IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 14, 2020, accepted January 26, 2020, date of publication February 4, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971528

A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network

XINTAO DUAN[1], DAIDOU GUO[1], NAO LIU[1], BAOXIA LI[1], MENGXIAO GOU[1], AND CHUAN QIN[2]

[1]College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China
[2]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

Corresponding author: Xintao Duan (duanxintao@htu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672354, and in part by the Key Scientific Research Project of Henan Provincial Higher Education under Grant 19B510005 and Grant 20B413004.

ABSTRACT Image steganography is a technology that hides sensitive information into an image. The traditional image steganography method tends to securely embed secret information in the host image so that the payload capacity is almost ignored and the steganographic image quality needs to be improved for the Human Visual System(HVS). Therefore, in this work, we propose a new high capacity image steganography method based on deep learning. The Discrete Cosine Transform(DCT) is used to transform the secret image, and then the transformed image is encrypted by Elliptic Curve Cryptography(ECC) to improve the anti-detection property of the obtained image. To improve steganographic capacity, the SegNet Deep Neural Network with a set of Hiding and Extraction networks enables steganography and extraction of full-size images. The experimental results show that the method can effectively allocate each pixel in the image so that the relative capacity of steganography reaches 1. Besides, the image obtained using this steganography method has higher Peak Signal-to-Noise Ratio(PSNR) and Structural Similarity Index(SSIM) values, reaching 40dB and 0.96, respectively.

INDEX TERMS Image steganography, DCT, ECC, deep neural network, SegNet.

I. INTRODUCTION

In the context of informatization, the development of network security and multimedia has brought a great convenience to people's daily life and work, but it has also exposed more and more security issues. For example, involving personal privacy and trade secrets, and even military defense security, once the confidential information is leaked, the consequences are immeasurable.To further cope with the challenges in the field of information security, in recent years, information steganography has received more and more attention and research.

Through some features of the host image, the secret image is hidden into the host image, which is image steganography. During the transmission of the host image, the detector does not observe any abnormality. Finally,the secret image can be safely transmitted to the receiver. Traditional image steganography schemes are generally implemented by artificial design algorithms, such as the space domain-based LSB [1], [2], HUGO [3], WOW [4] hidden methods and transform domain-based DCT [5], DWT [6] and DFT [7] hidden methods. Besides, many studies based on compressed domains have also been proposed, as in [8], To get the recovery of VQ images, a new image steganography scheme is based on traditional VQ and repair technology is proposed. References [9], [10] proposed block-cutting compression (BTC-Compressed) image for image steganography and article [11] further improvements to the work of [9], [10], their steganography is based on the implementation of the compression domain. Also, other steganographic schemes have been proposed. Reference [12] proposed two improved RDH technologies based on dual images, and this research mainly improved two aspects: the first one, dual stego-image based pixel pair LSB matching

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

with reversibility; the other one, dual stego-image based modified LSB matching with reversibility.In order to improve the information embedding ability, [13] proposed an image steganography technology based on the principle of pixel overlapping. This method has higher PSNR while improving the embedding ability.

In the information hiding system, there are mainly three indicators: Security, Capacity and Imperceptibility. The relationship between the three parameters is reciprocally constrained. For example, as the capacity increases, security and imperceptibility will reduce and vice versa.

At present, there are two challenges to restrict steganography performance. One is the case that the more steganographic information is, the worse the quality of steganographic images and the lower the security of steganographic images. The other is the case that the host image itself is very important, hiding information into noisy and rich semantic regions are more secure than information hiding in smooth regions. Therefore, to cope with the existing steganographic challenges, a series of deep models such as Generative Adversarial Networks(GAN) [14] and Convolutional Neural Networks(CNN) [15] have been introduced into the field of image steganography, further broadening the field. Taking advantage of this opportunity, more and more image steganography based on deep learning has been proposed. In [16], a GAN-based steganographic enhancement algorithm is proposed, which uses traditional algorithms to hide secret messages into the generated image and enhances security. However, the image generated by this method is semantically deformed and can easily cause suspicion. Knowledge of a hybrid deep learning framework rich model for JPEG image steganalysis was proposed in [17]. In [18], a selection region and a CNN-based combination method are proposed for adaptive steganalysis. Also, article [19] proposes a CNN structure (called XuNet) that achieves performance comparable to traditional Spatial Rich Models (SRM). In [20], coverless information steganography based on Deep Convolution Generation Against Network (DCGAN) is proposed. In this process, there is no need to modify the host information, and it has high security, but the steganographic capacity is still limited.

In the above-mentioned traditional steganography methods and steganography methods based on deep learning, there are such problems: as the steganography quality increases, the corresponding steganography capacity will be smaller; when the steganography capacity increases, the steganography quality will decrease, the reduction of steganography quality means that its imperceptibility will be broken, and steganography security will be affected. To achieve the best possible the balance between steganographic quality and steganographic capacity, the research in this paper aims to further improve the steganographic capacity of images while ensuring security. Therefore, we propose an image steganography framework based on the deep model and ECC [21]: The secret image after the DCT is further encrypted using an ECC method of the image, making the secret image unrecognizable to the HVS. Compared to Ron Rives Adi Shamir Leonard Adleman(RSA) [22], the advantage of ECC can use a shorter key to achieve comparable or even higher security. Deep Neural Network(This study uses the SegNet structure) is used to realize the hiding of image information. In this deep model, two network modules are included: Hiding network and Extraction network. The Hidding network hides the encrypted image into the host image through the convolution operation sends the hidden result to the receiver, and then extracts the encrypted image using the Extraction network based on the convolution operation.

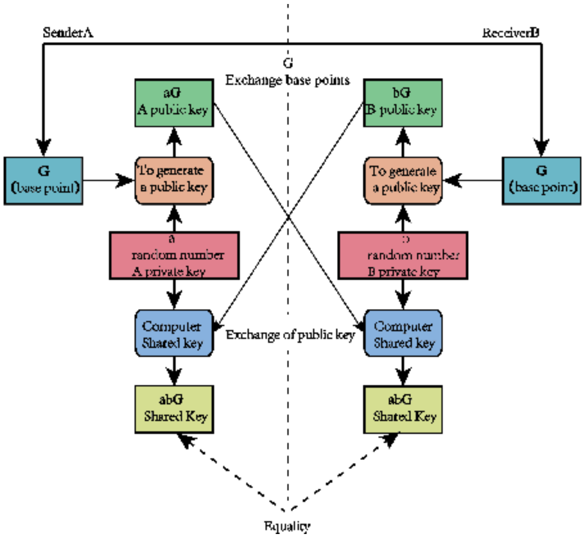


FIGURE 1. Elliptical encryption mechanism.

The organization of the article is as follows: The second section introduces preliminaries' work. The third section gives details of the proposed method. The fourth section describes the results and analysis of the implementation. The fifth section is the conclusion.

II. PRELIMINARIES

A. ENCRYPT IMAGES WITH THE ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

ECC [23]is an asymmetric encryption algorithm based on elliptic curve mathematics. Elliptic curve ciphers are currently being widely used. For example, in SSL/TLS, elliptic curve Diffie-Hellman key exchange is utilized. The specific algorithm flow is shown in Fig 1. The ECC algorithm has relatively higher security than the RSA algorithm and the Digital Signature Algorithm (DSA) [22]. In other words, the Elliptic Curve Cryptography key is short but strong. Therefore, ECC has attracted wide attention in the fields of certification [24], secure communication [25] and signal processing [26].

In recent years, many scholars have proposed image encryption methods based on ECC features. For example, [27] proposed an asymmetric image encryption algorithm based on ECC. The sender and receiver have agreed to use elliptic curve points based on Diffie-Hellman public key sharing techniques. To reduce the time it takes to encrypt, the sender combines the pixel values and converts them into large integers, after which the sender encrypts the large integers with ECC and chaotic systems. Encrypted images are obtained from encrypted large integers. Aiming at the potential security problems of key management and distribution of symmetric image encryption schemes, [28] proposed an asymmetric image encryption method based on the elliptic curve ElGamal (EC-ElGamal) cryptography and chaos theory. SHA-512 hash is used to generate the initial value of the chaotic system, and the crossover permutation of the chaotic index sequence is used to scramble the ordinary image. In addition, the generated scrambled image is embedded in the elliptic curve and encrypted by EC-ElGamal, which not only improves security but also helps resolve the key management problem. The method has high security, high efficiency, and strong robustness to the selection of plaintext attacks, making it a potential application for image security communication.

B. IMAGE STEGANOGRAPHY BASED ON DEEP LEARNING

Compared with the traditional steganography algorithm, the steganographic method based on deep learning can realize automatic hiding and extraction of image information. There is no need for manual intervention in the process of image steganography. Different information features and the strength of information embedding can be extracted by adjusting parameter information, which greatly improves the efficiency of image steganography.

Steganography based on Deep Neural Network models generally uses Neural Networks to find an embedded location information suitable for inclusion in images. For example, a deep steganography framework proposed by [29] in 2017 can embed the whole secret image into the host image. As shown in Fig 2. There are three parts in this network framework: pre-processing network, encoding network, and decoding network. The pre-processing network normalizes the secret image while extracting important features. The encoding network encodes the secret image and the host image of the same size to obtain a container image(steganographic image). At the same time, the model also trains a decoder corresponding to the encoder to extract the secret image. In the same year, [30] proposed another method that also includes a CNN structure for a set of encoders and decoders. It is proved by experiments that the steganographic image quality of this method is better than the former.

Based on the above two methods, [31] proposed to divide the host image into three channels: Y, U and V. Grayscale secret images are hidden by the encoder in host images. The U,V channel of the host image is then merged with the secret Y channel using the GAN model generator. The discriminator uses the steganographic analysis network of [19], which greatly improves the image generation effect. Also, there are other ways to use the deep learning model for information steganography. For example, [32] used the Extreme Learning Machine (ELM) to learn and select the best-embedded information position. This method had better visual effects and better imperceptibility. The MSA_ROI method proposed by [33] finds the complex object region in which information is steganized. Since there may be multiple objects in the image, multiple adaptive steganography algorithms are used to hide information in different object regions.

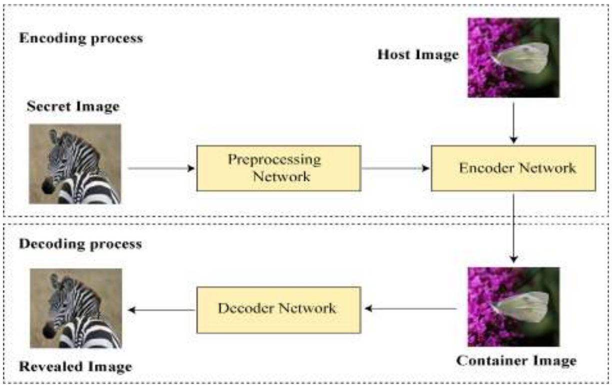


FIGURE 2. Deep steganography network framework.

C. SEGNET DEEP NEURAL NETWORK MODEL

SegNet [34] is a Fully Convolutional Neural Network, which was first used in the field of image segmentation. The main structures include an encoder, decoder, and a pixel-level classification layer. The coding network is used to generate low-resolution features and the decoder's role is to map this coarse feature to the pixel-level classification across the entire input image-level resolution feature map. The most iconic point of SegNet is that the decoder samples its low-resolution input feature map. In a word, it uses a pooled index to achieve nonlinear Upsampling. The pooled index is corresponding to the decoder. The encoder performs the calculation of the max-pooling operation. This eliminates the need to learn upsampling. The feature map after Upsampling is sparse, so a convolution operation is then performed using a trainable convolution kernel to generate a dense feature map. As shown in Fig 3, the left side is a convolution extraction feature, which increases the receptive field by pooling, and the picture becomes smaller, which is the encoding process. On the right are deconvolution and Upsampling. The features of the image classification are reproduced by deconvolution, and the Upsampling is restored to the original size of the image,which is a decoding process. Finally, the maximum value of different classifications is output by Softmax, and finally, the segmentation map is obtained.

III. PROPOSED IMAGE STEGANOGRAPHY SCHEME

In this section, we will provide a detailed description and explanation of each component of the proposed steganography framework.

A. OVERALL DESIGN IDEAS

As shown in Fig 4. In this framework, the hiding network and the revealed network are trained simultaneously,

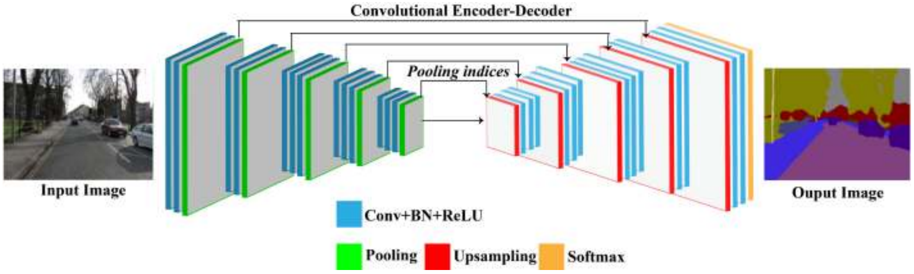


FIGURE 3. SegNet network model applied to image segmentation.

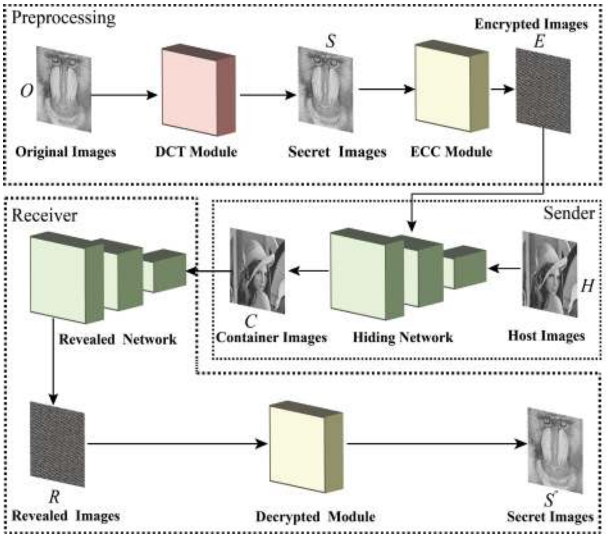


FIGURE 4. Flow chart of the proposed scheme.

and both are pre-trained. the proposed image steganography framework mainly includes three stages:

1) In the preprocessing stage of the image, an original image O of size M × N(M = N) is subjected to DCT and ECC to obtain a secret image S (The image is obtained by inverse DCT) and an encrypted image E.
2) The steganographic phase of the secret image, the Encrypted image E obtained in the previous stage is the secret image to be hidden, input it and the host image H into the hiding network of the SegNet network structure for information steganography, and finally get a container image C.
3) The extraction phase of the secret image, the container image C is processed through the revealed network to obtain an reveale image R.R is not the final result, it needs to be decrypted by the decryption algorithm, and finally S' is obtained. The detailed description is detailed in sections B, C and D.

B. IMAGE PREPROCESSING

We combine the DCT and image ECC to encrypt the secret image. Encrypted images are pseudo-random and look like noise. This property preserves the visual quality of the secret image and makes it unrecognizable by the HVS. Therefore, it can be transmitted securely through the common channel. In this way, the privacy needs of the secret image are met. It is worth mentioning that the domain conversion of the DCT changes the structure of the secret image. This makes the algorithm more robust to steganographic analysis attacks.

Image Encryption via ECC(P* represent the public Key,n* represent the private key.):

1) Randomly add 1 or 2 to each pixel value of the image to be encrypted, and save the current channel number of the image.
2) Group the pixels and convert each group into a single large integer value. The pixel values for grouping are obtained by $grp = length\ [IntergerDigits\ [p, 258] - 1]$.
3) The results obtained in 2) were paired and stored as Pm.
4) Choose a random Key and calculate $KeyG$ and $KeyPb$, where $KeyPb$ is the receiver's public key.
5) Point addition of $keyPb$ for each Pm value and store it as cipher text Pc.
6) Convert the ciphertext list from 5) to a value between 0 and 255.
7) Fill each list to 0 to the left in 6).The number of these lists is less than $grp + 1$ element to make each list equal in length.
8) Flatten the list in 7), group them according to the number of image channels we have recorded, and then divide them into the width of the plain image.
9) Convert the value in 8) to an encrypted image.

C. STEGANOGRAPHY OF SECRET IMAGES

The classic structure of the encoder and decoder was first proposed by Hinton in 2006. Initially, this structure is not suitable for image segmentation, but image compression and denoising. Input a picture, through the downsampling code, to get a string of features smaller than the original image, this process is equivalent to compression, and then through the decoder, ideally restored to the original image.

In the study, a SegNet network based on the encoder-decoder network structure is also used to implement steganography of secret images. As shown in Fig 5. At the left end of the figure, first input two images of size M × N (M = N),and generate a 6-channel feature tensor (RGB images) or 2-channel feature tensor (Grayscale images) by concatenation convolution operation. Each encoder generates

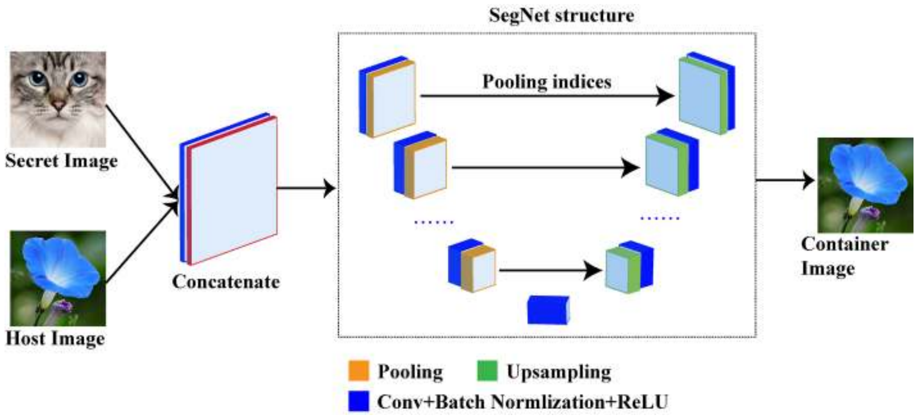


FIGURE 5. Hiding network structure.

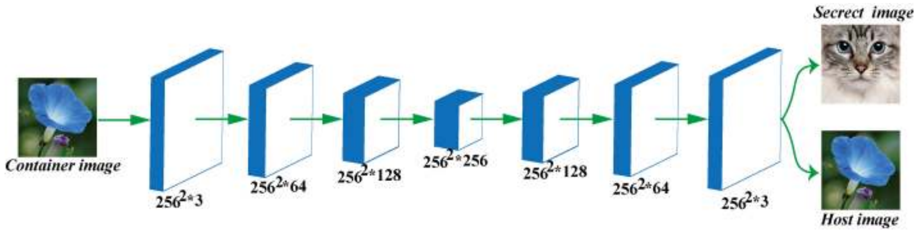


FIGURE 6. Revealed network structure.

TABLE 1. Hiding network structure.Conv means convolution and BN means batch normalization.

layer	*input size*	*filter size*	*channel*	*operation*	*pooling,upsampling and stride*	*output size*
Concatente Layer	256×256	4×4	6	Concatente Layer	-	128×128
layer1	128×128	4×4	64	Conv+BN+ReLU+Pooling	2×2,2	32×32
layer2	32×32	4×4	256	Conv+BN+ReLU+Pooling	2×2,2	8×8
layer3	8×8	4×4	512	Conv+BN+ReLU+Pooling	2×2,2	2×2
layer4	2×2	4×4	512	Conv+BN+ReLU+Pooling	2×2,2	4×4
layer5	4×4	4×4	512	Upsampling+Conv+BN+ReLU	2×2,2	16×16
layer6	16×16	4×4	1024	Upsampling+Conv+BN+ReLU	2×2,2	64×64
layer7	64×64	4×4	256	Upsampling+Conv+BN+ReLU	2×2,2	256×256
layer8	256×256	4×4	64	Upsampling+Conv+BN+ReLU+Softmax	2×2,2	256×256
layer9	256×256	4×4	3	Output	-	256×256

a series of feature maps through a set of convolutions, followed by batch normalization, ReLU activation function, and max-pooling layer (2×2, stride $= 2$). The original SegNet network uses the same convolution, which achieves the same size as the original image after the volume and operation. Max- pooling layer is used to achieving spatial invariance on small space movements, and there is a larger receptive field in feature mapping, and the 2×2 pooling window can be implemented with 2bit, which makes the efficiency higher. In the decoder on the right, the same applies to the same convolution, followed by pooling and upsampling. The feature map is upsampled according to the largest pooled index saved in the coding feature map. As shown in Table 1.

As shown in Fig 7, the generated sparse feature map is outputted through a series of trainable convolution kernels, and then the batch is returned. The normalization process regularization weakens the overfitting.

Since the network is based on the structure of the encoder-decoder, the container image of the intermediate representation is required to be as similar as possible to the Host image, and can be expressed by the following formula (1).

$$L(H, C, E, R) = ||H - C|| + \beta||E - R|| \tag{1}$$

where H and E represent the host image and the encrypted image, respectively, and how β balances their reconstruction errors. $\|H - C\|$ does not apply to the weight of the extraction network that accepts the container image and extracts the encrypted image, that is, its weight is not shared with the revealed network. All networks accept the error signal $\beta\|E - R\|$, so that the two networks will continuously adjust the error loss of the encrypted image and the host image through training to ensure that the encrypted image can be completely encoded into the host image. In addition,

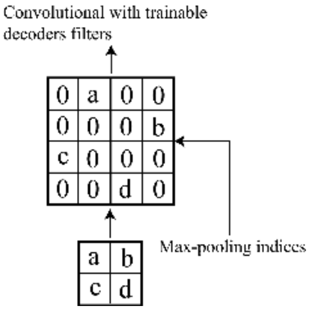


FIGURE 7. **Decoding process. a, b, c, and d correspond to feature map values. In this network, the max-pooling indices is used to upsampling feature maps, and a trainable decoder filter library are used for convolution.**

the cross-entropy cost function is mainly used:

$$L = -\sum_{c=1}^{M} y_c \log(p_c) \tag{2}$$

where M is the number of samples.

D. SECRET IMAGE EXTRACTION

The secret image extraction process refers to the network model of [35], as shown in Fig 6. In this network structure, the secret image is accurately extracted by 6 convolutional layers. On CNN, the Dropout operation is used. The activation functions and the pooling layer enhances the nonlinear learning ability of the network. The purpose of CNN is to use nonlinear features to learn the fitting parameters. Learn the weighting parameters in each layer of the network to accommodate the mapping between input and output 3 × 3. In this network, the filter size of each convolutional layer is designed to be 3×3, and each convolution layer is followed by a ReLU activation function and a batch normalization operation. In the left and right blocks of the network, the feature vectors of 64 components are mapped to the required number of categories using a convolution of 3 × 3, and the secret image and the host image are calculated using the Sigmoid activation function.In this network, stride is set to 1 and padding is set to 1, so it is guaranteed that the size of the image remains the same during the convolution process. As shown in Table 2.

Image Decryption via ECC(P* represent the public Key,n* represent the private key.):

1) Obtain the pixel values of the encrypted image, group them with $grp + 1$ pixels, and form a large integer value for each group with 256 as the base, and record the number of channels of the encrypted image at the same time.
2) Pair the integer values obtained in 1).
3) Multiply *KeyG* and *nB*, where *nB* is the receiver's private key.
4) Perform a point subtraction between the value in 2) and the value in 3).
5) From 4), use the base 258 to get a value between 0 and 255, and subtract the random number 2 from each value.
6) Group the flattened values obtained in 5) according to the number of recorded encrypted image channels and divide them into the width of the encrypted image.
7) Convert the value in 6) to a plain text image.

IV. EXPERIMENTAL ANALYSIS

In this part, we will evaluate the performance of the proposed algorithm through experimental simulation. In this experiment, the experimental environment is Python 3.6 programming languages and the Pytorch framework under the Ubuntu operating system. The experimental device has dual NVIDIA 1080 Ti GPU and 16G RAM, 1TB HDD and 256G SSD.

A. IMAGE PREPROCESSING RESULTS

The visual image of the image preprocessing results is shown in Fig 8.

In Fig 8, six Grayscale images are listed as the original images (Airplane, Baboon, Barbara, Goldhill, Man, and Yacht, respectively), and their sizes are uniformly set such that the above-mentioned images are derived from globally accepted image datasets [36].The first row original images (that is, secret images), and the second and third row is the result of DCT and inversed DCT of an image. The fourth row is the product graph of the ECC. It is worth taking note that the result of the third line is to make a hidden secret image (S').

B. IMAGE STEGANOGRAPHY AND RESULT ANALYSIS USING DEEP NEURAL NETWORK

Our image data comes from the ImageNet database. We extracted 60,000 images from it (55,000 for training and 5,000 for testing). The initial learning rate for the overall network is set to 0.001 and the hyperparameter β is set to 0.75. The Adam optimization method is utilized to automatically adjust the learning rate so that network parameters can be learned smoothly. The number of images per batch is set to 8, and the network trains 300 iterations. Fig 9 shows image hiding for three iterations of Epoch0, Epoch50, and Epoch100. It can be found that the initial iteration effect of the training effect shows that starting from the noise, as the number of iterations increases, the training effect will be better and better. When Epoch is 50 times, we can see that the noise is greatly reduced. When iterating to Epoch100, the noise is invisible to the human eye, achieving an indistinguishable effect of the HVS compared to the original image. After 100 iterations of data iterations, the network model tends to be robust at this time. Fig 10 shows the training effect after the model tends to be robust. The first to fourth rows of the graph are Host images, Container images, Secret images, and Revealed images. This is what we can find, the steganography and extraction of the image work well. To further analyze the quality of its generation, We randomly extracted a set of images to depict the distribution of histograms in a number of group experiments.As shown in Fig 11.

TABLE 2. Revealed network structure. Conv means convolution and BN means batch normalization.

layer	*input size*	*filter size*	*channel*	*stride*	*padding*	*operation*	*output size*
layer1	256×256	3×3	3	1	1	Conv+ReLU+BN	256×256
layer2	256×256	3×3	64	1	1	Conv+ReLU+BN	256×256
layer3	256×256	3×3	128	1	1	Conv+ReLU+BN	256×256
layer4	256×256	3×3	256	1	1	Conv+ReLU+BN	256×256
layer5	256×256	3×3	128	1	1	Conv+ReLU+BN	256×256
layer6	256×256	3×3	64	1	1	Conv+ReLU+BN	256×256
layer7	256×256	3×3	3	1	1	Sigmoid	256×256

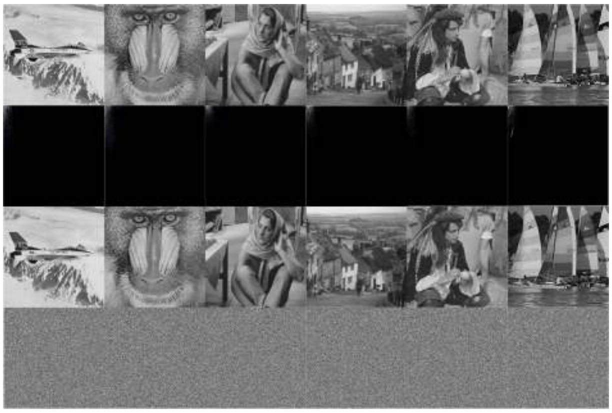


FIGURE 8. Image preprocessing effect.

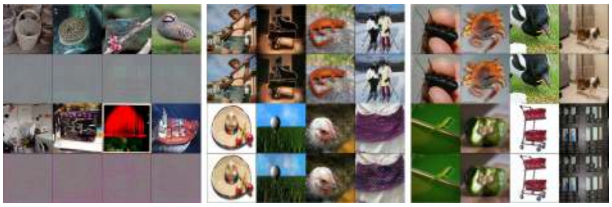


FIGURE 9. The model hide the effect in the middle of training (The first to fourth rows represent: Host Images, Container Images, Secret Images, and Revealed Images. The three blocks from left to right represent Epoch0, Epoch50, and Epoch100.

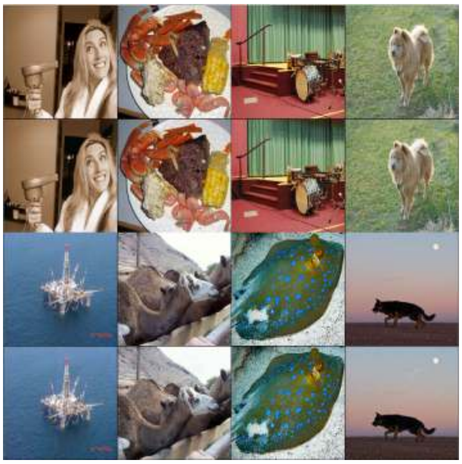


FIGURE 10. The model hide results after stable training.

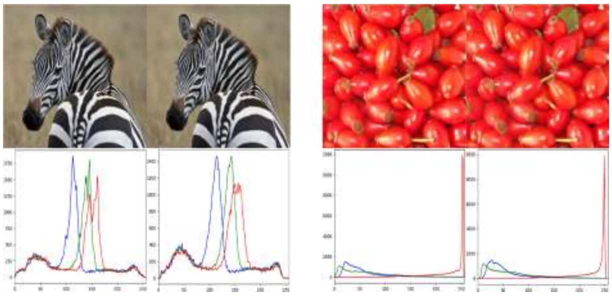


FIGURE 11. The difference between cover image and secret image before and after steganography: (left) *Host image, Container image and their histogram*,(right) *Secret image,Revealed imageand their histogram*.

Through the three-channel decomposition of R, G, and B of the above image, the three color channels of Host image and Container image and Secret image and Revealed image have little change, and the trend is close. The final experimental results prove that the Deep Neural Network model does not randomly embed the secret information bits. But follows the principle of supplementing pixels, and selects the pixel bits that can be modified on the image for embedding.

The above is the training and analysis process of Deep Neural Network for color image steganography and extraction. Fig 12 below shows the implementation and analysis of the Grayscale image for the entire experimental process. We selected 12 Grayscale images from 20 classic Grayscale images for the experiment. As you can see from Fig 12, when an original image is DCT transformed, it will get a secret image (the first row). The secret image is then ECC encrypted to obtain an encrypted image that requires steganography (the fourth row). The host image (the second row) is sent to the already trained network model along with the encrypted image, and finally, the container image (the third row) and the extracted image (the fifth row) are obtained. The decrypted image is obtained by ECC decryption (the sixth row). Fig 13 shows that we randomly extracted a set of experiments from the experiment for analysis. Whether it is observed from the human visual system or the frequency distribution histogram, we can find that the experimental method has good steganography and extraction effects.

C. STEGANOGRAPHIC RESULTS PEAK SIGNAL-TO-NOISE RATIO ANALYSIS (PSNR)

In general, the compressed image must be different from the original image. Therefore, the PSNR is usually used to evaluate the quality of an image after compression compared to the

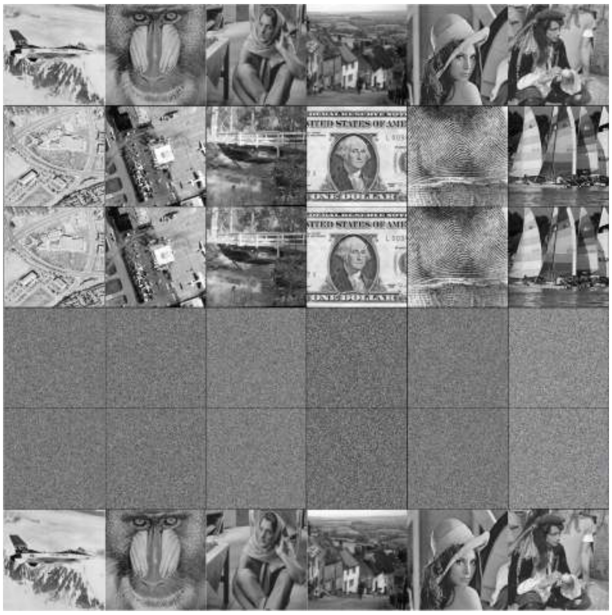


FIGURE 12. Overall structure experimental image (The first to sixth rows represent: Secret Images, Host Images, Container Images, Encrypted Images, Revealed Images and Decrypted Imges.)

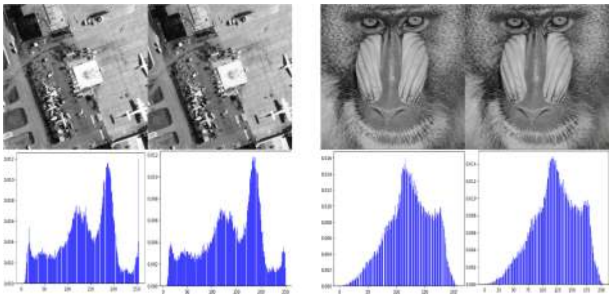


FIGURE 13. The difference between Host image and secret image before and after steganography: (left) *Host image, Container image and their histogram*, (right) *Secret image, Decrypted image and their histogram*.

original image. The higher the PSNR value, the smaller the distortion after compression. In the case of image steganography, the secret image is destructive noise, which reduces the quality of the steganographic image. Therefore, a higher PSNR indicates that the distortion of the secret image caused by the secret image is small. In other words, this standard measures the difference between a carrier image and a steganographic image.

Here two main values are defined. One is the mean squared MSE and the other is the peak signal-to-noise ratio (PSNR). The formula is as follows:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}||H(i,j){-}S(i,j)^2|| \tag{3}$$

Among them, H and S represent the host image and the secret image, respectively, and their sizes are set to the same. MSE indicates the mean variance of the host image compared with the steganographic image.

TABLE 3. Calculation of PSNR values based on our proposed method.

Category	*Figure*	*PSNR Value*
Color1	Figure11(a)	PSNR=39.4977
Color2	Figure11(b)	PSNR=42.1262
Grayscale1	Figure13(a)	PSNR=42.0099
Grayscale2	Figure13(b)	PSNR=43.2591
Color Dateset	Average PSNR Value	PSNR=40.5726
Grayscale Dataset	Average PSNR Value	PSNR=43.1383

[1] Average PSNR value of Color Dataset:200 color images were randomly selected from the experimental results.

[2] Average PSNR value of grayscale Dataset:50 color images were randomly selected from the experimental results.

[3] The values in this table are obtained by calculating Secret image (S) and decrypted Secret image (S'); Host image (H) and Container image (C).

TABLE 4. Calculation of SSIM values based on our proposed method.

Category	*Figure*	*SSIM Value*
Color1	Figure11(a)	SSIM=0.9546
Color2	Figure11(b)	SSIM=0.9793
Grayscale1	Figure13(a)	SSIM=0.9789
Grayscale2	Figure13(b)	SSIM=0.9887
Color Dateset	Average SSIM Value	SSIM=0.9602
Grayscale Dataset	Average SSIM Value	SSIM=0.9683

[1] Average SSIM value of Color Dataset:200 color images were randomly selected from the experimental results.

[2] Average SSIM value of grayscale Dataset:50 color images were randomly selected from the experimental results.

[3] The values in this table are obtained by calculating Secret image (S) and decrypted Secret image (S'); Host image (H) and Container image (C).

$$PSNR = 10\log_{10}(\frac{MAX_I^2}{MSE}) \tag{4}$$

where MAX_I represents the maximum pixel value of the image. In other words,MAX_I is equal to $2^b - 1$ and b represent the number of bits per pixel. For grayscale images, the maximum pixel value is 255. For RGB images (each pixel has three color parameters of R, G, and B), the PSNR is defined similarly.

D. STRUCTURAL SIMILARITY INDEX ANALYSIS OF STEGANOGRAPHIC RESULTS (SSIM)

SSIM is an indicator used to measure the similarity of two images. The larger the value, the better. This criterion measures the quality of given image based on a reference distortion-free image. In the context of image steganography. the examined image is the stego image, and host image is considered as the reference image. This criterion is formally stated as follows:

$$SSIM(C,S) = \frac{(2\mu_C\mu_S + C_1)(2\sigma_{CS} + C_2)}{(\mu_C^2 + \mu_S^2 + C_1)(\sigma_C^2 + \sigma_S^2 + C_2)} \tag{5}$$

where C_1 and C_2 are two variables to stabilize the division with weak denominator. Moreover, μ and σ present the average and covariance of the variables.

The PSNR value and SSIM value are calculated from the host image and the container image (including the dense image) generated by the hiding network, and the secret image

TABLE 5. Steganographic capacity comparison result.

Method	*Absolute capacity(bytes/image)*	*Image size*	*Relative capacity(bytes/image)*
[20]	≥ 37.5	64×64	$9.16e-3$
[37]	3.72	$\geq 512 \times 512$	$1.42e-5$
[38]	1.125	512×512	$4.29e-6$
[39]	2.25	512×512	$8.58e-6$
[40]	64×64	800×800	$6.40e-3$
[41]	$1535 \sim 4300$	1024×1024	$1.46e-3 \sim 4.10e-3$
Ours	256×256	256×256	1

* Note:The above table describes that the steganography capacity we obtained is 1 because our experiments can achieve full-size steganography, which is obtained through the capacity calculation formula.

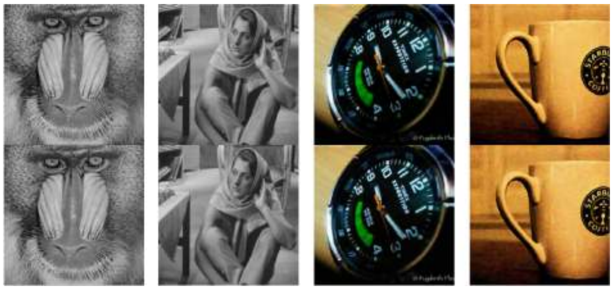


FIGURE 14. Randomly select images.From left to right are Baboon, women, watches and cups. The first row represents the secret image, and the second row represents the decrypted image.

and the decrypted image (decrypted by ECC) through the revealed network.The PSNR and SSIM values of ImageNet and grayscale images were calculated for the two parts of C and D respectively. It can be found that the PSNR value and the SSIM value are above (40/0.96) for both color image and grayscale image. From the comparison results of color images and grayscale images, whether it is for complex images or simple images, or color images and grayscale images, the model is applicable. We also calculate the image information payload capacity of this method by the following formula.

$$payload\ capacity = (1 - \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left|S_{i,j} - R_{i,j}\right|}{N \times M}) \times 8 \times 3(bpp) \quad (6)$$

where payload capacity refers to the number of bits of information contained in each pixel.N and M represent the width and height of the image, respectively.S and R denote the secret image and the decrypted image, respectively.We selected four groups from the experiment to calculate the payload capacity. The extracted images are shown in Fig 14, and the calculation results are shown in Table 6 (Note: The calculation data in this table is taken from Fig 14.).

In addition, for other natural images, hiding and extraction are good. As shown in Fig 15.

E. STEGANOGRAPHIC CAPACITY ANALYSIS

The steganographic method using the deep network-based information steganography method is higher than the traditional artificially designed embedded algorithm. The formula is as follows:

TABLE 6. Payload capacity calculation result.

Category	*Name*	*payload capacity(bpp)*
Grayscale1	Baboon	23.064 bpp
Grayscale2	woman	23.140 bpp
Color1	watches	23.280 bpp
Color2	cups	23.592 bpp

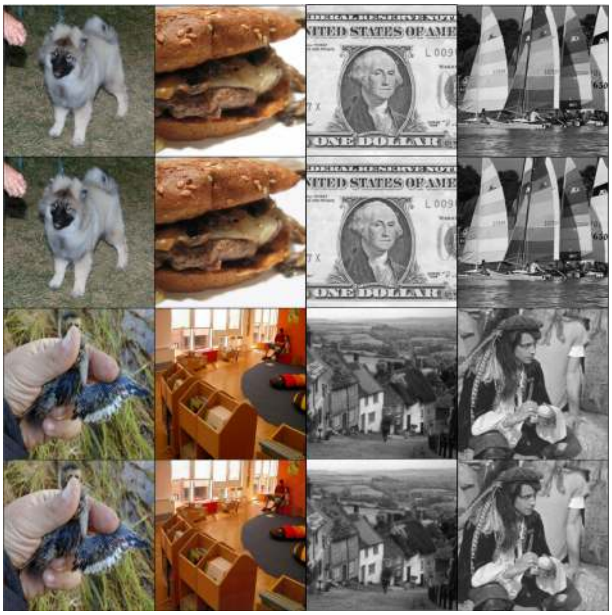


FIGURE 15. Random image test results.

$$Relative\ capacity = \frac{Absolute\ capacity}{The\ size\ of\ the\ image} \quad (7)$$

Our method compresses and distributes the secret image pixel information on all available bits of the steganographic image, so the relative capacity is 1 byte/pixel. According to Table 5, the steganographic capacity of our proposed method is much larger than Several other methods. This is also a major advantage of image steganography based on Deep Neural Network.

F. STATISTICAL ANALYSIS

StegExpose [42] is a steganalysis tool for detecting LSB (least significant bit) steganography in lossless images such as PNG and BMP.It can analyze LSB steganography images

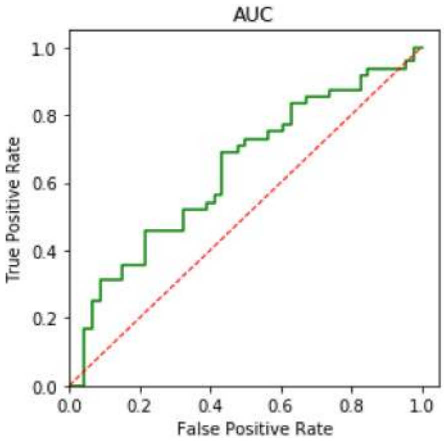


FIGURE 16. **ROC Curves: Detecting Steganography via StegExpose. (Note: In the statistical analysis of this figure, the data includes gray images and color images that have not been steganized and gray images and color images that have been steganized.)**

in a timely and efficient manner using a proven attack. When steganalysis methods are intelligently combined, they can produce more accurate results.StegExpose is currently a more general steganographic analysis tool. This article was tested with StegExpose. Four detection methods are included in the tool: sample pair analysis [43], RS analysis [44], chi-square attack [45] and primary sets [46]. The detection threshold is its hyperparameter, which is used to balance the True positive rate and False positive rate of StegExpose results. Fig 16 is an ROC curve. Among them, "True positive" represents an embedded image that is correctly identified as having hidden data inside, and "False positive" represents a clean graphic that is incorrectly classified as an embedded image. The graph is drawn with a green polyline, indicating that StegExpose can only be a little better than random guessing (red lines). In other words, the proposed steganography method can better resist StegExpose attacks.

V. CONCLUSION

In this paper, a method based on Deep Neural Network Model for image steganography and extraction is proposed. In this method, DCT and an ECC technique of an image is utilized. First, the Original image are subjected to DCT and converted by ECC to obtain a Secret image that needs to be steganographically written. At this time, the Secret image appears to be noisy. The classified image is embedded into the Host image through the SegNet deep network model. In the process of embedding and extracting, it is not necessary to modify the Host image, and the visual quality of the Host image is not seriously affected, and the anti-detection property is also improved. In addition, steganography capacity is guaranteed. Since the Deep Neural Network model is used, it is only necessary to adjust the corresponding parameters in the embedding and extraction process. Without the need to manually design algorithms, the methods used are more flexible and flexible.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable suggestions.

REFERENCES

[1] A. Z. Tirkel, G. A. Rankin, R. G. Schyndel, W. J. Ho, N. Mee, and C. F. Osborne, "Electronic watermark," in *Digital Image Computing, Technology and Applications*. Sydney, NSW, Australia: Australian Pattern Recognition Society, 1993, pp. 666–673.

[2] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[3] T. Pevny, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*. Berlin, Germany: Springer, 2010, pp. 161–177.

[4] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2012, pp. 234–239, doi: 10.1109/wifs.2012.6412655.

[5] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997, doi: 10.1109/83.650120.

[6] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Trans. Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008, doi: 10.1109/tmm.2008.922795.

[7] J. Ruanaidh, W. Dowling, and F. Boland, "Phase watermarking of digital images," in *Proc. 3rd IEEE Int. Conf. Image Process.*, Dec. 2002, pp. 239–242, doi: 10.1109/icip.1996.560428.

[8] C. Qin, C.-C. Chang, and K.-N. Chen, "Adaptive self-recovery for tampered images based on VQ indexing and inpainting," *Signal Process.*, vol. 93, no. 4, pp. 933–946, Apr. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0165168412004082, doi: 10.1016/j.sigpro.2012.11.013.

[9] Y. C. Hu, W. L. Chen, and C. C. Lo, "A novel tamper detection scheme for BTC-compressed images," *Opto-Electron. Rev.*, vol. 21, no. 1, pp. 137–146, 2013, doi: 10.2478/s11772-013-0078-6.

[10] Y.-C. Hu, C.-C. Lo, W.-L. Chen, and C.-H. Wen, "Joint image coding and image authentication based on absolute moment block truncation coding," *J. Electron. Imag.*, vol. 22, no. 1, Jan. 2013, Art. no. 013012, doi: 10.1117/1.jei.22.1.013012.

[11] S. Nguyen, C.-C. Chang, and T.-F. Chung, "A tamper-detection scheme for BTC-compressed images with high-quality images," *KSII Trans. Internet Inf. Syst.* vol. 8, no. 6, pp. 2005–2021, 2014, doi: 10.3837/tiis.2014.06.011.

[12] A. Sahu and G. Swain, "Dual stego-imaging based reversible data hiding using improved LSB matching," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 5, pp. 63–73, Sep. 2019, doi: 10.22266/ijies2019.1031.07.

[13] A. K. Sahu and G. Swain, "Pixel overlapping image steganography using PVD and modulus function," *3D Res.*, vol. 9, p. 40, Sep. 2018, doi: 10.1007/s13319-018-0188-5.

[14] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," 2014. *arXiv:1406.2661*. [Online]. Available: https://arxiv.org/abs/1406.2661

[15] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998, doi: 10.1109/5.726791.

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

[17] J. Zeng, S. Tan, B. Li, and J. Huang, "Large-scale JPEG image steganalysis using hybrid deep-learning framework," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1200–1214, May 2018, doi: 10.1109/tifs.2017.2779446.

[18] D. Hu, Q. Shen, S. Zhou, X. Liu, Y. Fan, and L. Wang, "Adaptive steganalysis based on selection region and combined convolutional neural networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, 2017, doi: 10.1155/2017/2314860.

[19] G. Xu, H.-Z. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, May 2016, doi: 10.1109/lsp.2016.2548421.

[20] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, pp. 38303–38314, 2018, doi: 10.1109/access.2018.2852771.

[21] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Comput. Sci.*, vol. 54, pp. 472–481, 2015, doi: 10.1016/j.procs.2015.06.054.

[22] A. Kumar, S. S. Tyagi, M. Rana, N. Aggarwal, and P. Bhadana, "A comparative study of public key cryptosystem based on ECC and RSA," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 5, pp. 1904–1909, 2011.

[23] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, Oct. 2011, doi: 10.15373/2249555x/mar2014/91.

[24] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, p. 1482, Jun. 2017, doi: 10.3390/s17071482.

[25] F.-H. Hsiao, "Applying elliptic curve cryptography to a chaotic synchronisation system: Neural-network-based approach," *Int. J. Syst. Sci.*, vol. 48, no. 14, pp. 3044–3059, Oct. 2017, doi: 10.1080/00207721.2017.1364446.

[26] L. Tawalbeh, M. Mowafi, and W. Aljoby, "Use of elliptic curve cryptography for multimedia encryption," *IET Inf. Secur.*, vol. 7, no. 2, pp. 67–74, Jun. 2013.

[27] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018, doi: 10.1109/access.2018.2879844.

[28] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/access.2019.2906052.

[29] S. Baluja, "Hiding images in plain sight: Deep steganography," in *Advances in Neural Information Processing Systems*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates, Inc., 2017, pp. 2069–2079.

[30] A. Rehman, R. Rahim, M. Nadeem, and S. ul Hussain, "End-to-end trained CNN encode-decoder networks for image steganography," 2017, *arXiv:1711.07201*. [Online]. Available: https://dblp.org/rec/bib/journals/corr/abs-1711-07201

[31] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8559–8575, Apr. 2019.

[32] H. A. Atee, R. Ahmad, N. M. Noor, A. M. S. Rahma, and Y. Aljeroudi, "Extreme learning machine based optimal embedding location finder for image steganography," *PLoS ONE*, vol. 12, no. 2, Feb. 2017, Art. no. e0170329, doi: 10.1371/journal.pone.0170329.

[33] S. G. J. X. Meng and R. Rice, "A fusion steganographic algorithm based on faster R-CNN," *Comput., Mater. Continua*, vol. 55, no. 1, pp. 1–16, 2018, doi: 10.3970/cmc.2018.055.001.

[34] V. Badrinarayanan, A. Kendall, and R. Cipolla, "SegNet: A deep convolutional encoder-decoder architecture for image segmentation," 2015, *arXiv:1511.00561*. [Online]. Available: https://arxiv.org/abs/1511.00561

[35] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019, doi: 10.1109/access.2019.2891247.

[36] J. Laaksonen, M. Koskela, S. Laakso, and E. Oja, "PicSOM–content-based image retrieval with self-organizing maps," *Pattern Recognit. Lett.*, vol. 21, nos. 13–14, pp. 1199–1207, 2000.

[37] Z.-L. Zhou, Y. Cao, and X.-M. Sun, "Coverless information hiding based on bag-of-words model of image," *J. Appl. Sci.*, vol. 34, pp. 527–536, Sep. 2016, doi: 10.3969/j.issn.0255-8297.2016.05.005.

[38] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Cloud Computing and Security*, Z. Huang, X. Sun, J. Luo, and J. Wang, Eds. Cham, Switzerland: Springer, 2015, pp. 123–132.

[39] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *Intelligent Computing Methodologies*, D.-S. Huang, A. Hussain, K. Han, and M. M. Gromiha, Eds. Cham, Switzerland: Springer, 2017, pp. 536–547.

[40] J. Xu, X. Mao, X. Jin, A. Jaffer, S. Lu, L. Li, and M. Toyoura, "Hidden message in a deformation-based texture," *Vis. Comput.*, vol. 31, no. 12, pp. 1653–1669, Dec. 2015, doi: 10.1007/s00371-014-1045-z.

[41] K.-C. Wu and C.-M. Wang, "Steganography using reversible texture synthesis," *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 130–139, Jan. 2015, doi: 10.1109/TIP.2014.2371246.

[42] B. Boehm, "StegExpose—A tool for detecting LSB steganography," 2014, *arXiv:1410.6656*. [Online]. Available: https://arxiv.org/abs/1410.6656

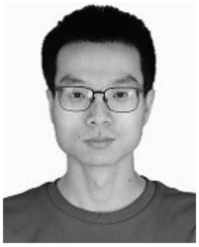
[43] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003, doi: 10.1109/TSP.2003.812753.

[44] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Workshop Multimedia Security New Challenges-MM&Sec*, 2001, pp. 27–30, doi: 10.1145/1232454.1232466.

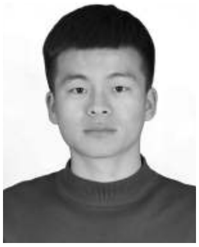
[45] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, A. Pfitzmann, Ed. Berlin, Germany: Springer, 2000, pp. 61–76.

[46] S. Dumitrescu, X. Wu, and N. Memon, "On steganalysis of random LSB embedding in continuous-tone images," in *Proc. Int. Conf. Image Process.*, vol. 3, Jun. 2003, pp. 641–644, doi: 10.1109/icip.2002.1039052.

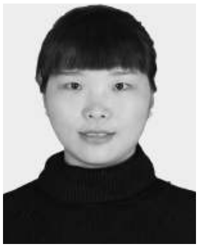
XINTAO DUAN received the master's degree in computer application technology from Shanghai Normal University, in 2004, and the Ph.D. degree in communication and information systems from Shanghai University, in September 2011. He has been teaching and researching with Henan Normal University, since July 2004. His research interests include image encryption, information hiding, image forensics, and deep learning.



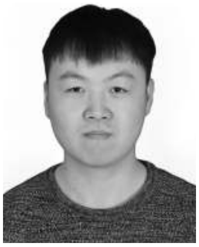
DAIDOU GUO received the B.S. degree from the Henan Institute of Science and Technology, China, in 2016. He is currently pursuing the M.S. degree with the College of Computer and Information Engineering, Henan Normal University. His research interests include image processing, deep learning, and image steganography.



NAO LIU received the B.S. degree from Henan Agricultural University, China, in 2018. He is currently pursuing the M.S. degree with the College of Computer and Information Engineering, Henan Normal University. His research interests include image processing, deep learning, and image steganography.



BAOXIA LI received the B.S. degree from Henan Normal University, China, in 2017, where she is currently pursuing the M.S. degree with the College of Computer and Information Engineering. Her research interests include image processing, deep learning, and image steganography.



MENGXIAO GOU received the B.S. degree from Henan Normal University, China, in 2018, where he is currently pursuing the M.S. degree with the College of Computer and Information Engineering. His research interests include image processing, deep learning, and image steganography.

CHUAN QIN received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from the Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the Faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Professor. He was with Feng Chia University, Taiwan, as a Postdoctoral Researcher, from 2010 to 2012. His research interests include image processing and multimedia security. He has published more than 110 articles in these research areas.