sight: Deep steganography," in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 2069–2079.

[40] R. Meng, S. G. Rice, J. Wang, and X. Sun, "A fusion steganographic algorithm based on faster R-CNN," *CMC, Comput., Mater. Continua*, vol. 55, no. 1, pp. 1–16, 2018.

[41] R. Meng, Z. Zhou, Q. Cui, X. Sun, and C. Yuan, "A novel steganography scheme combining coverless information hiding and steganography," *J. Inf. Hiding Privarcy Protection*, vol. 1, no. 1, pp. 43–48, 2019.

[42] Y. Zhang, W. Zhang, K. Chen, J. Liu, Y. Liu, and N. Yu, "Adversarial examples against deep neural network based steganalysis," in *Proc. 6th ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2018, pp. 67–72.

[43] R. Meng, Q. Cui, and C. Yuan, "A survey of image information hiding algorithms based on deep learning," *Comput. Model. Eng. Sci.*, vol. 117, no. 3, pp. 425–454, 2018.

[44] D. Volkhonskiy, I. Nazarov, B. Borisenko, and E. Burnaev, "Steganographic generative adversarial networks," 2017, *arXiv:1703.05502*. [Online]. Available: https://arxiv.org/abs/1703.05502

[45] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks," in *Proc. Pacific Rim Conf. Multimedia*. Cham, Switzerland: Springer, 2017, pp. 534–544.

[46] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," 2015, *arXiv:1511.06434*. [Online]. Available: https://arxiv.org/abs/1511.06434

[47] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis via convolutional neural networks," *Proc. SPIE*, vol. 9409, Mar. 2015, Art. no. 94090J.

[48] C. Chu, A. Zhmoginov, and M. Sandler, "CycleGAN, a master of steganography," 2017, *arXiv:1712.02950*. [Online]. Available: https://arxiv.org/abs/1712.02950

[49] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based Adversarial Embedding for Image Steganography," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2074–2087, Aug. 2019. doi: 10.1109/TIFS.2019.2891237.

[50] M. Heusel, H. Ramsauer, T. Unterthiner, B. Nessler, and S. Hochreiter, "GANs trained by a two time-scale update rule converge to a local nash equilibrium," in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 6626–6637.

[51] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, "Improved techniques for training GANs," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 2234–2242.

[52] D. Ulyanov, A. Vedaldi, and V. Lempitsky, "Instance normalization: The missing ingredient for fast stylization," 2016, *arXiv:1607.08022*. [Online]. Available: https://arxiv.org/abs/1607.08022
[53] G. Xu, H. Z. Wu, and Y. Q. Shi, "Ensemble of CNNs for steganalysis: An empirical study," in *Proc. 4th ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2016, pp. 103–107.
[54] S. Barratt and R. Sharma, "A note on the inception score," 2018, *arXiv:1801.01973*. [Online]. Available: https://arxiv.org/abs/1801.01973
[55] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, Oct. 2002, pp. 355–372.
[56] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[57] D. Lerch. *Aletheia*. Accessed: Aug. 9, 2018. [Online]. Available: https://github.com/daniellerch/aletheia
[58] P. Bas, T. Filler, and T. Pevný, "'Break our steganographic system': The ins and outs of organizing BOSS," in *Proc. Int. Workshop Inf. Hiding* Berlin, Germany: Springer, May 2011, pp. 59–70.
[59] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2016, pp. 2818–2826.
[60] J. Deng, W. Dong, R. Socher, L.-J. Li, and K. Li, "ImageNet: A large-scale hierarchical image database," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2009, pp. 248–255.

RUOHAN MENG received the B.S. degree in software engineering from Nanjing University of Information Science and Technology, China, in 2018, where she is currently pursuing the Ph.D. degree in information and communication engineering. Her research interests include deep learning, information hiding, covert communication, and data security.

QI CUI received the B.S. degree in software engineering from Nanjing University of Information Science and Technology, China, in 2017, where he is currently pursuing the Ph.D. degree in information and communication engineering. His research interests include deep learning, information hiding, steganalysis, data mining, and network security.

ZHILI ZHOU received the B.S. degree in communication engineering from Hubei University, in 2007, and the M.S. and Ph.D. degrees in computer application from the School of Information Science and Engineering, Hunan University, in 2010 and 2014, respectively.

He joined Nanjing University of Information Science and Technology, China, as an Assistant Professor, in 2014. He is currently a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. His current research interests include near-duplicate image/video retrieval, image search, image/video copy detection, coverless information hiding, digital forensics, and image processing.

ZHANGJIE FU received the Ph.D. degree in computer science from the College of Computer, Hunan University, China, in 2012. He was a Visiting Scholar of computer science and engineering at the State University of New York at Buffalo from 2015 to 2016. He is currently an Associate Professor with the School of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include cloud security, outsourcing security, digital forensics, and network and information security. His research has been supported by NSFC, PAPD, and GYHY. He is a member of ACM.

XINGMING SUN received the B.S. degree in mathematics from Hunan Normal University, China, in 1984, the M.S. degree in computing science from Dalian University of Science and Technology, China, in 1988, and the Ph.D. degree in computing science from Fudan University, China, in 2001.

He is currently a Professor with the College of Computer and Software, Nanjing University of Information Science and Technology, China. In 2006, he visited the University College London, U.K. He was a Visiting Professor at the University of Warwick, U.K., from 2008 to 2010. His research interests include network and information security, database security, and natural language processing.