A Larger Capacity Data Hiding Scheme Based on DNN

Lianshan Liu, Lingzhuang Meng, Weimin Zheng, Yanjun Peng, and Xiaoli Wang

1College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China
2Office of Network Security and Informatization, Shandong University of Science and Technology, Qingdao 266590, China

Correspondence should be addressed to Weimin Zheng; zhengweimin@sdust.edu.cn

Received 21 November 2021; Revised 29 January 2022; Accepted 1 March 2022; Published 16 March 2022

Academic Editor: Iftikhar Ahmad

Copyright © 2022 Lianshan Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the in-depth research in data hiding technology, the latest data hiding schemes using deep neural network (DNN) could hide the full-size color image into the same size color image. This paper proposed a larger capacity data hiding scheme based on DNN, which could hide large-size color image into small-size color image. This scheme used DNN in both the data hiding stage and data extraction stage. And the two networks were obtained through adversarial training and used in pairs. The information ratio between the carrier image and the secret image had reached 1:4. The image obtained after hiding the data did not change much compared with the carrier image, and the extracted image had the same size and no visual difference compared with the secret image. It could be seen from the simulation experiment that, compared with the existing DNN-based data hiding scheme, even if the capacity of the proposed scheme was 4 times larger than that of the existing scheme, the visual effect and PSNR were also better than some existing schemes.

1. Introduction

With the advent of the information age, privacy and communication security had become a topic of concern. Data hiding technology could hide secret data or images in a carrier image that could be disclosed and transmit the secret information through the carrier image. Therefore, data hiding technology was widely used in special fields such as secret information transmission and intellectual property protection [1].

The earliest data hiding technology used the spatial domain method. The spatial domain scheme used the correlation between pixels to hide, and the data was directly placed in the pixels of the carrier image. This scheme included least important bit (LSB) [2] and pixel value difference [3]. Then, the transform domain scheme appeared. The transform domain scheme was to transform the image through a series of transformations to obtain transform coefficients and hide the data in the transform coefficients. The main transforms used include wavelet transform [4], discrete cosine transform [5, 6], and Fourier transform [7].

The traditional data hiding scheme had a small hiding capacity, which could hide binary images or grayscale images into grayscale images [8] or color images [9, 10]. And as the hiding capacity increased, the visual effect of the hidden image decreased significantly. Guo et al. [11] analyzed the capacity and imperceptibility of traditional imperceptible watermarks. And a quantitative relationship between the capacity and peak signal-to-noise ratio of traditional data hiding schemes was proposed. They believed that the traditional information hiding and watermarking techniques could not embed information larger than the carrier image.

Based on deep neural networks (DNN), Baluja [12] proposed a scheme for plain sight data hiding in 2017, deep steganography, which could hide the full-size color image into the same size color image. And he further optimized the scheme; the latest research [13] could hide two full-size color images into color image of the same size. Rehman et al. [14] and Hussain and Zeng [15] proposed an end-to-end trained CNN model for steganography. The proposed scheme achieved a higher hiding capacity under the premise of higher PSNR and SSIM. The scheme proposed by
Subramanian et al. [16] concatenated the features extracted from the carrier and the secret image, instead of concatenating the original images. This reduced the amount of redundant data.

Liu et al. [17] and Wang et al. [18] proposed data hiding scheme using GAN. Since GAN network performed well in image generation and other fields, the hidden image generated by GAN network could also have higher visual effect. Li et al. [19] proposed a spatial steganography scheme based on GAN network. Multiple cross-feedback channels were established between the shrinking and expanding paths of the generator, through which downsampled information could be sent directly to the expansion layer. This scheme effectively improved feature utilization and could learn deep complex features. Li et al. [20] proposed a steganography scheme by combining GAN networks and chaotic systems. The scheme could hide the encrypted secret image into the carrier image, and the extracted encrypted image could still be decrypted to obtain secret data. Such a scheme had higher security and could avoid the leakage of secret images.

Data hiding techniques using deep learning had higher capacity than traditional schemes. Duan et al. [21] proposed the StegoCNN model, which could hide two color images into a carrier image of the same size. Among them, the hiding network was to directly connect and fuse the two secret images with the carrier image, and the extraction network was designed with two convolutional networks to extract the two secret images, respectively. In addition, using deep learning for data hiding could not only increase the capacity of the scheme but also improve the robustness. The scheme proposed by Chen et al. [22] designed an attack network in the network to simulate attacks such as Gaussian noise and sharpening. The network trained in this way was robust to some common attacks. Ahmadi et al. [23] also added an attack layer to the network. More attacks including JPEG compression and cropping were selected for training, and only one attack per iteration was selected for training. The robustness of this scheme against various attacks was very high, which was greatly improved compared with the traditional scheme.

Ronneberger et al. [24] proposed a U-shaped neural network structure called U-Net in 2015. The scheme proposed the idea of using cross-layer connections to fully supplement the underlying features. U-Net had good effects in the fields of medical image segmentation and image generation. Duan et al. [25] and Liu et al. [26] used an improved U-Net network to implement data hiding technology. Due to the good complementary effect of cross-layer connections on features, the two solutions performed well in terms of visual effects and hiding capacity. He et al. [27] proposed residual network (ResNet) for image classification in 2016, in which the unique shortcut could ensure the full use of features. Duan et al. [28] and Mo et al. [29] used ResNet for data hiding and had high visual effects and hiding capacity too. However, there was not much breakthrough in the current hiding capacity.

Aiming at the extended research of data hiding scheme based on DNN, a data hiding scheme with larger capacity was proposed in this paper. The scheme was using deep neural networks (DNN) to realize data hiding and extraction and realized a hiding network (hiding the secret data into the carrier image to get the hidden image) and an extraction network (extracting the secret data from the hidden image). Inspired by the GAN network, this scheme used an adversarial training method. The hiding network and the extraction network influenced each other during training and tend to be optimal at the same time. It made the difference between the hidden image and the carrier image smaller, and the extracted image was closer to the secret image. This paper included the following main contributions: (1) a larger capacity data hiding scheme with a brand-new network structure was proposed. (2) A similar network structure was use to achieve hiding and extraction, so that the two networks converge to the local optimum at the same time. (3) A comparative analysis method was proposed for the deep data hiding scheme, the scatter plots of PSNR and SSIM, which were convenient for comparative analysis of larger datasets.

2. Related Works

2.1. ResNet. In 2015, He et al. [23] proposed a residual network (ResNet) to solve the degradation problem caused by the increasing number of convolutional layers of neural networks at that time. ResNet connected the upper layer features to the lower layer, effectively supplemented the underlying features, and reduced feature loss. The concept of residual block was introduced in ResNet. The structure of the residual block was shown in Figure 1.

The connection method of the cross-layer connection in the residual block was called shortcut, which was represented as “⊕” in the figure. Shortcut was a pixel-level connection, which could be understood as the addition of \( F(x) \) and \( x \) for each pixel. Therefore, \( F(x) \) and \( x \) were required to have the same size and number of feature layers. If the features of the two layers were different, a convolution operation was required for dimensionality reduction. Figure 2 shown partial structure of a 34-layer ResNet network proposed by Ahmadi et al. [23].

Because multiple residual block connections were used in ResNet, image features could be reused. Feature reuse ensured the integrity of basic features. Therefore, the use of residual block connection mode could prevent feature loss to a large extent, which was easier to optimize than simple network layer stacking, and could achieve good results.

2.2. U-Net. In 2015, Ronneberger et al. [20] proposed a U-shaped network structure called U-Net, which could also solve the problem of gradient explosion and gradient disappearance. The network structure of U-Net was shown in Figure 3. Four times of downsampling and four times of upsampling were used in U-Net, and the features on the same level were connected after copy and crop. The connection mode in U-Net was series connection, and the number of feature layers after the connection was the sum of the number of layers of the two features.

In the original U-Net network, the output result was not consistent with the input image size. At the same time, since there was a small difference in the size of the two connected
features, cropping was required, so there would be some feature loss.

In U-Net, the initial features were copied and connected to the underlying network and supplemented the basic semantic features. This connection method made full use of image features and made the generated image details more accurate. Therefore, in image segmentation or other fields, the results obtained using U-Net had greater advantages in contour details and had better visual effects.

3. Proposed Method

At present, most DNN-based data hiding schemes could realize high-capacity color image data hiding. This paper proposed a data hiding scheme with larger capacity based on DNN, which could hide large-size color secret images into small-size color carrier images. In this scheme, a fully convolutional main network was proposed as the main structure of the hiding network and the extraction network. Compared with Baluja’s network, the proposed scheme introduced a more reasonable structure, such as shortcut and concatenation connection methods, which had higher theoretical support. The update of this network structure greatly improved the feature reuse utilization rate, and the resulting image was clearer and more complete.

According to the universal approximation theorem of neural network, in theory, neural network could approximate any function, as long as the network could learn the objective function. Therefore, using the hiding network to hide the data, the generated hidden image could infinitely approximate the pixel distribution of the carrier image. Similarly, the image extracted by the extraction network could infinitely approximate the pixel distribution of the secret image.

3.1. Main Network. In this scheme, a fully convolutional main network was proposed, which was used in both the hiding stage and the extraction stage. Therefore, the proposed hiding network and the extraction network were only different in the structure of the input and output parts. The proposed network structure was shown in Figure 4, and the network parameters were shown in Table 1.

According to Figure 4 and Table 1, the structure of the main structure (layer 1 to layer 8) of the hiding network and the extraction network was the same, while the structures and parameters of layers 0, 8, and 9 were different. The hiding network performed a convolution operation on the secret image in layer 0. The output part of the extraction network had one more deconvolution operation than the hiding network, and then, the extracted secret image was obtained. In this way, the size of the secret data and the carrier image could be balanced, so that larger-size images could be hidden into the carrier image and could be completely extracted.

In the scheme, except for layer 1 of the extraction network and the last layer of hiding and extraction network, the rest of the layers all used batch normalization (BN) acceleration. All convolutional layers used ReLU activation, and all deconvolutions used LeakyReLU activation (except for the deconvolution of layer 9 of the extraction network, which used Sigmoid activation).

The main network used two connection methods: pixel-level connection liked ResNet and cross-layer concatenation liked U-Net. The specific structure and parameters of ResBlock were shown in Figure 5. In ResBlock, because the input size and output size were different, a convolution operation was used to reduce the size, as shown in the upper right convolution operation of Figure 5. These two features were connected by shortcuts, that is, the corresponding
positions of all elements were added together. The size and dimensions of the two connected features were completely the same, so no cropping operation was required. The use of ResBlock improved the utilization of features, retained image features to the greatest extent, and prevented problems such as feature loss and gradient explosion.

In the hiding process, the complex and unimportant image features of the secret image were removed, and the important image features were preserved and integrated into the carrier image. The extraction process was to extract and restore the secret image based on the features of the secret data contained in the hidden image.
Table 1: The specific parameters of the proposed scheme include the data hidden network and the data extraction network.

| Layer | Output size of hiding | Output size of extraction | Type            |
|-------|-----------------------|---------------------------|-----------------|
| 0     | 6 × 256 × 256         | —                         | Convolution (1 × 1) |
| 1     | 32 × 128 × 128        | 32 × 128 × 128            | Convolution (3 × 1) |
| 2     | 64 × 64 × 64          | 64 × 64 × 64              | ResBlock        |
| 3     | 128 × 32 × 32         | 128 × 32 × 32             | ResBlock        |
| 4     | 256 × 16 × 16         | 256 × 16 × 16             | ResBlock        |
| 5     | 128 × 32 × 32         | 128 × 32 × 32             | Deconvolution   |
| 6     | 64 × 64 × 64          | 64 × 64 × 64              | Deconvolution   |
| 7     | 32 × 128 × 128        | 32 × 128 × 128            | Deconvolution   |
| 8     | 3 × 256 × 56          | 32 × 256 × 256            | Deconvolution   |
| 9     | —                     | 3 × 512 × 512             | Deconvolution   |

The training process adopted the method of adversarial training, and the two networks played games with each other. The goal of the hiding network was to get the least modified hidden image, and the goal of the extraction network was to get the extracted image closest to the secret image. This kind of adversarial training method made the features integrated into the carrier image become less, and the extracted image was closer to the secret image, and gradually approached the Nash equilibrium.

3.2. Loss Function. The loss function of the proposed scheme used mean square error (MSE), and the loss of the scheme was calculated by the average of loss1 in the hiding stage and loss2 in the extraction stage. The calculation formula of MSE was as follows.

$$\text{MSE}(I, I') = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_{ij} - I'_{ij})^2.$$  (1)

Among them, I and I’ represented two images, respectively, and M and N were the length and width of the images I and I’. Therefore, the loss1 in the data hiding stage could be calculated using the carrier image Ia and the hidden image Ib.

$$\text{loss1} = \text{MSE}(Ia, Ib).$$  (2)

Similarly, the loss2 in the data extraction stage can be calculated using the secret image Is and the extracted image Is’.

$$\text{loss2} = \text{MSE}(Is, Is').$$  (3)

The calculation method of the loss of the scheme was as follows.

$$\text{Loss} = \frac{\text{loss1} + \text{loss2}}{2}. $$  (4)

3.3. Adversarial Training. Inspired by the GAN network, the adversarial training method was used for training in the scheme of this paper. In the GAN network, the pictures obtained by the generator were sent to the discriminator for recognition. With training, the generator would generate better quality images, and the discriminator could not tell the difference between the generated image and the real image, at which point the network was well-fitted.

The proposed scheme also had two networks: the hiding network and the extraction network, and the two networks need to exist in pairs. So, during training, we feed the results of the hiding network into the extraction network. And calculated the loss based on the hidden and extracted results, as shown in Figure 6. In this way, the two networks formed a closed loop. In order to generate hidden images that were closer to the carrier image, the hiding network would include fewer secret image features or fuse them to be less obvious. At the same time, in order to extract clearer and more complete images, the extraction network would require hidden images to contain more features. Through training, the hidden image was closer to the carrier image, and the extracted image was closer to the secret image.

In order to train the two networks with similar gradients, the loss functions of the two networks used the same MSE loss function. This scheme used the main network as the main structure of the two networks, which were of similar order of magnitude. Both networks would converge to the local optimum at the same time during training, and there would be no overfitting of one of the networks.

3.4. The Process of Pixel Overflow. In the hiding network, layer 8 used the activation function LeakyReLU, and the value range of the activation function may appear to be less than 0 or greater than 1. When this happened, the resulting image pixel value would be less than 0 or greater than 255, which was an error in natural images, called pixel value underflow or overflow. In the proposed scheme, a forced conversion method was used to correct the pixel overflow problem. That is, when the pixel value of the hidden image was less than 0, it was forcibly converted to 0, and when the pixel was greater than 255, it was forcibly converted to 255. Such forced conversion was a correction of the image,
which could avoid data loss in the process of saving the image.

4. Experimental Analysis and Comparison

In this paper, the test set and training set used by the network were from the VOC 2012 [30] and ImageNet [31] dataset. There were 40,000 images for training and 6,000 images for testing. The secret image was randomly selected, regardless of training or testing. The carrier image was processed to a size of $256 \times 256$, and the secret image was processed to a size of $512 \times 512$. The initial network learning rate of the experiment was $lr = 0.001$, and the number of training rounds was $epoch = 500$.

This paper compared and analyzed the proposed schemes from the aspects of hiding capacity, image quality, residual image, and so on. The example images in the dataset used in this paper are shown in Figure 7, where the upper line was the carrier image, and the lower line was the secret image.

4.1. Image and Histogram. The histogram of the image could intuitively display the pixel distribution of the image. According to the histogram of the two images, the similarity and difference of the pixel distribution between the two
images could be seen. If there was no visual difference between the two images, the difference in the histogram would also be small. The result image obtained on the test set of the proposed scheme and the corresponding histogram of each image were shown in Figure 8.

According to the result images in Figure 8, there is almost no difference between the hidden image and the carrier image, even if an image four times larger than itself was hidden. Moreover, the extracted image had the same size as the secret image, and the two images looked almost identical. According to the histogram in Figure 8, it could be seen that hiding the secret image had little effect on the pixel distribution of the carrier image, and only some of the positions were slightly different. The pixel distribution of the extracted image was basically the same as the secret image, and the pixel restoration effect was very good.

4.2. Residual Image. The residual image was the difference image between two images, which could more intuitively show the difference between the two images. Since the data hiding scheme using deep learning did not scramble or encrypt the image, there was a mapping relationship between the hidden position and the image pixel distribution. If the network setting was improper, it was possible to observe the contour or afterimage of the secret image in the residual image. Figure 9 has shown the experimental result images of the proposed scheme on the test set, the residual images between the carrier image and the hidden image, and the 20-fold residual images. For better display, the secret image was displayed in the same size as the carrier image.

It can be seen from the third column of Figure 9 that the residual image of the proposed scheme had no visual meaning. Therefore, the pixels of the hidden image and the carrier image had very small differences, even if a large secret image was hidden. The outline of some carrier images could be seen from the 20 times residual image, but no outline of the secret image could be seen. Even if someone had the original image, he could not get any information about the secret image from the residual image. At the same time, combined with the histogram, the proposed scheme had certain resistance to the chosen plaintext attack.

4.3. Hiding Capacity Analysis. In order to prove the breakthrough of the proposed solution in data hiding capacity, this paper used effective capacity (EC) to represent the data hiding ability, and its unit was bits per pixel (bpp). The
method of calculating EC was as follows.

\[
EC = \frac{NS}{NC}.
\]  

Among them, NS represented the size (bits) of the secret image hidden into the image; NC represented the number of pixels of the carrier image (the color image had 3 channels). Table 2 has shown the comparison of the effective capacity between the proposed scheme and the traditional or DNN-based scheme.

In Table 2, compared with the traditional data hiding scheme, the DNN-based scheme had a huge improvement in capacity. But in fact, the comparison with the traditional scheme was not reasonable, because the hiding scheme did not require the lossless extraction of secret information. However, compared with the scheme that also did not require perfect reconstruction, the EC of the proposed
The method of calculating the SSIM between the images was as follows. When two images were exactly the same, the value of SSIM was 1.

The second was the structural similarity index (SSIM). SSIM measured the difference between two images in terms of brightness, contrast, and structure. Usually, when two images were exactly the same, the value of SSIM was 1. The method of calculating the SSIM between the images \( I \) and \( I_a \) was as follows.

\[
SSIM(I, I_a) = \frac{2\mu_I\mu_{I_a} + c_1}{\mu_I^2 + \mu_{I_a}^2 + c_1} \frac{2\sigma_{I_a} + c_2}{\sigma_{I_a}^2 + \sigma_{I_a}^2 + c_2},
\]

where \( \mu_I \) and \( \mu_{I_a} \) were the average values of \( I \) and \( I_a \), respectively, \( \sigma_I \) and \( \sigma_{I_a} \) were the variances of \( I \) and \( I_a \), respectively, and \( \sigma_{I_a}^2 \) and \( \sigma_{I_a}^2 \) were the variances of \( I \) and \( I_a \), respectively. \( c_1 \) and \( c_2 \) were the variables to avoid zero denominator.

Table 3 has shown the comparison between the proposed scheme and the latest DNN-based data hiding scheme in terms of PSNR and SSIM.

| Schemes                  | Hidden image | Extracted image |
|--------------------------|--------------|-----------------|
| Baluja [13]              | PSNR (Max\(^1\)) 36.7 | 35.75 |
| EC = 16                  | SSIM (Max) 0.96 | 0.955 |
| Rehman et al. [14]       | PSNR (Ave\(^1\)) 32.5 | 34.7571 |
| EC = 2.67                | SSIM (Ave) 0.9371 | 0.93 |
| Li et al. [20]           | PSNR (Ave) 42.3 | 38.45 |
| EC = 8                   | SSIM (Ave) 0.987 | 0.953 |
| Chen et al. [22]         | PSNR (Max) 37.35 | 31.38 |
| EC = 2.67                | SSIM (Max)  | — |
| Duan et al. [28]         | PSNR (Max) 42.6631 | 42.8779 |
| EC = 8                   | SSIM (Max) 0.9861 | 0.9850 |
| Proposed                | PSNR (Ave) 43.8073 | 37.2380 |
| EC = 32                  | SSIM (Ave) 0.9852 | 0.9437 |

\(^1\)Max was the maximum value (the average value not given) listed in the scheme. \(^2\)Ave was the average value given in the scheme.

The PSNR reached 32 bpp, which was 4 times higher than that of Li et al. [20] and Duan et al. [25] and 2 times higher than that of Baluja [13]. Therefore, it could be seen that this scheme had a higher capacity than the existing solution.

### 4.4. Comparison of PSNR and SSIM

In order to measure the effect of hidden image and the quality of the extracted image in the proposed scheme. This article compares with existing schemes in two aspects, the first was the peak signal-to-noise ratio (PSNR). PSNR measured the pixel difference between two images. If the difference between the images was small, the PSNR should be greater. The method of calculating the PSNR between the images \( I \) and \( I_a \) was as follows.

\[
PSNR = 10 \times \log_{10} \left( \frac{2^2 - 1}{\text{MSE}(I, I_a)} \right),
\]

The second was the structural similarity index (SSIM). SSIM measured the difference between two images in terms of brightness, contrast, and structure. Usually, when two images were exactly the same, the value of SSIM was 1. The method of calculating the SSIM between the images \( I \) and \( I_a \) was as follows.

The scatter plot of PSNR and SSIM. Because the deep neural network was used in data hiding scheme, the scale of test data was greatly increased, and the traditional scheme of comparing effects using the same image loses its advantage. This paper proposed a comparative analysis method for deep learning data hiding: the scatter plots of PSNR and SSIM. The abscissa of the scatter plot of PSNR and SSIM was the PSNR or SSIM of the hiding scheme, and the ordinate was the PSNR or SSIM of the extraction scheme. The scatter plot could be used to plot the distribution of all data on the test set to facilitate the analysis of the average value, maximum and minimum values, and other conditions. Figure 10 has shown the scatter plots of PSNR and SSIM of the proposed scheme.

In Figure 10(a), the PSNR scatter plot of the proposed scheme was mostly distributed in the upper right of Chen et al. [22], which showed that the proposed scheme was completely superior to Chen et al. [22] on the entire test set. According to Figures 10(a) and 10(b), it could be seen that the average value of the proposed scheme was lower than the maximum PSNR and SSIM of Duan et al. [28], but the maximum value hidden and extracted by this scheme was higher than that the maximum value of Duan et al. [28]. Therefore, even if the scheme realized the hiding of more secret data, it still had certain advantages in the effect of hidden image and the quality of the extracted image.

In addition, according to Figure 10, it could be seen that there were some points with extremely low PSNR or SSIM values on the left and below. The images corresponding to these scattered points were studied, and further experiments were shown in Figure 11.

According to Figures 11(a) and 11(b), it could be seen that smoother images could achieve better results, even if it was hidden in a completely white image (but it was meaningless). On the contrary, according to Figures 11(b) and 11(c), it could be seen that the visual changes of the hidden image obtained by hiding data in the disturbed image were very large. This was because the dataset used for training was a relatively smooth natural image. In addition, according to the research of the human visual system, the human eye was not easy to perceive the data hidden in the smooth image. Therefore, the effect of hiding in a smooth image...
would be better, and the effect of hiding in an image with complex contours or no natural image rules would be poor.

At the same time, the proposed scatter plots of PSNR and SSIM could clearly show the pros and cons of the proposed scheme on the entire test set, and it was convenient to analyze the maximum, minimum, average, and test set distribution of the PSNR and SSIM of the scheme.

4.6. Robustness Analysis. In order to test the robustness of the scheme, an attack experiment was carried out in this part. Attack experiments simulated common nongeometric attacks such as clipping, filtering, and noise. After the secret data was hidden in the carrier image, the hidden image was attacked, and the attacked image was used to extract the image. The resulting images of the attack experiment and the PSNR and SSIM between the extracted image and the original secret image were shown in Figure 12.

It can be seen from Figure 12 that the proposed scheme was robust to cropping, patterned elimination, and salt-and-pepper noise. The extracted image was close to the original secret image and had little effect on the recognizability of the human eye. However, the robustness to Gaussian filtering was not good, and the extracted image was relatively blurry. Since the scheme could hide the large-sized secret image into the small-sized image, the secret data contained in each pixel of the carrier image and its pixel correlation. Therefore, the proposed scheme was robust to attacks with small area pixel changes or attacks that do not change the correlation of image pixels. However, it was less robust to

![Figure 10: The scatter plot of PSNR and SSIM. (a) The scatter plot of PSNR. (b) The scatter plot of SSIM.](image)

![Figure 11: Experimental results of different smoothness images (the size of the last three columns of images is zoom out for better display).](image)
attacks that with large-area pixel variations such as compression, filtering, and rotation.

5. Conclusions

This paper proposed the larger capacity data hiding scheme based on DNN, which realized the hiding of larger-size secret images into smaller-size carrier images. This scheme used DNN to realize the hiding network and the extraction network, and the structure of the two networks was basically the same. The two networks were used in pairs and tend to be optimal in adversarial training. The proposed scatter plots of PSNR and SSIM could more completely display the experimental data on the test set and clearly reflect the advantages and disadvantages of the scheme. It can be seen from the simulation experiment that the obtained hidden image was almost indistinguishable from the original carrier image, and the extracted image was complete and clear. Compared with existing data hiding schemes, even if more data was hidden, this scheme still had certain advantages in terms of PSNR and SSIM.

The limitation of this paper was that the robustness performance was insufficient. In particular, the robustness was poor when dealing with geometric attacks and other attacks that will change the image pixels or pixel correlations in a large area. Future work will focus on the robustness of the scheme and improve the robustness of the scheme under the premise of high capacity.

Data Availability

Data can be obtained by contacting Lianshan Liu, email: lshliu6042@163.com.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgments

This project was funded by the National Key Research and Development Program of China (no. 11974373), Key Project of National Natural Science Foundation of China (no. 61932005), National Natural Science Foundation of China (no. 61976126), and Shandong Natural Science Foundation (no. ZR2019MF003).

References

[1] K. D. Ma, W. M. Zhang, X. F. Zhao, N. H. Yu, and F. H. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, pp. 553–562, 2013.
[2] S. Solak, “High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms,” IEEE Access, vol. 8, pp. 166513–166524, 2020.
[3] A. M. Alhomoud, “Image steganography in spatial domain: current status, techniques, and trends,” Intelligent Automation and Soft Computing, vol. 27, no. 1, pp. 69–88, 2021.
[4] L. Meng, L. Liu, G. Tian, and X. Wang, “An adaptive reversible watermarking in IWT domain,” *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 711–735, 2021.

[5] T. Rabie and I. Kamel, “High-capacity steganography: a global-adaptive-region discrete cosine transform approach,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6473–6493, 2017.

[6] M. M. Abdel-Aziz, K. M. Hosny, and N. A. Lashin, “Improved data hiding method for securing color images,” *Multimedia Tools and Applications*, vol. 80, no. 8, pp. 12641–12670, 2021.

[7] L. Ghouti, “Estimation of data hiding capacities in spatio-chromatic Fourier transform (SCFT) representations of color images,” *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3699–3718, 2019.

[8] K. H. Jung, “High-capacity reversible data hiding method using block expansion in digital images,” *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 159–170, 2018.

[9] Y. Yalman and F. Akar, “A high-capacity reversible data hiding method: HCRHide,” *Imaging Science Journal*, vol. 62, no. 2, pp. 121–126, 2014.

[10] L. Ghouti, “A perceptually-adaptive high-capacity color image watermarking system,” *Ksii Transactions on Internet and Information Systems*, vol. 11, no. 1, pp. 570–595, 2016.

[11] H. Guo, J. T. Xue, and Z. G. Jin, “The analysis of watermarking capacity of packing model and bits replacement model,” in *Proceedings of the 2016 12th World Congress on Intelligent Control and Automation*, Guilin, China, 2016.

[12] S. Baluja, “Hiding images in plain sight: deep steganography,” *Advances in Neural Information Processing Systems*, vol. 30, pp. 2066–2076, 2017.

[13] S. Baluja, “Hiding images within images,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 7, pp. 1685–1697, 2020.

[14] A. Rehman, R. Rahim, S. Nadeem, and S. U. Hussain, “End-to-end trained CNN encoder-decoder networks for image steganography,” in *Computer Vision-Eccv 2019 Workshops, Pt Iv*, vol. 11132., L. Leal Taixe and S. Roth, Eds., pp. 723–729, Lecture Notes in Computer Science, 2019.

[15] I. Hussain and J. S. Zeng, “A survey on deep convolutional neural networks for image steganography and steganalysis,” *Ksii Transactions on Internet and Information Systems*, vol. 14, no. 3, pp. 1228–1248, 2020.

[16] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “End-to-end image steganography using deep convolutional autoencoders,” *IEEE Access*, vol. 9, pp. 135585–135593, 2021.

[17] J. Liu, Y. Ke, Z. Zhang et al., “Recent advances of image steganography with generative adversarial networks,” *IEEE Access*, vol. 8, pp. 60575–60597, 2020.

[18] Z. Wang, N. Gao, X. Wang, J. Xiang, D. Zha, and L. Li, “HidingGAN: high capacity information hiding with generative adversarial network,” in *Computer Graphics Forum*, pp. 393–401, Wiley Online Library, 2019.

[19] F. Li, Z. Yu, and C. Qin, “GAN-based spatial image steganography with cross feedback mechanism,” *Signal Processing*, vol. 190, p. 108341, 2022.

[20] Q. Li, X. Y. Wang, X. Y. Wang et al., “A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks,” *IEEE Access*, vol. 8, pp. 168166–168176, 2020.

[21] X. T. Duan, N. Liu, M. X. Gou, W. X. Wang, and C. Qin, “SteganCNN: image steganography with generalization ability based on convolutional neural network,” *Entropy*, vol. 22, no. 10, 2020.

[22] B. J. Chen, J. X. Wang, Y. Y. Chen, Z. L. Jin, H. J. Shim, and Y. Q. Shi, “High-capacity robust image steganography via adversarial network,” *Ksii Transactions on Internet and Information Systems*, vol. 14, no. 1, pp. 366–381, 2020.

[23] M. Ahmad, A. Norouzi, N. Karimi, S. Samavi, and A. Emami, “ReDMark: framework for residual diffusion watermarking based on deep networks,” *Expert Systems with Applications*, vol. 146, 2020.

[24] O. Ronneberger, P. Fischer, and T. Brox, “U-Net: convolutional networks for biomedical image segmentation,” in *International Conference on Medical Image Computing and Computer-Assisted Intervention*, Cham, 2015.

[25] X. T. Duan, K. Jia, B. X. Li, D. 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.

[26] L. Liu, L. Meng, Y. Peng, and X. Wang, “A data hiding scheme based on U-net and wavelet transform,” *Knowledge-Based Systems*, vol. 223, p. 107022, 2021.

[27] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778, 2016.

[28] X. Duan, B. Li, Z. Xie, D. Yue, and Y. Ma, “High-capacity information hiding based on residual network,” *IEEE Transactions on Image Processing*, vol. 38, no. 1, pp. 172–183, 2021.

[29] L. Q. Mo, L. Q. Zhu, J. Q. Ma, D. D. Wang, and H. Y. Wang, “MDRSteg: large-capacity image steganography based on multi-scale dilated ResNet and combined chi-square distance loss,” *Journal of Electronic Imaging*, vol. 30, no. 1, 2021.

[30] M. Everingham, L. VanGool, C. K. I. Williams, J. Winn, and A. Zisserman, *The PASCAL Visual Object Classes Challenge 2012 (VOC2012) Results*.

[31] O. Russakovsky, J. Deng, H. Su et al., “ImageNet large scale visual recognition challenge,” *International Journal of Computer Vision*, vol. 115, no. 3, pp. 211–252, 2015.