

# A Survey of Image Information Hiding Algorithms Based on Deep Learning

Ruohan Meng<sup>1,2,\*</sup>, Qi Cui<sup>1,2</sup> and Chengsheng Yuan<sup>1,2,3</sup>

**Abstract:** With the development of data science and technology, information security has been further concerned. In order to solve privacy problems such as personal privacy being peeped and copyright being infringed, information hiding algorithms has been developed. Image information hiding is to make use of the redundancy of the cover image to hide secret information in it. Ensuring that the stego image cannot be distinguished from the cover image, and sending secret information to receiver through the transmission of the stego image. At present, the model based on deep learning is also widely applied to the field of information hiding. This paper makes an overall conclusion on image information hiding based on deep learning. It is divided into four parts of steganography algorithms, watermarking embedding algorithms, coverless information hiding algorithms and steganalysis algorithms based on deep learning. From these four aspects, the state-of-the-art information hiding technologies based on deep learning are illustrated and analyzed.

**Keywords:** Steganography, deep learning, steganalysis, watermarking, coverless information hiding.

## 1 Introduction

With the advent of the information age, more and more people use mobile devices to communicate, work and create. It brings great convenience in our life and work. But the increasingly safety problems are exposed. For example, personal privacy is being snooped, spread, stolen works, copyrighted ownership and so on. In solving this kind of problem, information hiding has been paid much attention to protect privacy and copyright. Information hiding means that secret information is hidden in the cover image by utilizing some characteristics of the cover image, and in the process of transmission of the cover image, no anomalies are found by the detector, so that the stego image can be safely transmitted to the receiver. The receiver extracts secret information through a certain algorithm to realize secret communication. Among them, secret information can be a piece of text, an image and so on. In the process of hiding, the usual method is to

---

<sup>1</sup> School of Computer and Software, Nanjing University of Information Science and Technology, Ning Liu Road, No. 219, Nanjing, 210044, China.

<sup>2</sup> Jiangsu Engineering Centre of Network Monitoring, Ning Liu Road, No. 219, Nanjing, 210044, China.

<sup>3</sup> Department of Electrical and computer Engineering, University of Windsor, 401 Sunset Avenue, Windsor, ON, N9B 374, Canada.

\* Corresponding Author: Ruohan Meng. Email: ruohanmeng.melody@gmail.com.

convert secret information into a bit stream and hide the bit information in the cover media. In addition, the image can be directly hidden in another image, or the secret information can be corresponded to the mapping dictionary, and the information containing the mapping objects can be transmitted to the receiver. Steganography is a means of covert communication, and has great significance in national security and military affairs. However, steganography is also used by people who are not good intentions while safeguarding the security of network communication. In fact, information hiding has also been used in espionage, terrorist attacks, crimes and other activities recent years. Under such circumstances, how to effectively supervise steganography and prevent and block its malicious or illegal application has become an urgent need of military and security departments in various countries. So steganalysis has been widely concerned and developed in the development of information hiding. Steganalysis refers to the process in which the detector determines whether the stego image contains secret information or not after publishing the stego image. Steganography and steganalysis are two kinds of algorithms which restrict each other and oppose each other.

## **2 Related works**

### ***2.1 Deep learning***

In 2006, G.E. Hinton et al. [Hinton and Salakhutdinov (2006)] proposed the method of unsupervised pre-training to optimize the initial value of network weights, and then fine-tune the weights, which opened the prelude of deep learning. Deep learning is essentially divided into three types: Supervised learning, unsupervised learning and reinforcement learning. Supervised learning refers to machine learning with both characteristic value and label values in input data. By calculating the error between the network output value and label value, it is expected to train the network iteratively to find the best output value. The problems that need to be solved in supervised learning can be divided into two categories: regression [Fu, Gong, Wang et al. (2018)] and classification [Gurusamy and Subramaniam (2017); Yuan, Li, Wu et al. (2017)]. As an essential classification task, image classification is a research field that attracts much attention. The classification of 1,000 categories on ImageNet [Russakovsky, Deng, Su et al. (2014)] contributed to the development of CNN such as VGG [Simonyan and Zisserman (2014)] and ResNet [He, Zhang, Ren et al. (2016)]. Currently, some popular supervised learning algorithms are represented by convolutional neural network (CNN) and deep belief network (DBN). Extreme learning machine [Gautam, Tiwari and Leng (2017)] is a machine learning based on feedforward neuron network. It is also a kind of supervised learning. It is used for prediction [Dutta, Murthy, Kim et al. (2017)], classification and so on. The goal of unsupervised learning is to find some common features, structures, or correlations between the characteristic value of input data through machine learning. Unsupervised learning methods such as auto-encoder [Kingma and Welling (2013)], deep boltzmann machine [Montavon and Müller (2012)] (RBM) and current popular generative adversarial networks (GAN) [Goodfellow, Pouget-Abadie, Mirza et al. (2014)]. Reinforcement learning [Mnih, Kavukcuoglu, Silver et al. (2015)] emphasizes how to act on the environment to maximize the expected benefits. In application, deep learning has been greatly developed in the fields of video [Feichtenhofer, Fan, Malik et al. (2018)];

Wichers, Villegas, Erhan et al. (2018); Wang, Liu, Zhu et al. (2018)], image [Xie, He, Zhang et al. (2018); Barz and Denzler (2018); Wang and Chan (2018)], voice [Yang, Lalitha, Lee et al. (2018); Arik, Chen, Peng et al. (2018); Qian, Du, Hou et al. (2017)], semantic understanding [Qin, Kamnitsas, Ancha et al. (2018); Zhuang and Yang (2018); Sanh, Wolf and Ruder (2018)], and has been further applied in object detection [Roddick, Kendall and Cipolla (2018); Jaeger, Kohl, Bickelhaupt et al. (2018)], image forensics [Yu, Zhan and Yang (2016), Cui, McIntosh and Sun (2018)], intelligent management [Liang, Jiang, Chen et al. (2018); Le, Pham, Sahoo et al. (2018); Duan, Lou, Wang et al. (2017)] and medicine [Mobadersany, Yousefi, Amgad et al. (2018); Rajpurkar, Irvin, Zhu et al. (2017); Akkus, Galimzianova, Hoogi et al. (2017)].

In the field of supervised learning, image classification methods that based on deep learning have been mature, which can be applied to object detection and image retrieval. Object detection is to detect the categories of objects (such as dogs, vehicles or people) in digital images or videos. Faster R-CNN [Ren, He, Girshick et al. (2015)], R-FCN [Dai, Li, He et al. (2016)], YOLO [Redmon, Divvala, Girshick et al. (2016)] and SSD [Liu, Anguelov, Erhan et al. (2016)] are the four most widely used object detection models based on deep learning. Compared with traditional methods, CNN can handle tasks better when traditional methods can not recognize features effectively.

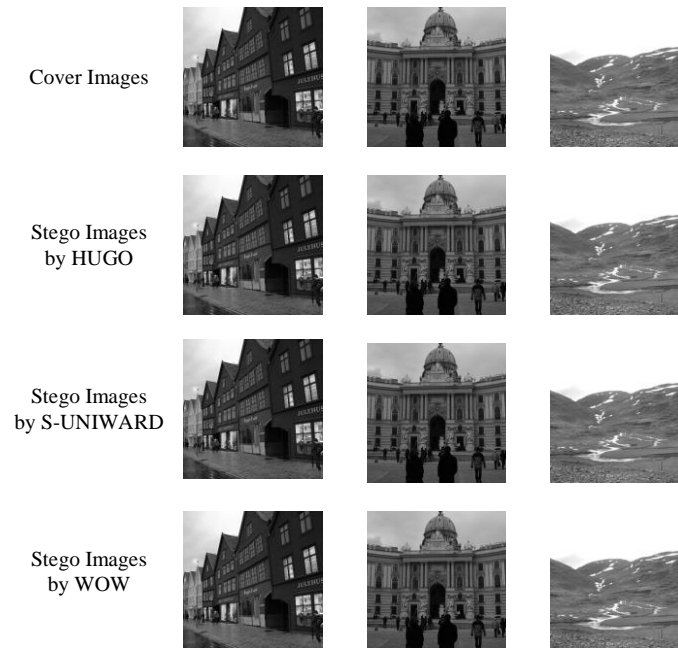
In the field of unsupervised learning, GAN is a typical representative. The basic principle of GAN is that it has two models: A generator and a discriminator. The task of a discriminator is to determine whether a given data looks “natural”, in other words, whether it is generated by machine beings. The generator's task is to constantly capture the data in the training database, so as to generate seemingly “natural” data, which requires the distribution of the original data as consistent as possible. At present, GAN is widely used in many fields, such as image, vision and language. In addition, GAN can also be combined with reinforcement learning. The WGAN (Wasserstein GAN) proposed by Arjovsky et al. in 2017 effectively optimized GAN [Arjovsky, Chintala and Bottou (2017)]. It solves the problem of unstable GAN training, proposes effective methods to ensure the diversity of generated samples, uses specific cross-entropy function to indicate the training process, and uses multi-layer neural network to complete training without designing a specific network structure. Least squares GAN (LSGAN) [Mao, Li, Xie et al. (2017)] optimizes GAN by using a smoother and non-saturating gradient loss function in the discriminator. Hjelm et al. [Hjelm, Jacob, Che et al. (2017)] improve GAN model, which is boundary-seeking GAN. It can be used to train generators with discrete output. Maximum-Likelihood Augmented Discrete GAN [Che, Li, Zhang et al. (2017)] uses the corresponding output following logarithmic likelihood to derive new and low variance targets. Mode regularized GAN [Che, Li, Jacob et al. (2016)] can help to achieve a fair probability quality distribution in the data generation and distribution mode at the early stage of training, thus providing a unified solution to the problem of missing the mode. In Brock et al. [Brock, Donahue and Simonyan (2018)], there is a new achievement of high-resolution results, making impressive progress. The latest research progress in image style transfer is designed based on GAN [karras, Laine and Aila (2018); Zhu, Park, Isola et al. (2017); Yi, Zhang, Tan et al. (2017); Kim, Cha, Kim et al. (2017)]. The aim of training process is reducing the transferring loss between the two transformation targets.

## 2.2 Information hiding

Information hiding technology has a long history. Initially, people used their hair to cover up secret information by hiding secret information in their scalp and waiting for hair to grow long, so as to transmit military information.

In the era of rapid development of computer, the field of information hiding has developed rapidly. In the field of image information hiding, in the early stage, the most representative information hiding algorithm is the spatial least significant bit (LSB) steganography algorithm. In this algorithm, the secret information is hidden to the lowest significant bit of each pixel by using the color insensitivity of human eyes, so as to transmit the secret information. For color images, they are generally composed of three channels: Red (R), Green (G) and Blue (B), each of which occupies 8 bits, ranging from 00x00 to 0Xff. LSB steganography refers to modifying the lowest significant bit of RGB color component. For example, for R channel, assume that  $R_{(x,y)}=11011010$ , the lowest significant bit is the last bit 0, if the hidden secret bit is 1, the lowest effective bit 0 is changed to 1, and the final  $R_{(x,y)}=11011011$ ; if the hidden secret bit is 0, the lowest significant bit is not modified,  $R_{(x,y)}=11011010$ . The hidden capacity of LSB steganography algorithm is very impressive, but it is difficult to resist statistical characteristics. Among the steganography methods in spatial domain, secret information is concealed mainly by calculating the pixel values. Typical methods include LSB replacement [Wu, Wu, Tsai et al. (2005)], LSB matching [Mielikainen (2006); Xia, Wang, Sun et al. (2014); Xia, Wang, Sun et al. (2016)], Multi Bit Plane Image Steganography (MBPIS) [Nguyen, Yoon and Lee (2006)] histogram-based algorithm [Li, Chen, Pan et al. (2009)], color palette [Johnson and Jajodia (1998)], Multiple-Based Notational System (MBNS) [Zhang and Wang (2005)] Quantization index modulation (QIM) [Chen and Wornell (2001)] and so on. For frequency-domain steganography, secret information is hidden mainly by modifying some specified frequency coefficients. The transformation algorithms are discrete cosine transform (DCT), Fourier transform, discrete wavelet transform (DWT) and so on. The steganography methods are usually divided into two categories, which are JPEG steganography [Westfeld (2001); Provos and Honeyman (2001); Sallee (2003); Provos and Honeyman (2003)] and discrete wavelet transform steganography [Al-Ataby and Al-Naima (2008); Yang and Deng (2006); Chen and Lin (2006); Talele and Keskar (2010)].

In order to improve the security of secret information transmission, image adaptive steganography algorithms such as S-UNIWARD [Holub, Fridrich and Denemark (2014)], WOW [Holub and Fridrich (2012)], HUGO [Pevný, Filler and Bas (2010)] are proposed. These algorithms select regions with complex texture by setting distortion threshold according to the embedding distortion of image pixels. As can be seen in Fig.1, there is the comparison of effect diagrams in HUGO, S-UNIWARD and WOW. From the comparison of stego images and cover images, it is difficult to visually detect the anomalies of stego images.



**Figure 1:** The comparison of effect diagrams in HUGO, S-UNIWARD and WOW

### 2.3 Watermarking

Nowadays, digital media has been widely used, and the problems of modification and reuse have also been paid too much attention. In order to solve the copyright problem of digital media, digital watermarking has been proposed and has been developed [Fridrich (1999); He, Zhang and Tai (2009); He, Chen, Tai et al. (2012)]. Digital watermarking refers to embedding the information of digital, serial number, text or image logo into audio, video or image, thus playing the role of copyright protection, authenticity identification, secret communication and so on. At the same time, after the watermark is embedded in the multimedia data, it can be detected and extracted. Digital watermarking includes two aspects: Watermark embedding, watermark detection and extraction. Although the digital watermark has not been proposed for a long time, it has also developed. The watermarking algorithms are divided into six aspects, blind watermarking [Dorairangaswamy (2009); Eggers and Girod (2001); Kang and Lee (2006)], semi-blind watermarking [Liu, Zhang, Chen (2009); Rahman, Ahammed, Ahmed et al. (2017)], non-blind watermarking [Gunjal and Mali (2015)], robust watermarking [Deng, Gao, Li et al. (2009)], fragile watermarking [Chang, Fan and Tai (2008), Nazari, Sharif and Mollaeefar (2017)] and semi-fragile watermarking [Wu, Hu, Gu et al. (2005)]. Recently, there has been a mutual application between deep learning and digital watermarking. In the deep learning model, the use of digital watermarks to protect the attributes of deep learning models is also a relatively new research method. And there has been some progress in using deep learning method to enhance the robustness of digital watermarking.

#### **2.4 Coverless information hiding**

Information hiding is the hiding of secret information by modifying the pixels of the cover image. Modifying the cover image means that it may be detected by detector. In order to avoid this problem completely and resist steganalysis fundamentally, coverless information hiding was proposed by experts in 2014. The coverless information hiding means that the secret information is used as a driver to find or generate a stego image corresponding to the secret information [Gunjal and Mali (2015); Zhou, Sun, Harit et al. (2015); Zhou, Cao and Sun (2016); Yuan, Xia and Sun (2016)]. There is no need to change the cover image during this process. The general approach is to construct a mapping dictionary to form a mapping relationship between secret information and feature information. The sender shares the mapping dictionary with the receiver. By transmitting a natural image or text having a mapping relationship with the secret information to the receiver, the receiver extracts the secret information according to the mapping relationship, thereby resisting the steganalysis. There are two main branches in the field of coverless information hiding. One is coverless text information hiding that is on the transits of text. Due to the prosperity of natural language processing (NLP), the effectiveness of the algorithms on word embedding is witnessed such as word2vec [Goldberg and Levy (2014)] and LSTM [Sak, Senior and Beaufays (2014)]. On the basis of the strong similarity between the mapping relationship of word embedding and text coverless information hiding, there are some achievements which are combining the advanced knowledge of NLP with coverless text information hiding [Zhang, Huang, Wang et al. (2017); Long and Liu (2018); Zhang, Shen, Wang et al. (2016)]. The other is on the transits of image, which is called image coverless information hiding [Duan and Song (2018)].

#### **2.5 Steganalysis**

Steganalysis is used to determine whether the stego image contains secret information or not, which means it is to perform a binary classification task, that is, to determine whether the image is stego images or cover images. Early steganographic algorithms can be detected by human perceptual organs, but with the further development of steganographic algorithms, human perceptual organs cannot distinguish the stego image, so steganalysis can effectively distinguish by analyzing the statistical features of the image. At present, the high-order statistical features based on the complex correlation of image neighborhoods have become the mainstream features in steganalysis, such as SRM/SRMQ1 (Spatial Rich Model) [Fridrich and Kodovsky (2012)] and PSRM (Projection Speciation Rich Model) [Holub and Fridrich (2013)] models based on high-order and high-dimensional features, which have achieved good detection results. There are many studies to evaluate the selection of features. Chen et al. [Chen and Shi (2008)] proposed a feature selection based on block Markov features. Pevny et al. [Pevny and Fridrich (2007)] designed PEV features for steganalysis. As a tentative work of high-dimensional rich model for JPEG steganalysis, CC-C300 was proposed by Kodovsky et al. [Kodovský and Fridrich (2010)]. It initiated the development of the high-dimensional feature of steganalysis. Kodovsky et al. [Kodovský, Fridrich and Holub (2012)] improved their algorithm by pruning to a more compact feature selection. Considering the typical characteristics in image's mode of DCT, Kodovsky et al. [Kodovský and Fridrich (2012)]

proposed CC-JRM\*\*. Aiming at the detection of S-UNIWARD, Denmark et al. [Denemark, Fridrich and Holub (2014)] proposed the residual feature on content selected of images. To reduce the complexity of the steganalysis algorithm, Holub et al. [Holub and Fridrich (2015a)] proposed DCTR that extract features from residual maps of DCT domain. The phase-aware projection model (PHARM) proposed by Holub et al. [Holub and Fridrich (2015b)] is designed based on the observation on the distinguishing feature in grid of JPEG. In the consideration of selection-cannel, Denmark et al. [Denemark, Fridrich and Comesaña-Alfaro (2016); Denmark, Boroumand and Fridrich (2016)] proposed algorithms those extracting features of images in independent channel. In addition to traditional methods based on artificial features, steganalysis methods based on deep learning have been further developed.

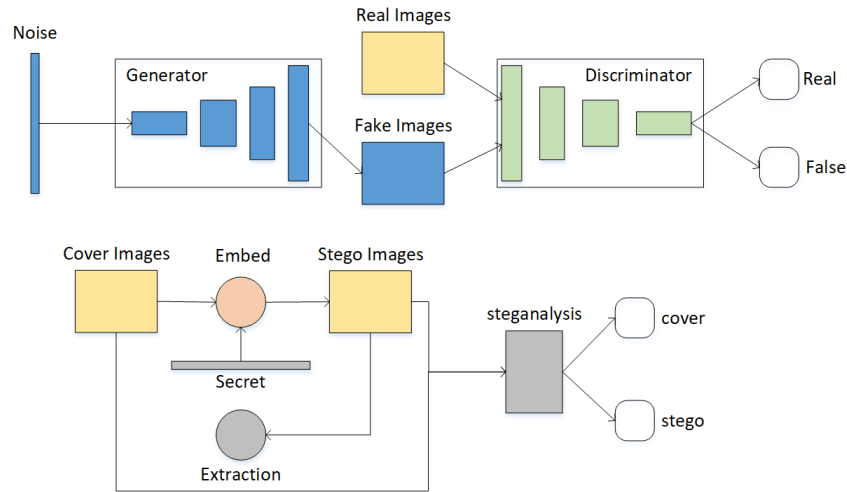
### **3 Image information hiding technology based on deep learning**

The application of deep learning in information hiding has gradually developed. Deep learning can be applied to the field of information hiding because part of the model, characteristics, and processes of deep learning correspond to information hiding. In addition, the models of deep learning also have different degrees of cross-application in each branch of classification method when applied to information hiding. Specially, the adversarial theory in GAN is naturally corresponding to information hiding and the detection. GAN based approaches can resist steganalysis more purposeful when applied to potential steganalysis algorithms. The applications related to GAN in coverless information hiding can generate qualified stego images by mapping dictionary, and avoid detection by its high-quality generation effect.

#### ***3.1 Steganographic algorithms based on deep learning***

##### ***3.1.1 Steganographic algorithms of adversarial method***

GAN is antagonistic by generator and discriminator, which makes the generated image by generator can resist the discriminator. In the basic application of GAN, the generator simulates the distribution of object categories, and each simulated distribution result is given to the discriminator for two classifications, that is, real images or fake images. If it is determined that the image is a generated image, the determination result is fed back to the generator, and the generator regenerates the image distribution according to the feedback. By continuously cycling through this process, a relatively realistic image is finally generated. In this process, we find that there is a certain similarity between the confrontation between the generator and the discriminator and the confrontation between steganography and steganalysis. As shown in Fig. 2, the process of steganography is to obtain stego images by hiding the secret message into cover images using the embedding algorithm. For the receiver, the secret information in the stego images is extracted by the extraction algorithm; for the steganalysis, after the stego images are public, the detector determines whether the image is a cover image or a stego image by determining whether the stego images contain a secret message. In GAN, the generative network generates an image by inputting a piece of noise into the generator. The discriminative network inputs the fake images and real images to the discriminator, and the discriminator gives the result of whether it is a real image, that is, judges the authenticity of the generated image.



**Figure 2:** Comparison between steganography and corresponding steganalysis and GAN

Through analysis, it is clear that the structure of GAN completely corresponds to the structure of the steganography. The generation network corresponds to steganography to generate a stego image, and the discrimination network corresponds to the steganalysis to determine whether it is a false (stego) image. Therefore, many papers apply GAN to steganography. It is proved by experiments that the combination of steganography and GAN makes the steganography process more robust, and the obtained stego image is more concealed and safe. The total optimization function of GAN is shown in Eq. (1).

$$\min_G \max_D V(D, G) = E_{x \sim P_{data}(x)} [\log(D(x))] + E_{z \sim P_z(z)} [\log(1 - D(G(z)))] \quad (1)$$

Where  $x$  represents input data,  $P_z(z)$  is a noise variable,  $P_{data}(x)$  is real data, and  $D(x)$  represents the probability that  $x$  is derived from real data rather than generated data.

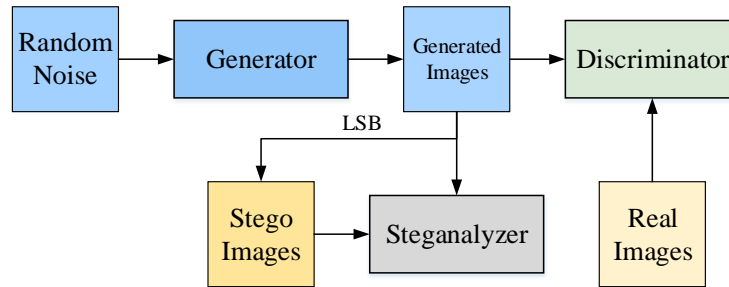
This method was first proposed by Hayes et al. [Hayes and Danezis (2017)]. They define a three-party game, Alice, Bob, and Eve. Alice and Bob tried to hide the secret information into the image, use it for secret communication, and Eve eavesdropped on their conversation and judged whether it contained secret information or not. In this process, all three parties are neural networks. Alice is a steganographic constructor as a generator, Eve is a steganalysis as a discriminator, and Bob is an extractor. The stego image generated by the generator is adjusted according to the feedback of the steganalysis, that is, the discriminator. Bob extracts the information on the bits from the resulting stego image. Volkhonskiy et al. [Volkhonskiy, Nazarov, Borisenko et al. (2017)] propose SGAN (Steganographic Generative Adversarial Networks), mainly adding a discriminator that is steganalysis based on GAN. As shown in Fig. 3, the structure of SGAN is a generator and two discriminators those are discriminator and steganalyzer. The role of the discriminator is used to determine whether the image is true and steganalyzer is used to judge whether the image contains secret information. The total optimization function is shown in Eq. (2), and the optimization function of the steganalyzer is added to the optimization function of the GAN model. This method reduces the detection rate of steganalysis, making information hiding more secure. SGAN has increased the



discriminator based on DCGAN [Radford, Metz and Chintala (2015)]. The visual effects of SGAN are shown in Fig. 4.

$$\min_G \max_D \max_S V(D, S, G) = \partial \left( E_{x \sim P_{data}(x)} [\log(D(x))] + E_{z \sim P_z(z)} [\log(1 - D(G(z)))] \right) + (1 - \partial) E_{z \sim P_z(z)} [\log S(\text{Stego}(G(z))) + \log(1 - S(G(z)))] \quad (2)$$

Among them,  $P_z(z)$  is the noise variable,  $P_{data}(x)$  is the real image,  $\text{Stego}(x)$  is the stego image,  $\alpha$  is the weight parameter, which is used to control the importance of the loss function to D and S when G generating image.



**Figure 3:** The structure of SGAN



**Figure 4:** The visual effects of SGAN

Shi et al. [Shi, Dong, Wang et al. (2017)] improved on the basis of SGAN. By changing the basic network DCGAN of SGAN to WGAN, the generated image is more real, the image quality is higher, and the network training speed is faster. In addition, the steganalysis network has been improved to GNCNN [Qian, Dong, Wang et al. (2015)]. Through the resistance between GNCNN and generator, the stego image is more concealed and the robustness is enhanced. Tang et al. [Tang, Tan, Li et al. (2017)] propose a new framework, ASDL-GAN, which realizes steganography by finding

suitable steganographic locations for cover images. In addition, the network modifies the structure of the discriminator and changes the discriminator to the steganalysis model of Xu et al. [Xu, Wu and Shi (2016)]. Yang et al. [Yang, Liu, Kang et al. (2018)] make three improvements on the basis of ASDL-GAN: modifying activation function to Tanh-simulator to reduce the epoch of training; changing generator based on U-NET [Ronneberger, Fischer and Brox (2015)]; adding SCA [Denemark, Boroumand and Fridrich (2016)] to discriminator to enhance the performance of resisting SCA based steganalysis schemes. Ma et al. [Ma, Guan, Zhao et al. (2018)] propose using adversarial samples to train a network to actively attack steganalysis methods. After synthesizing several different steganalysis methods, their steganographic ability has been verified experimentally. Hu et al. [Hu, Wang, Jiang et al. (2018)] propose that secret information be mapped into a noise vector as the input of the generator, and secret image can be directly generated without modifying the image. The algorithm is divided into three steps. 1. The GAN network is trained by meaningful noise vectors, so that the generator can directly generate the cover images. 2. The stego images are used as the input of the extractor, and the corresponding network with the generator is used as the extracting network to train the stego image to a one-dimensional vector, so that the recovered vector is as consistent as possible with the original input noise vector, so as to extract secret information. The extractor's loss function is shown in Eq. (3). 3. The parameters of the generator are supplied to the sender, and the parameters of the extractor are provided to the receiver. This method takes into account the extracting part of secret information, and solves the difficult problem of extracting secret information after using GAN method to hide information.

$$L(E) = \sum_{i=1}^n (z - E(stego))^2 = \sum_{i=1}^n (z - E(G(z)))^2 \quad (3)$$

Here,  $z$  represents the random noise of the input GAN,  $E(stego)$  is the noise vector recovered by extractor.  $G(z)$  represents the generated by generator from noise  $z$ .

Li et al. [Li, Jiang and Cheslyar (2018)] propose the method of using GAN-synthesized texture images as the secret cover. The input noise is mapped to a small patch selected from the original image. The network can generate different textures even with the same original image which makes it difficult for a middle attacker to obtain. The synthesized texture image together with the secret message is sent to another information hiding network to realize secret communication. The information hiding network follows the auto-encoder network architecture to encode and decode the secret message at the same time. Two separate datasets are used in their experiments, one for texture generation and the other for the information concealment.

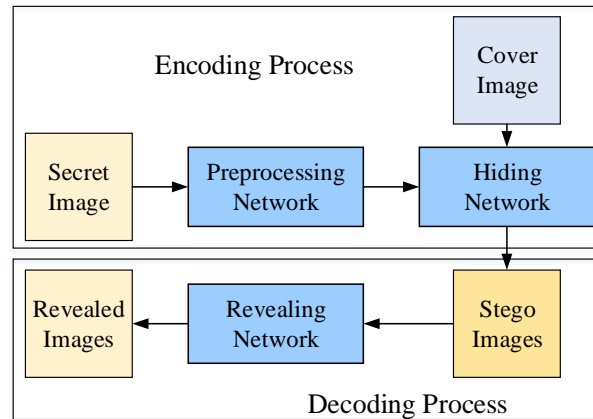
When there are potential steganalysis methods in the transmission channel, the steganography method based on GAN can effectively solve the problem by reducing the rate of detection of the specific steganalysis methods. Through the confrontation between steganalysis algorithm and generator of GAN, the resulting stego image has higher security and stronger steganalysis resistance. Although this method can resist steganalysis to some extent, the visual effect of stego image generated is not good, and can be further improved in anti-stealth analysis capabilities.

### 3.1.2 Steganographic algorithms of hiding entire secret image

In addition to using GAN model to hide secret messages, some people propose to hide a entire secret image into a cover image based deep learning and auto-encoder, and the receiver can recover the secret image and the cover image. Baluja [Baluja (2017)] proposes to use neural networks to find the location where is appropriate to embed secret information in the image. As shown in Fig. 5, the encoding process is trained to embed entire secret image to cover image so that the secret information can be dispersed in each bit of the image. Firstly, the secret image is normalized by preprocessing network and important features are extracted at the same time. Then the secret image and cover image with the same size are encoded through hiding network to get stego image. At the same time, the model also trains a decoder corresponding to the encoder to extract the secret image. It is the process of decoding. Although this method can realize the hiding of the entire image, and achieve double recovery of the cover image and the secret image. However, there are still certain problems. For example, after hiding the secret image in the cover image, the hidden secret image can still be seen. At the same time, this method is not resistant to steganalysis. Another method similar to this method is propose by Rahim et al. [Rahim and Nadeem (2017)], which also incorporates encoder-decoder networks and CNN. The experimental results show that the image quality of the stego image is very good, but according to the experimental results, it is found that the color of stego image is different from that of cover image. The loss function for the whole network is defined as Eq. (4):

$$L(I_{secret}, I_{cover}) = \alpha \|I_{cover} - O_{stego}\|^2 + \beta \|I_{secret} - O_{recover}\|^2 + \lambda (\|W_{encode}\|^2 + \|W_{decode}\|^2) \quad (4)$$

Where  $I_{cover}$  and  $I_{secret}$  represent the input of cover images and secret images,  $O_{stego}$  and  $O_{recover}$  represent the output of stego images and recover images.  $W_{encode}$  and  $W_{decode}$  represent are the weights for encoder and decoder.  $\alpha$ ,  $\beta$  and  $\lambda$  are the controlling parameters for the corresponding terms.



**Figure 5:** The main structure of Baluja [Baluja (2017)]: Encoding process and decoding process

Based on these two methods, Zhang et al. [Zhang, Dong and Liu (2018)] propose that divide the cover image into three channels: Y, U and V. A grayscale secret image is hidden into the Y channel of the cover image through the encoder. Then, using the generator of the GAN model, the U, V channel of the cover image is merged with stego Y channel. The discriminator uses the steganalysis network of Xu et al. [Xu, Wu and Shi (2016)] to resist. Finally, the stego image is generated. Receiver extracts secret images by using decoder. This method has greatly improved the effect compared to the previous algorithm. The color of the stego image and the cover image seem to be the same as the naked eye, and the effect of the residual enhancement is also invisible to naked eye. The effect diagrams of the algorithm are shown in Fig. 6, the first column is cover images, the second column is secret images, the third column is stego images, and the fourth column is recovered secret images.



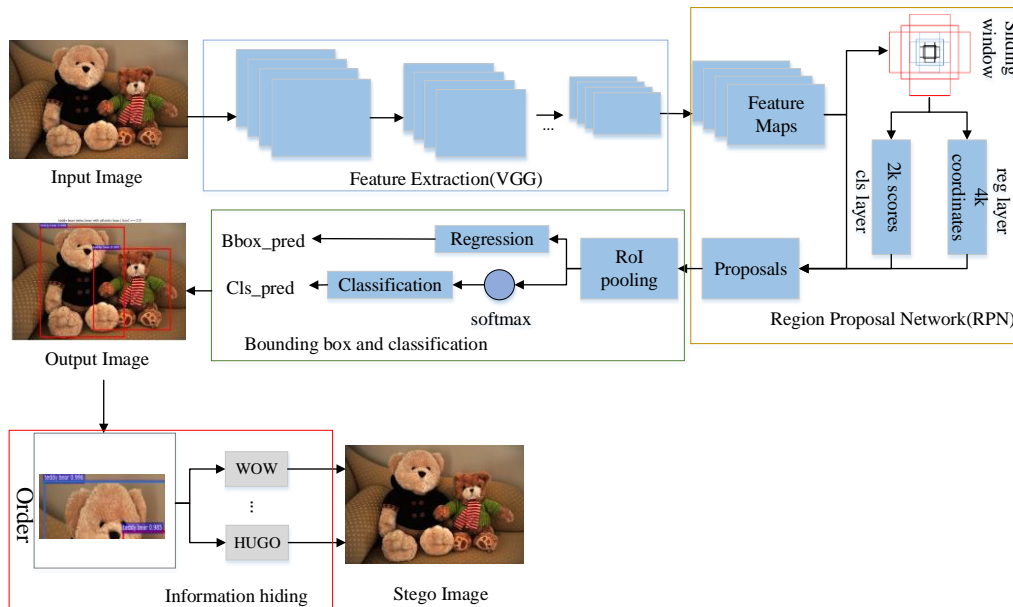
**Figure 6:** The effect diagrams of the algorithm in Zhang et al. [Zhang, Dong and Liu (2018)]

The above algorithms can realize high capacity information hiding. The unique features of these methods are those they can hide the whole image in the same size cover image and can recovery cover images and secret images. So we classify them as information hiding classes of hiding entire secret images. This type of methods is suitable for high-capacity secret information transmission or secret image transmission. The advantages of this kind of methods are those these algorithms can improve the hiding capacity and can hide a secret image in one image instead of a small amount of bit information. However, these approaches cannot resist steganalysis on their high embedding rate, that their security is poor.

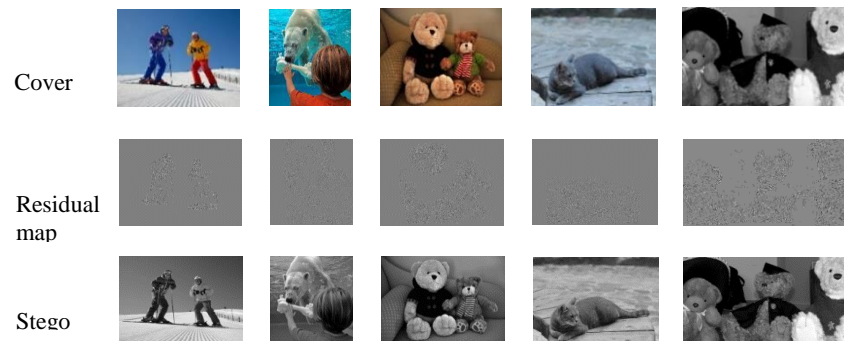
### *3.1.3 Steganographic algorithms of selecting embedding location and others*

In addition to the above two methods, there are other algorithms that use deep learning models for information hiding. Wu et al. [Wu, Wang and Shi (2016)] used the machine learning method to realize the hiding of LSB. Atee et al. [Atee, Ahmad, Noor et al.

(2017)] propose learning based on Extreme Learning Machine (ELM) and selecting the optimal embedded information position. The method can better guarantee the visual effect of the image and has better imperceptibility. Meng et al. [Meng, Rice, Wang et al. (2018)] propose to use the object detection method of faster rcnn to find the complex object area for information hiding, which is called MSA\_ROI. Since there may be multiple objects in an image, multiple adaptive steganography algorithms are used to hide information in different objects areas. The structure of this algorithm as shown in Fig. 7, firstly, the cover image is used as an input image to extract image features through VGG. Secondly, feature maps get proposals through the region proposal network. Thirdly, classification and border regression of proposals are considered. Lastly, area steganography is performed using different adaptive steganography algorithms in different target areas. Although this method can be steganographic in a specific area, it cannot accurately hide secret information from foreground objects and reduce the hiding capacity. The effect of the algorithm is shown in Fig. 8.



**Figure 7:** The structure of MSA\_ROI

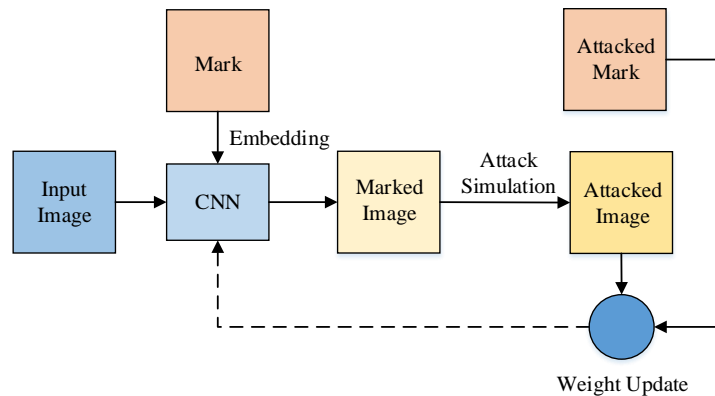


**Figure 8:** The structure of MSA\_ROI

### ***3.2 Watermarking algorithms based on deep learning***

The sharing of deep learning network greatly reduces the debugging and training burden of engineers and researchers, but the following problems, such as model tampering and copyright loss, bring security risks. Therefore, how to guarantee the intellectual property rights of deep learning network and how to guarantee the rights and interests of researchers are the problems that need to be solved in the promotion and application of deep learning. At present, the research is still in its infancy.

Yalcin et al. [Yalcin and Vandewalle (2002)] propose a fragile watermarking technique and a CNN-UM structure that can be used to generate pseudorandom noise patterns added to the host image. Mun et al. [Mun, Nam, Jang et al. (2017)] propose a method for implementing blind watermarking through the CNN model. As shown in Fig. 9, the method mainly includes three parts: watermark embedding, simulated attack and weight modification. First, mark is embedded into input image through CNN, and marked image is obtained. Second, the attack simulation is performed on the marked image, and the attack simulation includes JPEG compression, noising, Gaussian filtering, median filtering and so on, and finally the attacked image is obtained. Last, continue to attack the image through the attacked mark, so as to continuously update the weight. According to the type of attack, adaptively captures more robust regions. Compared with QDFT, this method can be hidden on a special domain through network learning. Kandi et al. [Kandi, Mishra and Gorthi (2017)] propose a CNN-based codebook for robust non-blind watermarking, which is superior to the transform domain method. In addition, in the aspect of deep neural network model protection, Uchida et al. [Uchida, Nagai, Sakazawa et al. (2017)] propose to embed the digital watermark into the trained neural network model to achieve the purpose of copyright protection. Li et al. [Li, Deng, Gupta et al. (2018)] propose a security-guaranteed image watermarking generation scenario for city applications based on CNN. Rouhani et al. [Rouhani, Chen and Koushanfar (2018)] propose deepsigns. It is a novel end to end structure in the field of systematic watermarking and IP protection based on deep learning. The advantages of the algorithm are those it proposes deepsigns, applies a set of metrics to assess the effect of watermark embedding method for deep learning models and so on.



**Figure 9:** The structure of watermarking algorithm in Mun et al. [Mun, Nam, Jang et al. (2017)]

### 3.3 Coverless information hiding algorithms based on deep learning

The application of deep learning in coverless information hiding is mainly through the combination of GAN and coverless information hiding. GAN can generate the required image according to certain requirements. Combined with the features, coverless information hiding can directly generate stego image driven by secret information. Thus, the hiding capacity is enhanced and the security is improved.

Liu et al. [Liu, Zhang, Liu et al. (2017)] propose to use the ACGAN generator directly for coverless information hiding. The method divides and expresses secret information into image category information by establishing a mapping dictionary between image categories and text. The image category information is then input into the generator to generate an image as a stego image, thereby implementing coverless information hiding. In order to ensure the security of GAN, Ke et al. [Ke, Zhang, Liu et al. (2017)] propose a generator that satisfies the Kerckhoffs principle, directly generating the stego image by directly using the key and the cover image as the input of the generator in the GAN. Duan et al. [Duan, Song, Qin et al. (2018)] propose that generate two images with same visual based on generative model.

### 3.4 Steganalysis algorithms based on deep learning

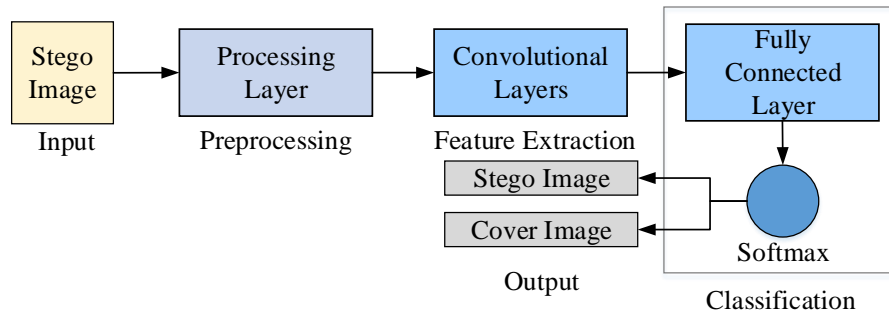
CNN model is widely used in steganalysis owing to the traditional steganalysis algorithm process corresponds to CNN classification process.

Prior to applying deep learning to information hiding, Qian et al. [Qian, Dong, Wang et al. (2015)] propose a steganalysis framework based on deep learning in 2015. The structure of this algorithm can be seen in Fig. 10. The main purpose of this algorithm is to enhance the noise by preprocessing the image with a high-pass filter using a traditional algorithm. The preprocessed image is input into the CNN model for image feature extraction. The activation function is a Gaussian function as shown in (5), and the activation function will have a positive feedback close to 1 only when the input is near zero. Finally, the images are classified at the fully connected layer, so that the distinguishing images are cover images or stego images.



$$f(x) = e^{-\frac{x^2}{\sigma^2}} \quad (5)$$

Where  $\sigma$  is used to determines the width of the curve. Only when the input is near zero will the activation function have an obvious positive feedback.



**Figure 10:** The framework of steganalysis algorithm in Qian et al. [Qian, Dong, Wang et al. (2015)]

Zheng et al. [Zheng, Zhang, Wu et al. (2017)] propose a steganography detection framework based on deep learning methods. The deep residual network is trained to distinguish between a cover image and a stego image containing a weak signal. The learning model is used to extract features from the image, and a condensed hierarchical clustering algorithm is used to find the stego image based on the maximum distance metric from the cover image. After these methods, steganalysis based on deep learning is mainly divided into two classes of method. One method is to improve or transform the network model structure, and the other is to further enhance the model expression ability and generalization performance by means of migration learning and model fusion [Dong, Qian and Wang (2017)].

### 3.4.1 Steganalysis method for improving or transforming network model structure

In the method of improving or transforming the network model structure, Xu et al. [Xu, Wu and Shi (2017)] propose a steganalysis model based on CNN, which still uses the high-pass filter propose by Qian et al. [Qian, Dong, Wang et al. (2015)]. However, the article improves the CNN structure by adding an activation layers (ABS), a batch normalization (BN), and modifying some activation functions to tanh activation functions. Salomon et al. [Salomon, Couturier, GUYEUX et al. (2017)] propose another steganalysis model based on CNN structure model. Compared to the network model of Qian et al. [Qian, Dong, Wang et al. (2015)], the model uses only two layers of convolutional layers and increases the number of feature maps in each convolutional layer. In addition, since the scaling operation of the pooling layer is considered to smooth the noise, it is disadvantageous for the subsequent steganalysis operation, so the pooling layer is removed. For the detection of JPEG steganography algorithms, the traditional method relies on extracting features of JPEG. However, Chen et al. [Chen, Sedighi, Boroumand et al. (2017)] propose to convert the JPEG phase perception into the architecture of the CNN network, thereby improving the detection accuracy of the detector. Xu et al. [Xu



(2017)] propose a method for detecting J-UNIWARD [Holub, Fridrich and Denemark (2014)] with a 20-layer CNN structure for the BOSSBase dataset [Bas, Filler and Pevný (2011)] of size  $256 \times 256$  and CLS-LOC dataset of size  $512 \times 512$ . Tan et al. [Tan and Li (2014)] propose using a convolutional auto-encoder in the pre-training process, and multiple convolutional auto-encoders form a CNN. At present, in the method of improving the model structure, the better effect is the CNN structure improvement model proposed by Ye et al. [Ye, Ni and Yi (2017)]. Some experiments can achieve 99.9% detection accuracy. There are four main improvements in this algorithm: (1) Use the high-pass filter kernel in SRM to initialize the weight of the first layer of convolutional layer in CNN, thus replacing the way of random initialization; (2) Define a new truncated Linear Unit that allows the network to adapt well to the distribution of embedded signals; 3. Combine the selected channel when inputting a stego image; 4. For steganalysis of low embedding rates, use migration learning strategies. Wu et al. [Wu, Zhong and Liu (2017)] proposed shared normalization (SN) for sharing statistics during training and test process. This approach can train the network effective by seizing the weak signal of stego image. For the transformation network model structure, Wu et al. [Wu, Zhong and Liu (2016)] use a deep residual network in the article for steganalysis. In DNA steganalysis, Bae et al. [Bae, Lee, Kwon et al. (2017)] mainly use deep recurrent neural networks to simulate the internal structure of DNA sequences by extracting hidden layers composed of circulating neural networks (RNNs). In the method of improving the CNN model to make it suitable for steganalysis, many algorithms are still being proposed [Yedroudj, Comby and Chaumont (2018); Ma, Guan, Zhao et al. (2018); Yang, Shi, Wong et al. (2017); Zhang, Zhu and Liu (2018)].

### *3.4.2 Steganalysis method based on migration learning*

In the method of further enhancing the expressive ability of the model by means of migration learning, model fusion, etc., Qian et al. [Qian, Dong, Wang et al. (2016)] propose a new framework based on migration learning to improve the ability of feature learning of CNN model. The model firstly uses the training image composed of high payload and the corresponding coverage rate to pre-train the CNN model, and then transforms the learned feature representation into a regularized CNN model to better detect the hidden low payload. In this way, auxiliary information from high load concealment can be effectively utilized to help detect hidden tasks with low payload. Based on the domain knowledge of Steganalysis Rich Model (SRM) [Kodovský and Fridrich (2013)]; Zeng et al. [Zeng, Tan, Li et al. (2018)] propose a general JPEG steganalysis framework for hybrid deep learning. The framework proposed by the author involves two main stages: The first stage is manufactured, which corresponds to the convolution stage and the quantization truncation stage of SRM, and the second stage contains a composite depth neural network, which learns model parameters in the training process. Xu et al. [Xu, Wu and Shi (2016)] propose a steganalysis model based on regularized CNN in this paper. It uses the priori information of traditional artificial design features (such as SRM, maxSRM [Denemark, Sedighi, Holub et al. (2014)], etc.) to regularize CNN model and reduce the over-fitting problem in CNN training, so as to improve the steganalysis performance of the model. In the traditional steganalysis feature, the effective global statistical information is not easily obtained by the convolutional

network structure. Therefore, this paper proposes to use this kind of information in the training of CNN network by model regularization, so as to promote CNN to learn more effective steganalysis feature expression.

In the steganalysis methods based on deep learning, this kind of method has better detectability in traditional information hiding method, and can also detect stego images well in the steganography algorithms based on deep learning. This brings some challenges to steganography.

#### 4 Evaluation and comparison

This section focuses on the comparison and analysis of algorithm performance in the case of quantifying some variables.

**Table 1:** Comparison of SGAN [Volkhonskiy, Nazarov, Borisenko et al. (2017)] and SSGAN [Shi, Dong, Wang et al. (2017)] in time costs and accuracy of steganalysis using methods of Qian et al. [Qian, Dong, Wang et al. (2015)] under 0.4bpp on CelebA dataset [Liu, Luo, wang et al. (2015)]

Algorithms	Categories	Time costs (s)	Accuracy
SGAN	Real images	34.33	0.92
	Generated images		0.90
SSGAN	Real images	32.50	0.87
	Generated images		0.72

In Tab. 1, the comparisons are expressed as the detection accuracy of SGAN and SSGAN and training time consumption when using the same steganalysis method. Obviously, SSGAN is more effective in resisting detector detection due to its lower rate.

Tab. 2 shows the performances of anti-detection for steganalysis among the three related steganography algorithms under the circumstance of employing SRM steganalysis algorithm. It can be concluded that S-UNIWARD has obtained the most concealed effect from the results due to its experimental result. However, the GAN based approaches demonstrate their potential for development on the advantages in feature learning.

**Table 2:** Comparison of ASDL-GAN [Tang, Tan, Li et al. (2017)], UT-GAN [Yang, Liu, Kang et al. (2018)] and S-UNIWARD [Holub, Fridrich and Denmark (2014)] in accuracy of steganalysis using methods of Fridrich et al. [Fridrich and Kodovsky (2012)] under 0.4 bpp on BOSSBase dataset [Bas, Filler and Pevný (2011)]

Algorithms	Accuracy
ASDL-GAN	0.83
UT-GAN	0.88
S-UNIWARD	0.79

In Tab. 3, the contradistinctions for value of PSNR are showed. The highest value between stego images and cover images reflects the best quality of images, which

implemented from ISGAN. But the best quality on recover secret images and original secret images are obtained by ENDS. The experiments show the balance on robustness and concealment.

**Table 3:** Comparison of DS [Baluja (2017)], EDNS [Rahim and Nadeem (2017)] and ISGAN [Zhang, Dong and Liu (2018)] in PSNR between stego images and cover images and between recover images and secret images on Tiny-ImageNet set

Algorithms	PSNR of stego/cover	PSNR of recover/secret
DS	34.57	33.53
ENDS	32.90	34.60
ISGAN	34.89	33.42

As can be seen in Tab. 4, we convert the experimental data in the paper into uniform standard that is bit-per-pixel (bpp). Under this quantity, the hiding capacity of algorithm [Ke, Zhang, Liu et al. (2017)] is better than that of algorithm [Liu, Zhang, Liu et al. (2017)].

**Table 4:** Comparison of experimental results for the hiding capacity in Liu et al. [Liu, Zhang, Liu et al. (2017)]; Ke, Zhang, Liu et al. (2017)]

Algorithms	Capacity(bpp)
[Liu, Zhang, Liu et al. (2017)]	0.0019
[Ke, Zhang, Liu et al (2017)]	0.0051

The comparisons of the PSNR value of watermarked images without noise and with attacked are shown in Tab. 5 and Tab. 6. Under the quantities, it is found that the average value of PSNR in Kandi et al. [Kandi, Mishra and Gorthi (2017)] is the highest without any attack. However, the anti-attack of the approach in Mun et al. [Mun, Nam, Jang et al. (2017)] is better than Kandi et al. [Kandi, Mishra and Gorthi (2017)].

**Table 5:** Comparison of experimental results for the PSNR value of watermarked images in Li et al. [Li, Deng, Gupta et al. (2018)]; Mun, Nam, Jang et al. (2017); Kandi, Mishra and Gorthi (2017)]

Image name	[Li, Deng, Gupta et al. (2018)]	[Mun, Nam, Jang et al. (2017)]	[Kandi, Mishra and Gorthi (2017)]
Barbara	50.12	—	—
Living room	49.78	—	—
Lena	—	38.90	—
Mandrill	—	38.90	—
Peppers	48.41	39.00	—
Average	49.44	38.93	58.91

**Table 6:** Comparison of experimental results for the PSNR value of watermarked images being attacked by different methods in Mun et al. [Mun, Nam, Jang et al. (2017); Kandi, Mishra and Gorthi (2017)]

Method	[Mun, Nam, Jang et al. (2017)]	[Kandi, Mishra and Gorthi (2017)]
No noise	38.93	58.91
Median filtering	39.22	36.42
Gaussian filtering	39.44	31.27
Average filtering	—	30.12

**Table 7:** Comparison of detection errors of steganalysis algorithms for steganographic algorithms at embedding change rate of 0.1 bpp and 0.4 bpp on BOSSBase

Steganography	Steganalysis	0.1 bpp	0.4 bpp
S-UNIWARD	[Wu, Zhong and Liu (2017)]	0.3521	0.1653
	[Wu, Zhong and Liu (2016)]	—	0.0630
	[Ye, Ni and Yi (2017)]	0.3220	0.1281
	[Qian, Dong, Wang et al. (2015)]	—	0.3090
	[Zheng, Zhang, Wu et al. (2017)]	—	0.0000
	[Tan and Li (2014)]	—	—
	[Xu, Wu and Shi (2016)]	0.4267	0.1976
	[Qian, Dong, Wang et al. (2016)]	0.4293	0.2205
	HUGO	[Wu, Zhong and Liu (2017)]	0.3081
[Wu, Zhong and Liu (2016)]		—	0.0410
[Ye, Ni and Yi (2017)]		—	—
[Qian, Dong, Wang et al. (2015)]		—	0.2890
[Zheng, Zhang, Wu et al. (2017)]		—	—
[Tan and Li (2014)]		—	0.3100
[Xu, Wu and Shi (2016)]		—	—
WOW	[Qian, Dong, Wang et al. (2016)]	—	—
	[Wu, Zhong and Liu (2017)]	0.3002	0.1426
	[Wu, Zhong and Liu (2016)]	—	0.0430

[Ye, Ni and Yi (2017)]	0.2442	0.0959
[Qian, Dong, Wang et al. (2015)]	—	0.2930
[Zheng, Zhang, Wu et al. (2017)]	—	—
[Tan and Li (2014)]	—	—
[Xu, Wu and Shi (2016)]	—	—
[Qian, Dong, Wang et al. (2016)]	0.3843	0.2028

Tab. 7 denotes the performance of different deep learning based steganalysis algorithms on different steganography algorithms. For the case of using S-UNIWARD steganography algorithm with 0.1 bpp, steganalysis algorithm proposed in Ye et al. [Ye, Ni and Yi (2017)] has the best detection effect, it is the lowest detection error of 0.3220. When the payload is 0.4 bpp with S-UNIWARD, the proposed steganalysis methods in Wu et al. [Wu, Zhong and Liu (2016); Zheng, Zhang, Wu et al. (2017)] show good results those are 0.0630 and 0.0000 respectively. Meanwhile, the steganalysis method of Wu et al. [Wu, Zhong and Liu (2016)] in the detections of stego images those are got by HUGO and WOW with 0.4 bpp also have low detection errors of 0.0410 and 0.0430 respectively. The steganalysis method proposed by Ye et al. [Ye, Ni and Yi (2017)] has better experimental results when stego images are steganalysed by WOW steganography algorithm.

## 5 Conclusion and future work

This paper describes and analyses image information hiding algorithms based on deep learning from four aspects: steganography, watermarking, coverless information hiding and steganalysis. In these fields, although some researches have been done, there are still some problems that can be further improved. For example, some steganography based algorithms have strong robustness, but the corresponding extraction methods still need to be improved. In addition, the existing algorithms can be further optimized by introducing a new optimization function suitable for algorithm of information hiding, adding or using a deep learning model that suitable for the algorithm.

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

## References

- Al-Ataby, A.; Al-Naima, F.** (2008): A modified high capacity image steganography technique based on wavelet transform. *Changes*, vol. 4, pp. 6.
- Akkus, Z.; Galimzianova, A.; Hoogi, A.; Rubin, D. L.; Erickson, B. J.** (2017): Deep learning for brain MRI segmentation: State of the art and future directions. *Journal of*

*Digital Imaging*, vol. 30, no. 4, pp. 449-459.

**Arik, S. O.; Chen, J.; Peng, K.; Ping, W.; Zhou, Y.** (2018): Neural voice cloning with a few samples. *Computation and Language*.

**Arjovsky, M.; Chintala, S.; Bottou, L.** (2017): Wasserstein GAN. *Machine Learning*.

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

**Bae, H.; Lee, B.; Kwon, S.; Yoon, S.** (2017): DNA steganalysis using deep recurrent neural networks. *Machine Learning*.

**Barz, B.; Denzler, J.** (2018): Hierarchy-based image embeddings for semantic image retrieval. *Computer Vision and Pattern Recognition*.

**Bas, P.; Filler, T.; Pevný, T.** (2011): "Break our steganographic system": The ins and outs of organizing BOSS. *International Workshop on Information Hiding*, pp. 59-70.

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

**Brock, A.; Donahue, J.; Simonyan, K.** (2018): Large scale GAN training for high fidelity natural image synthesis. *Machine Learning*.

**Chang, C. C.; Fan, Y. H.; Tai, W. L.** (2008): Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, vol. 41, no.2, pp. 654-661.

**Che, T.; Li, Y.; Jacob, A. P.; Bengio, Y.; Li, W.** (2016): Mode regularized generative adversarial networks. *Machine Learning*.

**Che, T.; Li, Y.; Zhang, R.; Hjelm, R. D.; Li, W. et al.** (2017): Maximum-likelihood augmented discrete generative adversarial networks. *Artificial Intelligence*.

**Chen, B.; Wornell, G. W.** (2001): Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423-1443.

**Chen, C.; Shi, Y. Q.** (2008): JPEG image steganalysis utilizing both intrablock and interblock correlations. *IEEE International Symposium on Circuits and Systems*, pp. 3029-3032.

**Chen, M.; Sedighi, V.; Boroumand, M.; Fridrich, J.** (2017): JPEG-phase-aware convolutional neural network for steganalysis of JPEG images. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, pp. 75-84.

**Chen, P. Y.; Lin, H. J.** (2006): A DWT based approach for image steganography. *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275-290.

**Cui, Q.; McIntosh, S.; Sun, H.** (2018): Identifying materials of photographic images and photorealistic computer generated graphics based on deep CNNs. *Computers, Materials & Continua*, vol. 55, no. 2, pp. 229-241.

**Dai, J.; Li, Y.; He, K.; Sun, J.** (2016): R-FCN: object detection via region-based fully convolutional networks. *Advances in Neural Information Processing Systems*, pp. 379-387.

**Denemark, T.; Boroumand, M.; Fridrich, J.** (2016): Steganalysis features for content-

adaptive JPEG steganography. *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1736-1746.

**Denemark, T.; Fridrich, J.; Comesaña-Alfaro, P.** (2016): Improving selection-channel-aware steganalysis features. *Electronic Imaging*, vol. 2016, no. 8, pp. 1-8.

**Denemark, T.; Fridrich, J.; Holub, V.** (2014): Further study on the security of S-UNIWARD. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 9028.

**Denemark, T.; Sedighi, V.; Holub, V.; Cogramne, R.; Fridrich, J.** (2014): Selection-channel-aware rich model for steganalysis of digital images. *IEEE International Workshop on Information Forensics and Security*, pp. 48-53.

**Deng, C.; Gao, X.; Li, X.; Tao, D.** (2009): A local Tchebichef moments-based robust image watermarking. *Signal Process*, vol. 89, no. 8, pp. 1531-1539.

**Dong, J.; Qian, Y.; Wang, W.** (2017): Recent advances in image steganalysis. *Journal of Image and Signal Processing*, vol. 6, no. 3, pp. 131-138.

**Dorairangaswamy, M. A.** (2009): A novel invisible and blind watermarking scheme for copyright protection of digital images. *International Journal of Computer Science and Network Security*, vol. 9, no. 4, pp. 71-78.

**Duan, L.; Lou, Y.; Wang, S.; Gao, W.; Rui, Y.** (2017): AI oriented large-scale video management for smart city: Technologies, standards and beyond. *IEEE MultiMedia*, pp. 1.

**Duan, X.; Song, H.** (2018): Coverless information hiding based on generative model. *Computer Vision and Pattern Recognition*.

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

**Dutta, S.; Murthy, A. R.; Kim, D.; Samui, P.** (2017): Prediction of compressive strength of self-compacting concrete using intelligent computational modeling. *Computers, Materials & Continua*, vol. 53, no. 2, pp. 157-174.

**Eggers, J. J.; Girod, B.** (2001): Blind watermarking applied to image authentication. *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, pp. 1977-1980.

**Feichtenhofer, C.; Fan, H.; Malik, J.; He, K.** (2018): SlowFast networks for video recognition. *Computer Vision and Pattern Recognition*.

**Fridrich, J.** (1999): Protection of digital images using self-embedding. *Symposium on Content Security and Data Hiding in Digital Media*, New Jersey Institute of Technology.

**Fridrich, J.; Kodovsky, J.** (2012): Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868-882.

**Fu, H.; Gong, M.; Wang, C.; Batmanghelich, K.; Tao, D.** (2018): Deep ordinal regression network for monocular depth estimation. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2002-2011.

**Gautam, C.; Tiwari, A.; Leng, Q.** (2017): On the construction of extreme learning machine for online and offline one-class classification-an expanded toolbox.

*Neurocomputing*, vol. 261, pp. 126-143.

**Goldberg, Y.; Levy, O.** (2014): Word2vec explained: deriving Mikolov et al.'s negative-sampling word-embedding method. *Computation and Language*.

**Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D. et al.** (2014): Generative adversarial nets. *Advances in Neural Information Processing Systems*, pp. 2672-2680.

**Gunjal, B. L.; Mali, S. N.** (2015): MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain. *Springer Plus*, vol. 4, no. 1, pp. 126.

**Gurusamy, R.; Subramaniam, V.** (2017): A machine learning approach for MRI brain tumor classification. *Computers, Materials & Continua*, vol. 53 no. 2, pp. 91-108.

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

**He, H.; Chen, F.; Tai, H. M.; Kalker, T.; Zhang, J.** (2012): Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 185-196.

**He, H. J.; Zhang, J. S.; Tai, H. M.** (2009): Self-recovery fragile watermarking using block-neighborhood tampering characterization. *International Workshop on Information Hiding*, pp. 132-145.

**He, K.; Zhang, X.; Ren, S.; Sun, J.** (2016): Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770-778.

**Hinton, G. E.; Salakhutdinov, R. R.** (2006): Reducing the dimensionality of data with neural networks. *Science*, vol. 313, no. 5786, pp. 504-507.

**Hjelm, R. D.; Jacob, A. P.; Che, T.; Trischler, A.; Cho, K. et al.** (2017): Boundary-seeking generative adversarial networks. *Machine Learning*.

**Holub, V.; Fridrich, J.** (2012): Designing steganographic distortion using directional filters. *IEEE International Workshop on Information Forensics and Security*, vol. 2, no. 4, pp. 234-239.

**Holub, V.; Fridrich, J.** (2013): Random projections of residuals for digital image steganalysis. *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996-2006.

**Holub, V.; Fridrich, J.** (2015a): Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219-228.

**Holub, V.; Fridrich, J.** (2015b): Phase-aware projection model for steganalysis of JPEG images. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 9409.

**Holub, V.; Fridrich, J.; Denmark, T.** (2014): Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1.



- Hu, D.; Wang, L.; Jiang, W.; Zheng, S.; Li, B.** (2018): A novel image steganography method via deep convolutional generative adversarial networks. *IEEE Access*, vol. 6, pp. 38303-38314.
- Jaeger, P. F.; Kohl, S. A.; Bickelhaupt, S.; Isensee, F.; Kuder, T. A. et al.** (2018): Retina U-Net: Embarrassingly simple exploitation of segmentation supervision for medical object detection. *Computer Vision and Pattern Recognition*.
- Johnson, N.; Jajodia, S.** (1998): Exploring steganography: Seeing the unseen. *Computer*, vol. 31, pp. 2634.
- Kandi, H.; Mishra, D.; Gorthi, S. R. S.** (2017): Exploring the learning capabilities of convolutional neural networks for robust image watermarking. *Computers & Security*, vol. 65, pp. 247-268.
- Kang, S. I.; Lee, I. Y.** (2006): A study on the electronic voting system using blind signature for anonymity. *International Conference on Hybrid Information Technology*, vol. 2, pp. 660-663.
- Karras, T.; Laine, S.; Aila, T.** (2018): A style-based generator architecture for generative adversarial networks. *Neural and Evolutionary Computing*.
- Ke, Y.; Zhang, M.; Liu, J.; Su, T.** (2017): Generative steganography with Kerckhoffs' principle based on generative adversarial networks. *Multimedia*.
- Kim, T.; Cha, M.; Kim, H.; Lee, J. K.; Kim, J.** (2017): Learning to discover cross-domain relations with generative adversarial networks. *Computer Vision and Pattern Recognition*.
- Kingma, D. P.; Welling, M.** (2013): Auto-encoding variational bayes. *Machine Learning*.
- Kodovský, J.; Fridrich, J.** (2011): Steganalysis in high dimensions: Fusing classifiers built on random subspaces. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 7880.
- Kodovský, J.; Fridrich, J.** (2012): Steganalysis of JPEG images using rich models. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 8303.
- Kodovský, J.; Fridrich, J.** (2013): Quantitative steganalysis using rich models. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 8665.
- Kodovský, J.; Fridrich, J.; Holub, V.** (2012): Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432-444.
- Li, C.; Jiang, Y.; Cheslyar, M.** (2018): Embedding image through generated intermediate medium using deep convolutional generative adversarial network. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 313-324.
- Li, Z.; Chen, X.; Pan, X.; Zeng, X.** (2009): Lossless data hiding scheme based on adjacent pixel difference. *International Conference on Computer Engineering and Technology*, vol. 1, pp. 588-592.
- Li, D.; Deng, L.; Gupta, B. B.; Wang, H.; Choi, C.** (2018): A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. *Information Sciences*. <https://doi.org/10.1016/j.ins.2018.02.060>.

**Liang, Z.; Jiang, K.; Chen, H.; Zhu, J.; Li, Y.** (2018): Deep reinforcement learning in portfolio management. *Portfolio Management*.

**Liu, M. M.; Zhang, M. Q.; Liu, J.; Zhang, Y. N.; Ke, Y.** (2017): Coverless information hiding based on generative adversarial networks. *Cryptography and Security*.

**Liu, N.; Zhang, Y.; Chen, Z.; Zhang, S.** (2009): Chaos-based semi-blind watermarking for CAD models. *WRI Global Congress on Intelligent Systems*, vol. 3, pp. 411-414.

**Liu, W.; Anguelov, D.; Erhan, D.; Szegedy, C.; Reed, S. et al.** (2016): SSD: Single shot multibox detector. *European Conference on Computer Vision*, pp. 21-37.

**Liu, Z.; Luo, P.; Wang, X.; Tang, X.** (2015): Deep learning face attributes in the wild. *Proceedings of the IEEE International Conference on Computer Vision*, pp. 3730-3738.

**Le, H.; Pham, Q.; Sahoo, D.; Hoi, S. C.** (2018): URLNet: Learning a url representation with deep learning for malicious URL detection. *Cryptography and Security*.

**Long, Y.; Liu, Y.** (2018): Text coverless information hiding based on word2vec. *International Conference on Cloud Computing and Security*, pp. 463-472.

**Ma, S.; Guan, Q.; Zhao, X.; Liu, Y.** (2018): Weakening the detecting capability of CNN-based steganalysis. *Multimedia*.

**Ma, S.; Guan, Q.; Zhao, X.; Liu, Y.** (2018): Adaptive spatial steganography based on probability-controlled adversarial examples. *Multimedia*.

**Mao, X.; Li, Q.; Xie, H.; Lau, R. Y.; Wang, Z. et al.** (2017): Least squares generative adversarial networks. *IEEE International Conference on Computer Vision*, pp. 2813-2821.

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

**Mielikainen, J.** (2006): LSB matching revisited. *IEEE Signal Processing Letters*, vol. 13, pp. 285-287.

**Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A. A.; Veness, J. et al.** (2015): Human-level control through deep reinforcement learning. *Nature*, vol. 518, no. 7540, pp. 529.

**Mobadersany, P.; Yousefi, S.; Amgad, M.; Gutman, D. A.; Barnholtz-Sloan, J. S. et al.** (2018): Predicting cancer outcomes from histology and genomics using convolutional networks. *Proceedings of the National Academy of Sciences*, vol.115, no. 13, pp. E2970-E2979.

**Montavon, G.; Müller, K. R.** (2012): Deep Boltzmann machines and the centering trick. *Neural Networks: Tricks of the Trade*, pp. 621-637.

**Mun, S. M.; Nam, S. H.; Jang, H. U.; Kim, D.; Lee, H. K.** (2017): A robust blind watermarking using convolutional neural network. *Multimedia*.

**Nazari, M.; Sharif, A.; Mollaefar, M.** (2017): An improved method for digital image fragile watermarking based on chaotic maps. *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16107-16123.

**Nguyen, B. C.; Yoon, S. M.; Lee, H. K.** (2006): Multi bit plane image steganography. *International Workshop on Digital Watermarking*, pp. 61-70.

**Pevný, T.; Filler, T.; Bas, P.** (2010): Using high-dimensional image models to perform highly undetectable steganography. *Lecture Notes in Computer Science*, vol. 6387, pp.

161-177.

**Pevný, T.; Fridrich, J.** (2007): Merging Markov and DCT features for multi-class JPEG steganalysis. *International Society for Optics and Photonics on Security, Steganography, and Watermarking of Multimedia Contents*, vol. 6505.

**Provost, N.; Honeyman, P.** (2001): Detecting steganographic content on the internet. *Chemia Analityczna*, vol. 46, no. 4, pp. 569-577.

**Provost, N.; Honeyman, P.** (2003): Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, vol. 99, no. 3, pp. 32-44.

**Qian, J.; Du, H.; Hou, J.; Chen, L.; Jung, T. et al.** (2017): VoiceMask: Anonymize and sanitize voice input on mobile devices. *Cryptography and Security*.

**Qian, Y.; Dong, J.; Wang, W.; Tan, T.** (2015): Deep learning for steganalysis via convolutional neural networks. *Media Watermarking, Security, and Forensics, International Society for Optics and Photonics*, vol. 9409.

**Qian, Y.; Dong, J.; Wang, W.; Tan, T.** (2016): Learning and transferring representations for image steganalysis using convolutional neural network. *IEEE International Conference on Image Processing*, pp. 2752-2756.

**Qin, Y.; Kamnitsas, K.; Ancha, S.; Nanavati, J.; Cottrell, G. et al.** (2018): Autofocus layer for semantic segmentation. *Computer Vision and Pattern Recognition*.

**Radford, A.; Metz, L.; Chintala, S.** (2015): Unsupervised representation learning with deep convolutional generative adversarial networks. *Machine Learning*.

**Rahim, R.; Nadeem, M. S.** (2017): End-to-end trained CNN encode-decoder networks for image steganography. *Computer Vision and Pattern Recognition*.

**Rahman, M. M.; Ahammed, M. S.; Ahmed, M. R.; Izhar, M. N.** (2017): A semi blind watermarking technique for copyright protection of image based on DCT and SVD domain. *Global Journal of Research in Engineering*, vol. 16, no. 7-F.

**Rajpurkar, P.; Irvin, J.; Zhu, K.; Yang, B.; Mehta, H. et al.** (2017): Chexnet: Radiologist-level pneumonia detection on chest x-rays with deep learning. *Computer Vision and Pattern Recognition*.

**Redmon, J.; Divvala, S.; Girshick, R.; Farhadi, A.** (2016): You only look once: Unified, real-time object detection. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 779-788.

**Ren, S.; He, K.; Girshick, R.; Sun, J.** (2015): Faster R-CNN: Towards real-time object detection with region proposal networks. *Advances in Neural Information Processing Systems*, pp. 91-99.

**Roddick, T.; Kendall, A.; Cipolla, R.** (2018): Orthographic feature transform for monocular 3D object detection. *Computer Vision and Pattern Recognition*.

**Rouhani, B. D.; Chen, H.; Koushanfar, F.** (2018): Deepsigns: A generic watermarking framework for IP protection of deep learning models. *Cryptography and Security*.

**Ronneberger, O.; Fischer, P.; Brox, T.** (2015): U-net: Convolutional networks for biomedical image segmentation. *International Conference on Medical Image Computing and Computer-Assisted Intervention*, vol. 9351, pp. 234-241.

- Russakovsky, O.; Deng, J.; Su, H.; Krause, J.; Fei-Fei, L.** (2014): Imagenet large scale visual recognition challenge. *International Journal of Computer Vision*, vol. 115, pp. 3.
- Sak, H.; Senior, A.; Beaufays, F.** (2014): Long short-term memory recurrent neural network architectures for large scale acoustic modeling. *Fifteenth Annual Conference of the International Speech Communication Association*, pp. 338-342.
- Sallee, P.** (2003): Model-based steganography. *International Workshop on Digital Watermarking*, pp. 154-167.
- Salomon, M.; Couturier, R.; Guyeux, C.; Couchot, J. F.; Bahi, J. M.** (2017): Steganalysis via a convolutional neural network using large convolution filters for embedding process with same stego key: A deep learning approach for telemedicine. *European Research in Telemedicine*, vol. 6, no. 2, pp. 79-92.
- Sanh, V.; Wolf, T.; Ruder, S.** (2018): A hierarchical multi-task approach for learning embeddings from semantic tasks. *Computation and Language*.
- Shi, H.; Dong, J.; Wang, W.; Qian, Y.; Zhang, X.** (2017): SSGAN: secure steganography based on generative adversarial networks. *Pacific Rim Conference on Multimedia*, pp. 534-544.
- Simonyan, K.; Zisserman, A.** (2014): Very deep convolutional networks for large-scale image recognition. *Computer Vision and Pattern Recognition*.
- Talele, D. S. G. K.; Keskar, D. A.** (2010): Steganography security for copyright protection of digital images using DWT. *International Journal of Computer and Network Security*, vol. 2, pp. 4.
- Tan, S.; Li, B.** (2014): Stacked convolutional auto-encoders for steganalysis of digital images. *Signal and Information Processing Association Annual Summit and Conference*, pp. 1-4.
- Tang, W.; Tan, S.; Li, B.; Huang, J.** (2017): Automatic steganographic distortion learning using a generative adversarial network. *IEEE Signal Processing Letters*, vol. 24, no. 10, pp. 1547-1551.
- Uchida, Y.; Nagai, Y.; Sakazawa, S.; Satoh, S. I.** (2017): Embedding watermarks into deep neural networks. *Proceedings of the 2017 ACM on International Conference on Multimedia Retrieval*, pp. 269-277.
- Volkhonskiy, D.; Nazarov, I.; Borisenko, B.; Burnaev, E.** (2017): Steganographic generative adversarial networks. *Multimedia*.
- Wang, T. C.; Liu, M. Y.; Zhu, J. Y.; Liu, G.; Tao, A. et al.** (2018): Video-to-video synthesis. *Computer Vision and Pattern Recognition*.
- Wang, Q.; Chan, A. B.** (2018): CNN+CNN: Convolutional decoders for image captioning. *Computer Vision and Pattern Recognition*.
- Westfeld, A.** (2001): F5-A steganographic algorithm. *Information Hiding: 4th International Workshop*, vol. 2137, pp. 289.
- Wichers, N.; Villegas, R.; Erhan, D.; Lee, H.** (2018): Hierarchical long-term video prediction without supervision. *International Conference on Machine Learning*.
- Wu, H. Z.; Wang, H. X.; Shi, Y. Q.** (2016): Can machine learn steganography?-

implementing LSB substitution and matrix coding steganography with feed-forward neural networks. *Multimedia*.

**Wu, H. C.; Wu, N. I.; Tsai, C. S.; Hwang, M. S.** (2005): Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEEE Proceedings-Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611-615.

**Wu, S.; Zhong, S. H.; Liu, Y.** (2016): Steganalysis via deep residual network. *International Conference on Parallel and Distributed Systems*, pp. 1233-1236.

**Wu, S.; Zhong, S. H.; Liu, Y.** (2017): A novel convolutional neural network for image steganalysis with shared normalization. *Multimedia*.

**Wu, X.; Hu, J.; Gu, Z.; Huang, J.** (2005): A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters. *Proceedings of the 2005 Australasian Workshop on Grid Computing and E-Research*, vol. 44, pp. 75-80.

**Xia, Z.; Wang, X.; Sun, X.; Liu, Q.; Xiong, N.** (2016): Steganalysis of LSB matching using differences between nonadjacent pixels. *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 1947-1962.

**Xia, Z.; Wang, X.; Sun, X.; Wang, B.** (2014): Steganalysis of least significant bit matching using multi-order differences. *Security and Communication Networks*, vol. 7, no. 8, pp. 1283-1291.

**Xie, J.; He, T.; Zhang, Z.; Zhang, H.; Zhang, Z. et al.** (2018): Bag of tricks for image classification with convolutional neural networks. *Computer Vision and Pattern Recognition*.

**Xu, G.** (2017): Deep convolutional neural network to detect J-UNIWARD. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, pp. 67-73.

**Xu, G.; Wu, H. Z.; Shi, Y. Q.** (2016): Ensemble of CNNs for steganalysis: an empirical study. *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, pp. 103-107.

**Xu, G.; Wu, H. Z.; Shi, Y. Q.** (2016): Structural design of convolutional neural networks for steganalysis. *IEEE Signal Processing Letters*, vol. 23, no. 5, pp. 708-712.

**Yalçın, M. E.; Vandewalle, J.** (2002): Fragile watermarking and unkeyed hash function implementation for image authentication on CNN-UM. *Cellular Neural Networks and Their Applications*, pp. 399-406.

**Yang, B.; Deng, B.** (2006): Steganography in gray images using wavelet. *Proceedings of ISCCSP*.

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

**Yang, J.; Shi, Y. Q.; Wong, E. K.; Kang, X.** (2017): JPEG steganalysis based on densenet. *Multimedia*.

**Ye, J.; Ni, J.; Yi, Y.** (2017): Deep learning hierarchical representations for image steganalysis. *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545-2557.

**Yedroudj, M.; Comby, F.; Chaumont, M.** (2018): Yedrouj-net: An efficient CNN for spatial steganalysis. *IEEE International Conference on Acoustics, Speech and Signal*

Processing.

**Yang, Y.; Lalitha, A.; Lee, J.; Lott, C.** (2018): Automatic grammar augmentation for robust voice command recognition. *Computation and Language*.

**Yi, Z.; Zhang, H. R.; Tan, P.; Gong, M.** (2017): DualGAN: Unsupervised dual learning for image-to-image translation. *International Conference on Computer Vision*, pp. 2868-2876.

**Yu, J.; Zhan, Y.; Yang, J.; Kang, X.** (2016): A multi-purpose image counter-anti-forensic method using convolutional neural networks. *International Workshop on Digital Watermarking*, pp. 3-15.

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

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

**Zeng, J.; Tan, S.; Li, B.; Huang, J.** (2018): Large-scale jpeg image steganalysis using hybrid deep-learning framework. *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1200-1214.

**Zhang, J.; Huang, H.; Wang, L.; Lin, H.; Gao, D.** (2017): Coverless text information hiding method using the frequent words hash. *International Journal Network Security*, vol. 19, no. 6, pp. 1016-1023.

**Zhang, J.; Shen, J.; Wang, L.; Lin, H.** (2016): Coverless text information hiding method based on the word rank map. *International Conference on Cloud Computing and Security*, pp. 145-155.

**Zhang, R.; Dong, S.; Liu, J.** (2018): Invisible steganography via generative adversarial networks. *Multimedia Tools and Applications*, pp. 1-7.

**Zhang, R.; Zhu, F.; Liu, J.; Liu, G.** (2018): Efficient feature learning and multi-size image steganalysis based on CNN. *Multimedia*.

**Zheng, M.; Zhang, S. H.; Wu, S.; Jiang, J.** (2017): Steganographer detection via deep residual network. *IEEE International Conference on Multimedia and Expo*, pp. 235-240.

**Zhang, X.; Wang, S.** (2005): Steganography using multiple-base notational system and human vision sensitivity. *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 67-70.

**Zhou, Z.; Cao, Y.; Sun, X.** (2016): Coverless information hiding based on bag-of-words model of image. *Journal of Applied Sciences*, vol. 34, no. 5, pp. 527-536.

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

**Zhu, J. Y.; Park, T.; Isola, P.; Efros, A. A.** (2017): Unpaired image-to-image translation using cycle-consistent adversarial networks. *International Conference on Computer Vision*, pp. 2223-2232.

**Zhuang, J.; Yang, J.** (2018): ShelfNet for real-time semantic segmentation. *Computer Vision and Pattern Recognition*.