Single Exposure Phase-Only Optical Image Encryption and Hiding Method via Deep Learning

Qinnan Zhang and Jiaosheng Li

***Abstract*—Phase-only optical image security technology Based on one-time pad is an encryption and hiding method by introducing random key through phase modulation, which can improve the security of the system to a great extent. The application of traditional phase-only optical image encryption and hiding (POIEH) method is often limited by the amount of data and the quality of decrypted image. In this paper, a single exposure POIEH method using deep learning (DL) is proposed. The original image and corresponding encrypted hidden interferogram acquired with POIEH system are constructed to the train datasets for the learning of an end-to-end designed U-net, then the corresponding relationship between the encrypted hidden interferogram and the reconstructed image is learned and only single-frame encrypted hidden interferogram is needed to perform the reconstruction of POIEH. This method can realize real-time image encryption and hiding and high-quality decryption with only one interferogram. Simulation results and performance analysis show that the proposed method has higher security, stronger generalization ability and robustness.**

***Index Terms*—Deep learning, holographic interferometry, image processing, image security.**

I. Introduction

OPTICAL image security technology is implemented by using different optical information processing principles and technologies. It has been widely studied and applied because of its advantages of high efficiency and security. Since the double random phase encoding (DRPE) method was introduced in 1995 [1], many methods to improve security and simplify encryption system have been proposed [2]–[5]. Optical image hiding technology is another kind of encryption method by embedding the original information to be encrypted into the host image without destroying the form of the original host image. It can hide the information without attracting the attention of the attacker, so as to reduce the possibility of being attacked [6]. The hiding technology can tolerate different types of attacks, such as cutting, rotation, JPEG compression, etc., which is safe enough and not easy to be illegally accessed by unauthorized users. Among the existing image hiding methods, various systems have been proposed to realize image hiding, including classical DRPE system [7], Joint transform correlator (JTC) architecture [8], ghost imaging system [9], ptychography and digital holography system [10]. To further improve the security of the system and make full use of the advantages of optical parallel processing, many research works combining image encryption and hiding methods have been proposed [11]–[13]. The reported approach [11] first realize optical encryption, and then transform the encrypted image to digital data to complete image hiding through electronic means. The existing phase-shifting interferometry-based optical image encryption and hiding method [12] needs to make a complex optical mask to achieve the purpose of encryption, and once the optical encryption and decryption system is established, its key is difficult to replace, and some common attack methods will pose a great threat to it.

Optical image encryption and hiding technology based on phase-shifting interferometry has many advantages, such as simple algorithm, simple operation and high recording accuracy. Phase-only optical image encryption and hiding (POIEH) technology based on one-time pad is an image encryption method by introducing random key through phase modulation. It uses spatial light modulator (SLM) to improve the flexibility of encryption system, which can resist known plaintext attacks to a great extent, so as to improve the security of the system [13], [14]. However, it is difficult for such system to have both security and efficiency at the same time. The encrypted data is multiplied compared with the original data, which greatly affects the transmission efficiency and also limits its application in 3D image/video security. In addition, in the experiment, the quality of decrypted image is easily affected by nonlinear noise and phase shifts deviation. The quality of decrypted image is difficult to meet the practical application, especially for complex and detailed images, the decrypted image is even illegible. These problems directly affect the practical application in the field of information security.

In this work, Deep learning (DL) is a machine learning technology, in which a large amount of prior information is used for obtaining the optimal model approximation of the system (data-driven). It is an end-to-end learning method with the ability of automatic extraction of high-dimensional features. It can directly obtain the mapping relationship from the original input to the desired output. So far, it has been widely used to solve problems in the field of computational imaging [15], [16], including phase extraction [17], classification of cell morphology

Manuscript received December 15, 2021; revised January 19, 2022; accepted January 23, 2022. Date of publication January 27, 2022; date of current version February 8, 2022. This work was supported in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2021A1515110664, in part by the National Natural Science Foundation of China under Grant 61805086, and in part by the Start-Up Funding of Guangdong Polytechnic Normal University under Grant 2022SDKYA008. *(Corresponding author: Jiaosheng Li.)*

Qinnan Zhang is with the School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan 523808, China (e-mail: zhangqinnan520@126.com).

Jiaosheng Li is with the School of Photoelectric Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China (e-mail: 565159239@qq.com).

Digital Object Identifier 10.1109/JPHOT.2022.3146456

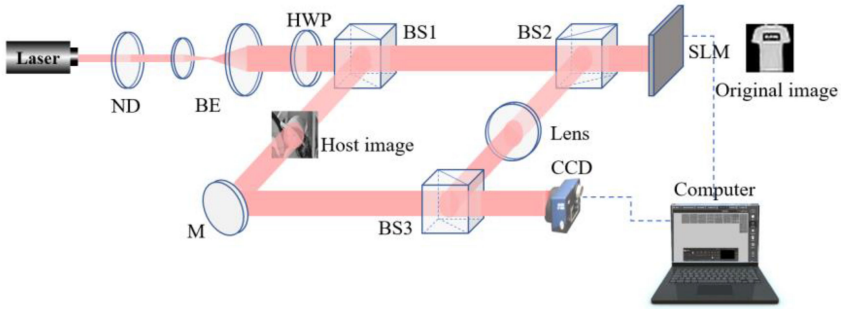

Fig. 1. The schematic of single exposure phase-only optical image encryption and hiding system. ND: Neutral density filter; BE: Beam expander; HWP: Half wave plate; BS1, BS2, BS3: Nonpolarized beam splitter; SLM: Spatial light modulator; M: Mirror; CCD: Charge coupled device.

[18], single-pixel imaging and other fields [19]. It also provides a new research idea for solving the problems in image security using deep network. For example, the DL-based methods can effectively attack the DRPE system [20], the interference-based optical encryption system [21], the asymmetric encryption system [22] and the JTC architecture [23]. Meanwhile, in 3D image hiding and 3D cryptosystem, deep revolutionary neural networks are used to resolve the problem of low resolution effectively [24], [25]. Various DL-based methods have been implemented to enhance image security and cryptanalysis, which are not limited to single image, but also include multiple images [26], [27]. The use of POIEH technology can afford high security and flexibility. Therefore, the application scope of the POIEH method can be further improved by solving the problems of data volume, reconstruction quality and efficiency using the DL method.

Based on this, an end-to-end designed U-net is used to analyze the single exposure POIEH system. The input of the network is the encrypted hidden interferogram, and the output of the network is the original reconstructed image. The proposed method can reduce the number of the recorded interferograms, which greatly reduces the amount of transmitted data and improves the encryption efficiency. In addition, despite the reduction of data, the proposed method still has high robustness. Especially in the processing of complex images, this method still gets good image reconstruction quality. The analysis of simulation results, security and robustness prove the feasibility and advantages of the method.

II. Principle and Network Analysis

A. Principle of Single Exposure Phase-Only Optical Image Encryption and Hiding Approach

Generally, the schematic of single exposure POIEH system is shown in Fig. 1. The 2D intensity image $O(x_0, y_0)$ to be encrypted is placed in the object light path, which is first phase encoded as $\exp[iO(x_0, y_0)]$, and then the encoded image is further encoded by the random key loaded on the SLM. The complex amplitude distribution of object beam on SLM can be expressed as:

$$U_0(x_0, y_0) = A_0 \exp[iO(x_0, y_0)] \exp[iP(x_0, y_0)] \quad (1)$$

Where $P(x_0, y_0)$ is the random phase key generated by the computer. Then, SLM and charge coupled device (CCD) are placed on the front focal plane and imaging plane of the lens, respectively. The complex amplitude distribution imaged on the CCD plane through the lens can be expressed as:

$$\begin{aligned} U(x, y) &= \frac{1}{M} U_0 \left(-\frac{x}{M}, -\frac{y}{M}\right) \\ &= A_1 \cdot \varphi_0(x, y) \end{aligned} \quad (2)$$

where M represents the magnification, $A_1 = \frac{A_0}{M}$ and $\varphi_0(x, y) = \exp[iO(-\frac{x}{M}, -\frac{y}{M})] \exp[i2\pi \cdot P(-\frac{x}{M}, -\frac{y}{M})]$ represent the amplitude and phase distribution of object beam on the CCD plane, respectively. In the reference light path, the complex amplitude distribution of the reference light modulated by the host image can be written as:

$$\begin{aligned} U_R(x, y; \varphi_R) &= \exp(i\varphi_R) Frt[h(x_0, y_0)] \\ &= A_h(x, y) \exp\{i[\varphi_h(x, y) + \varphi_R]\} \end{aligned} \quad (3)$$

In (3), $h(x_0, y_0)$ refers to the host image placed in the reference light path, *Frt* represents the Fresnel transform. $A_h(x, y)$ and $\varphi_h(x, y)$ are the amplitude information and phase information of the host image on the CCD plane. Where φ_R represents the phase shifts introduced by the phase shift device.

Then, the two beams will overlap on the CCD plane to form interference fringes to hide the encrypted image. The light intensity on CCD plane can be expressed as:

$$\begin{aligned} I(x, y) = {A_1}^2 + A_h^2(x, y) \\ + 2A_1 A_h(x, y) \cos[\varphi_h(x, y) + \varphi_R - \varphi_0(x, y)] \end{aligned} \quad (4)$$

In the traditional decryption method, different phase shifts need to be introduced into the reference optical path, and then the multi-step phase-shifting method with equal step or unknown phase shifts combined with the correct key is used for decryption, which not only increases the amount of recorded data, but also limits its application in dynamic encryption to a certain extent. Moreover, the unstable factors in phase-shifting device will also lead to poor decryption quality, which greatly limits the application of this method. In this paper, the corresponding relationship between the encrypted hidden interferogram and the original image will be trained to achieve the approximation of the physical model between them, and to achieve high-quality

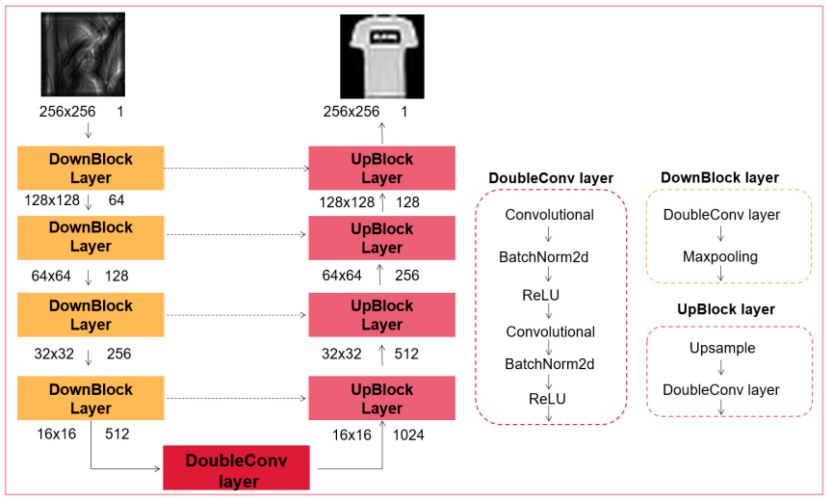

Fig. 2. The designed U-net based optical image encryption and hiding architecture. The encrypted hidden interferogram is used as the input of the network, and the reconstructed original image is used as the output of the network.

image decryption with only one collected interferogram. For simplicity, the coordinates (x, y) will be omitted in the following derivation.

B. Network Description

The designed U-net based optical image encryption and hiding architecture is shown in Fig. 2. Using the designed U-net [28], the mapping relationship between the encrypted hidden interferogram and reconstructed original image is learned in an end-to-end manner, and this process can be described as:

$$\bar{O} = \Gamma_{U-net}(I) \tag{5}$$

where $\bar{O}$ indicates the preliminary reconstructed image estimated from the designed U-net, and $\Gamma_{U-net}(\cdot)$ indicates the mapping function between the encrypted hidden interferogram I and ground truth image O. The mapping function $\Gamma_{U-net}(\cdot)$ can be optimized after training the designed U-net using N pairs of different label training dataset, and this process of continuous optimization can be represented as

$$\hat{\Gamma}_{U-net} = \arg\min \frac{1}{N} \sum_{1}^{N} \left\| \bar{O}^n - O^n \right\| \tag{6}$$

where $n = 1, 2, \ldots, N$. Thus, the reconstructed original image can be predicted from the optimized U-net model:

$$\hat{O} = \hat{\Gamma}_{U-net}(I) \tag{7}$$

where $\hat{O}$ and $\hat{\Gamma}_{U-net}(\cdot)$ indicate the reconstructed image and optimized U-net model, respectively.

The designed U-net is mainly composed of two paths, one down sampling path for image feature extraction and one up sampling path for image reconstruction. One encrypted hidden interferogram with the size of 256 × 256 is used as the input of the designed U-net. As shown in Fig. 2, the feature extraction part includes four Downblock layers, and each layer is composed of a Doubleconv layer and a Maxpooling layer. The Doubleconv layer successively includes a convolution layer, a regularization layer, an activation layer, a convolution layer, a regularization layer and an activation function. And the output parameters of each Downblock layer are shown in Fig. 2, in which the final features are entered into a Doubleconv layer. In the up sampling path, according to the construction idea of U-net, we copy and crop the output features with the corresponding features of each layer, and use it for upconversion. Symmetric, the up sampling path consists of four Upblock layers, each layer consists of an upsample and a Doubleconv layer, and the mode of up sampling is "bilinear". The kernel size is 3×3, and Strides = 1, the activation function is ReLu, and the regularization layer is BatchNorm2d, BN. In the network applications, two different datasets are used for training, which are simple image from Fashion-MNIST dataset [29] and complicated natural image from Faces-LFW dataset [30]. Taking the above datasets as the original images to be encrypted, the corresponding encrypted hidden interferograms are obtained combined with (1) to (4), in which the whole process is implemented by simulation with MATLAB [13]. Each dataset contains 6000 original images, 5400 original images are randomly selected as training samples, and the other 600 original images that did not participate in training are selected as test dataset. In the training, Adam optimizer [31] is used to optimize the weight and deviation of designed U-net, and the loss function is written as:

$$Loss = \frac{1}{N} \sum_{1}^{N} \left\| \hat{O} - O \right\| \tag{8}$$

The weights initialization is the normal random distribution; the Batch size is 1 and the number of iterations is 200. All the training are carried out in the environment of Python V3.7, and the programs are written using pytorch. The NVIDIA Geforce GTX1080Ti GPU is implemented for accelerating. The training and testing error curves of the trained convolution network are shown in Fig. 3. These curves converge quickly to almost the same value, which shows that the network has a good performance in the testing dataset.

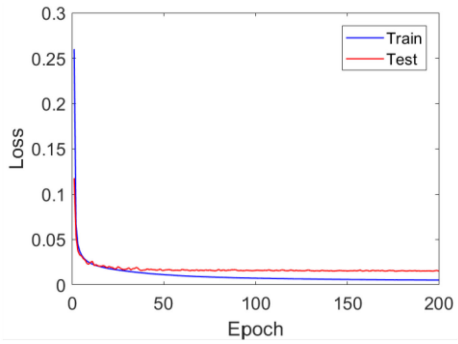

Fig. 3. The training and testing error curves.

TABLE I
SSIM VALUES FOR FASHION-MNIST AND FACES-LFW DATASET

	1	2	3	4	5	6
Fashion-MNIST	0.9893	0.9843	0.9865	0.9875	0.9878	0.9853
Faces-LFW	0.9472	0.9315	0.9139	0.9288	0.9180	0.9497

TABLE II
PSNR VALUES FOR FASHION-MNIST AND FACES-LFW DATASET (DB)

	1	2	3	4	5	6
Fashion-MNIST	35.85	38.06	39.70	35.59	39.74	35.53
Faces-LFW	32.10	31.37	29.47	31.06	28.71	33.07

III. ANALYSIS OF SIMULATION RESULTS

In the simulation part, two different datasets are selected for training and testing, which are Fashion-MNIST dataset and Faces-LFW dataset. Three indicators including peak signal to noise ratio (PSNR), structural similarity (SSIM) [32] and correlation coefficient (CC) are calculated to quantitatively analyze the simulation results. Six sets of the reconstruction results in each dataset are shown in Figs. 4 and 5, respectively. The results show that the decrypted images are basically consistent with the ground truth images, and some detail information can be recovered well, especially for complex face images. For quantitative comparison, PSNR, SSIM and CC of the two groups of simulation results are calculated and shown in Tables I, II and III, respectively. Table data shows that the PSNR, SSIM and CC values of Fashion-MNIST testing dataset are higher than those of Faces-LFW dataset, mainly because the Fashion-MNIST testing dataset is relatively simpler and has less image information. But in any case, the PSNR, SSIM and CC values of the two groups are very high, which verifies the feasibility and effectiveness of the proposed method.

TABLE III
CC VALUES FOR FASHION-MNIST AND FACES-LFW DATASET

	1	2	3	4	5	6
Fashion-MNIST	0.9996	0.9977	0.9981	0.9992	0.9987	0.9992
Faces-LFW	0.9951	0.9964	0.9866	0.9957	0.9861	0.9940

IV. METHOD PERFORMANCE

A. Safety Analysis

The security of the proposed POIEH method is studied. The main keys of the method are the information of the host image and the random phase mask. When the host image is replaced with another image, the encrypted hidden interferogram is input into the trained network, and the correct decryption result cannot be obtained. The decryption result is similar to noise distribution, as shown in Fig. 6(a). In addition, when the random phase mask is replaced, the decryption result is also similar to the noise distribution (Fig. 6(b)). When the irradiation wavelength is set to 600 nm and there is an error in the diffraction distance of the host image, the correct decryption result cannot be obtained, as shown in Fig. 6(c) and 6(d). The above analysis results prove that the proposed method has high security, and the decrypted image is very sensitive to the main key. This further proves that the random key replacement realized by SLM can greatly improve the flexibility and security of the encryption system.

B. Generalization Ability

In this section, the generalization ability of the network is further studied. The network trained with Faces-LFW dataset is selected as the test network, and five groups of datasets not participating in the training are selected as the test dataset, which are Fashion-MNIST dataset, Chinese character, MNIST dataset, Dog dataset and ImageNet dataset [33], respectively. On the premise of combining the correct key, five groups of encrypted hidden interferograms are input to the trained network to obtain the corresponding decryption results, as shown in Fig. 7. The displayed results show that although the five groups of data did not participate in the training, the correct decryption results can still be obtained. Moreover, to quantitatively analyze the results in Fig. 7, the PSNR values of each group of images are calculated and showed in Fig. 7(f). According to the curve distribution results, the PSNR values in Fig. 7(a), 7(d) and 7(e) are higher, basically maintained at about 30dB, while the PSNR value of Fig. 7(c) is lower because there is noise-like distribution in the reconstruction results, but these recovered numbers are still clearly identifiable.

V. ROBUSTNESS ANALYSIS

In this section, we discuss the robustness of the method in detail, calculate and compare the results using same interferogram with traditional decryption method. Firstly, we study the impact of JPEG compression attack on the proposed method.

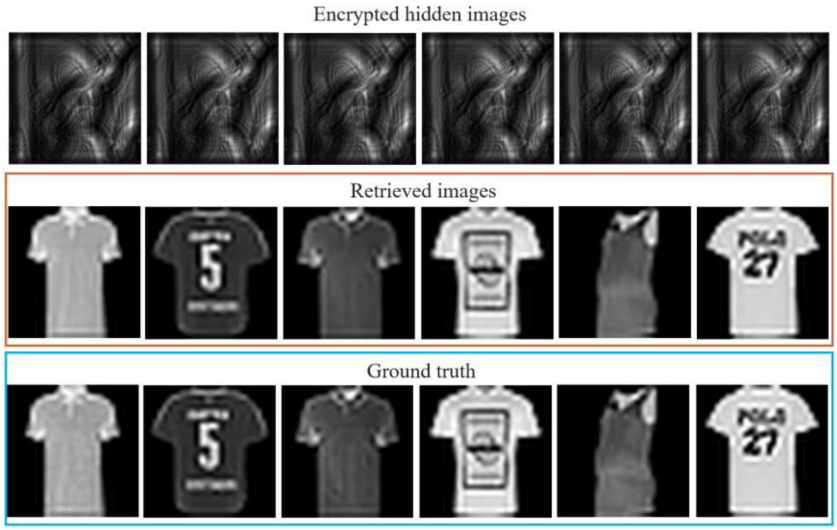

Fig. 4. Partially decrypted images from Fashion-MNIST testing dataset. The first row shows the encrypted hidden interferograms, the second row and third row show the decrypted images from the trained U-net model and ground truth images.

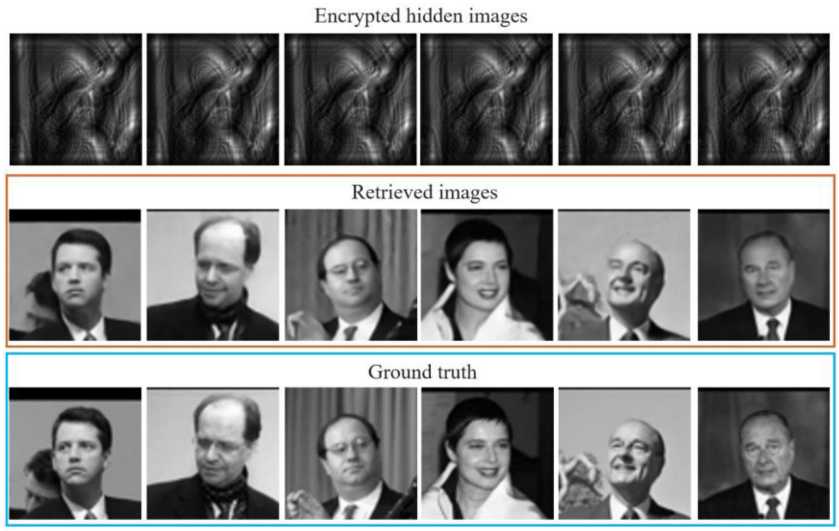

Fig. 5. Partially decrypted images from Faces-LFW dataset. The first row shows the encrypted hidden interferograms, the second row and third row show the decrypted images from the trained U-net model and ground truth images.

The image to be encrypted is a capital letter A, the quality factor of JPEG compression is changed from 100 to 96, and the interval is 1. The compressed encrypted hidden interferograms with different quality factor are shown in Fig. 8(a), and the decrypted images obtained by using the four-step phase-shifting method combined with the correct key are shown in Fig. 8(b). Similarly, after inputting one of the same interferograms into the trained network, the decrypted images are shown in Fig. 8(c). When the quality factor is 100 and 99, the letter A is vaguely visible in the decryption results obtained by the four-step phase-shifting algorithm, but when the quality factor decreases, the original images cannot be recognized. However, the proposed method can still get the correct and clear original image.

Then, the impact of shear attack on the proposed method is discussed. Firstly, we cut the interferograms with different area sizes and the encrypted hidden interferograms after cutting are shown in Fig. 9(a). Similar to the above analysis, the interferograms are decrypted by the traditional method, and the reconstruction results are shown in Fig. 9(b). It can be seen from the results that when the cut area does not involve the main information, it will not affect the decryption of the main information, but when the interferogram area of the main information is cut, the information in cut area cannot be reconstructed correctly. Similarly, the decrypted image reconstructed by the proposed method also has the same problem (Fig. 9(c)). Therefore, for shear attack, the DL-based method has similar robustness with the traditional method.

Furthermore, we also discuss the influence of rotation attack on the reconstruction results. The interferograms are rotated at angles of 0.1°, 0.5°, 1°, 1.5° and 2°, and the rotating

Fig. 6. Retrieved images with the incorrect keys in the decryption process: (a) Incorrect host image; (b) Incorrect random phase mask; (c) the wavelength is 600 nm; and (d) the diffraction distance of the host image has an error of 5%.

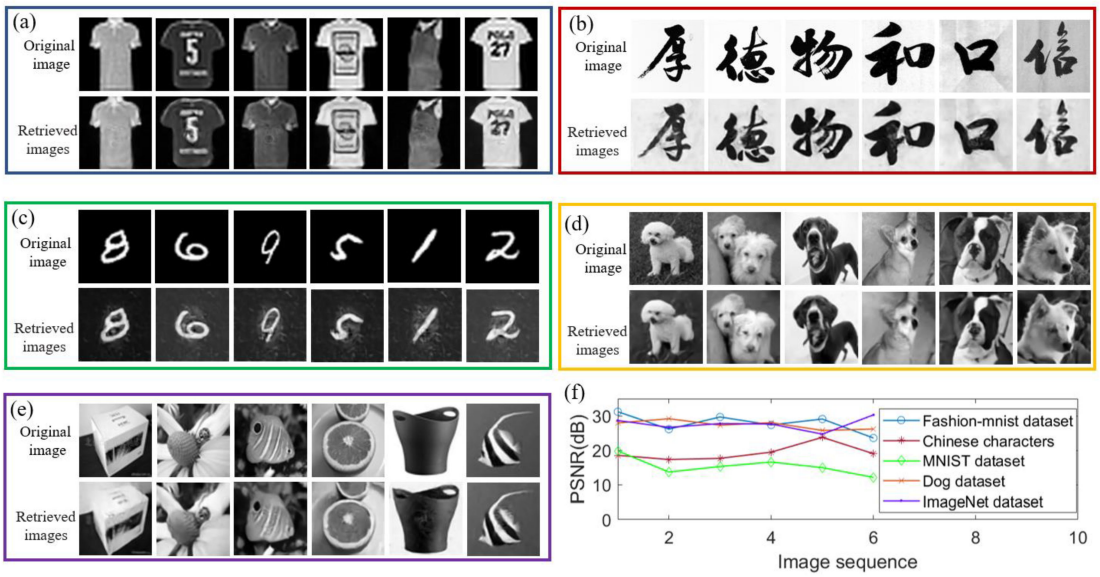

Fig. 7. Generalization ability of the proposed method. Where the model is trained by Faces-LFW dataset and tested on other datasets that did not participate in the training. (a) Fashion-MNIST dataset. (b) Chinese characters. (c) MNIST dataset. (d) Dog dataset and (e) ImageNet dataset. (f) PSNR values are calculated using above five sets of datasets.

interferograms are shown in Fig. 10(a). The decryption results obtained by the traditional method and the DL-based method are shown in Fig. 10(b) and 10(c). When the rotation angle is less than 1 degree, the image decrypted by the traditional method is still clearly visible, but when the rotation angle is greater than 1 degree, the decryption image is similar to the clutter noise distribution, and the original image cannot be identified. However, the proposed method is basically not affected by the variety of angle.

Finally, we discuss the influence of multiplicative noise on the reconstruction results. The interferograms are respectively added with multiplicative noise with mean value of 0 and variance of 0.01 to 0.05, and the decryption results are shown in Fig. 11. The interferograms with different level noise, corresponding decryption results obtained using traditional method and DL-based method are showed in Fig. 11(a) to Fig. 11(c). It can be seen from the results that when the noise variance is 0.01 and 0.02, the image decrypted by the traditional method is

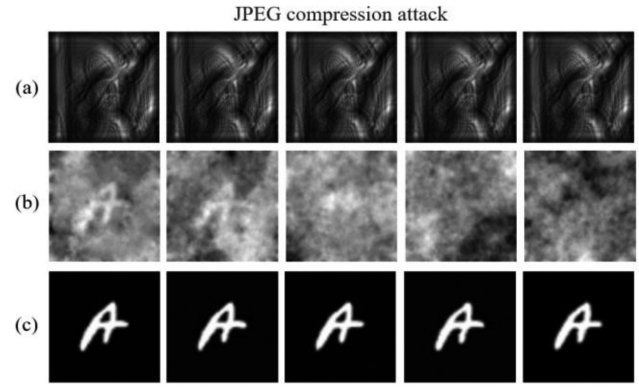

Fig. 8. The robustness against JPEG compression attack. (a) Interferograms with different quality factor of JPEG compression; Decrypted images obtained by different methods. (b) Four-step phase-shifting algorithm. (c) DL-based method.

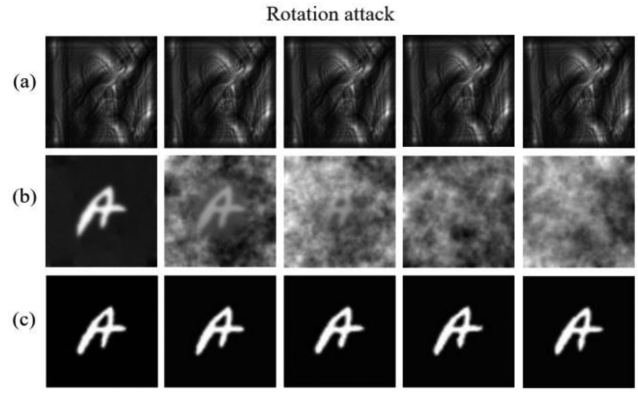

Fig. 10. The robustness against rotation attack. (a) Interferograms with different rotation angles; Decrypted images obtained by different methods. (b) Four-step phase-shifting algorithm. (c) DL-based method.

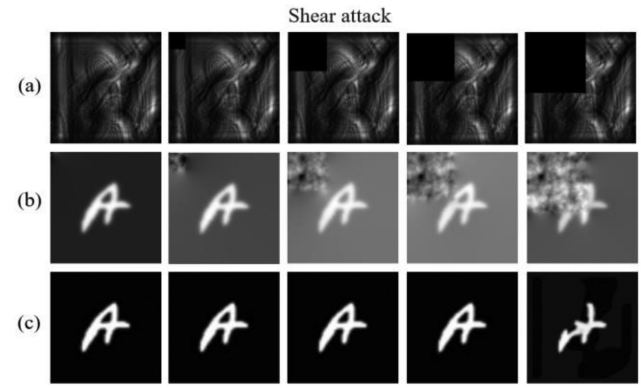

Fig. 9. The robustness against shear attack. (a) Interferograms with different shear sizes; Decrypted images obtained by different methods. (b) Four-step phase-shifting algorithm. (c) DL-based method.

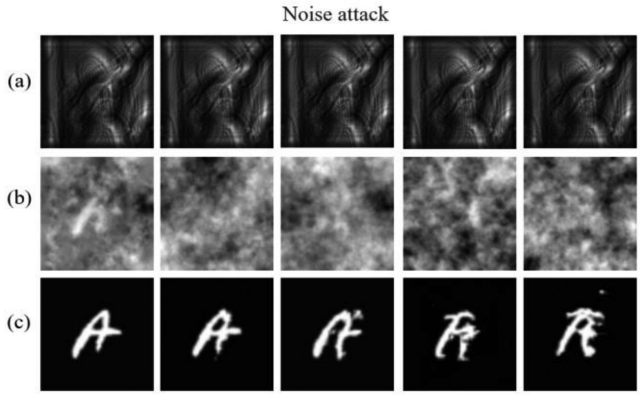

Fig. 11. The robustness against multiplicative noise attack. (a) Interferograms with different noise level; Decrypted images obtained by different methods. (b) Four-step phase-shifting algorithm. (c) DL-based method.

vaguely visible, which shows that the POIEH method is sensitive to the attack of multiplicative noise. The results decrypted using the proposed method are also affected when the noise variance is greater than 0.02, but the original image can be recognized basically.

Therefore, the above four groups of results and analysis prove that the proposed method can greatly improve the robustness of POIEH scheme and further improve its anti-attack, which is very useful in practical application.

VI. Conclusion

In this paper, we propose a single exposure phase-only optical image encryption and hiding method using deep learning. The corresponding relationship between the encrypted hidden interferogram and the reconstructed image is learned through constructing the train datasets for the learning of an end-to-end designed U-net. The simulation results prove that the proposed deep learning-based reconstruction method can realize high-quality image decryption by using only one interferogram, and the performance of the method proves the proposed method has higher security, stronger generalization ability and robustness. This will greatly solve the limitation problem in the original decryption method and further improve the application scope of image security. However, the proposed method is a static method for decryption, and each key needs to be trained respectively. This deficiency will be further solved in our future work.

VII. References

[1] P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995, doi: 10.1364/OL.20.000767.

[2] G. H. Situ and J. J. Zhang, "Double random-phase encoding in the fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, Jul. 2004, doi: 10.1364/OL.29.001584.

[3] B. Javidi *et al.*, "Roadmap on optical security," (in English), *J. Opt.-Uk*, vol. 18, no. 8, Aug. 2016, doi: 10.1088/2040-8978/18/8/083001.

[4] S. X. Xi *et al.*, "Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram," *Opt. Exp.*, vol. 25, no. 7, pp. 8212–8222, Apr. 2017, doi: 10.1364/Oe.25.008212.

[5] K. Nakano and H. Suzuki, "Analysis of singular phase based on double random phase encoding using phase retrieval algorithm," *Opt. Laser Eng.*, vol. 134, Nov. 2020, doi: 10.1016/j.optlaseng.2020.106300.

[6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - A survey," *Proc. IEEE*, vol. 87, no. 7, Jul. 1999, pp. 1062–1078, doi: 10.1109/5.771065.

[7] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Appl. Opt.*, vol. 41, no. 26, pp. 5462–5470, Sep. 2002, doi:10.1364/Ao.41.005462.

[8] J. Li, T. Zhong, X. F. Dai, C. X. Yang, R. Li, and Z. L. Tang, "Compressive optical image watermarking using joint fresnel transform correlator architecture," *Opt. Laser Eng.*, vol. 89, pp. 29–33, Feb. 2017, doi: 10.1016/j.optlaseng.2016.02.024.

[9] L. S. Sui, J. O. Wang, A. L. Tian, and A. Asundi, "Optical image hiding under framework of computational ghost imaging based on an expansion strategy," *Opt. Exp.*, vol. 27, no. 5, pp. 7213–7225, Mar. 2019, doi: 10.1364/Oe.27.007213.

[10] S. M. Jiao, C. Y. Zhou, Y. S. Shi, W. B. Zou, and X. Li, "Review on optical image hiding and watermarking techniques," *Opt. Laser Technol.*, vol. 109, pp. 370–380, Jan. 2019, doi: 10.1016/j.optlastec.2018.08.011.

[11] M. Z. He, L. Z. Cai, Q. Liu, and X. L. Yang, "Phase-only encryption and watermarking based on phase-shifting interferometry," *Appl. Opt.*, vol. 44, no. 13, pp. 2600–2606, May 2005, doi:10.1364/Ao.44.002600.

[12] J. Li, J. S. Li, L. N. Shen, Y. Y. Pan, and R. Li, "Optical image encryption and hiding based on a modified Mach-Zehnder interferometer," *Opt. Exp.*, vol. 22, no. 4, pp. 4849–4860, Feb. 2014, doi: 10.1364/Oe.22.004849.

[13] J. S. Li *et al.*, "A one-time pad encryption method combining full-phase image encryption and hiding," *J. Opt.-Uk*, vol. 19, no. 8, Aug. 2017, doi: 10.1088/2040-8986/aa7469.

[14] J. S. Li, X. X. Lu, Q. N. Zhang, J. D. Tian, and L. Y. Zhong, "Phase-only optical image encryption and hiding based on normalization and orthogonalization phase-shifting algorithm," *Proc. SPIE*, vol. 11209, 2019, doi: 10.1117/12.2548749.

[15] Y. Rivenson, Y. C. Wu, and A. Ozcan, "Deep learning in holography and coherent imaging," *Light-Sci. Appl.*, vol. 8, pp. 370–380, Sep. 2019, doi: 10.1038/s41377-019-0196-0.

[16] K. Q. Wang, K. M. Qian, J. L. Di, and J. L. Zhao, "Y4-Net: A deep learning solution to one-shot dual-wavelength digital holographic reconstruction," *Opt. Lett.*, vol. 45, no. 15, pp. 4220–4223, Aug. 2020, doi: 10.1364/Ol.395445.

[17] S. J. Feng *et al.*, "Fringe pattern analysis using deep learning," *Adv. Photon.*, vol. 1, no. 2, Mar. 2019, Art. no. 025001, doi: 10.1117/1.Ap.1.2.025001.

[18] Y. Li, J. L. Di, K. Q. Wang, S. F. Wang, and J. L. Zhao, "Classification of cell morphology with quantitative phase microscopy and machine learning," *Opt. Exp.*, vol. 28, no. 16, pp. 23916–23927, Aug. 2020, doi: 10.1364/Oe.397029.

[19] I. Hoshi, T. Shimobaba, T. Kakue, and T. Ito, "Single-pixel imaging using a recurrent neural network combined with convolutional layers," *Opt. Exp.*, vol. 28, no. 23, pp. 34069–34078, Nov. 2020, doi: 10.1364/Oe.410191.

[20] H. Hai, S. X. Pan, M. H. Liao, D. J. Lu, W. Q. He, and X. Peng, "Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning," *Opt. Exp.*, vol. 27, no. 15, pp. 21204–21213, Jul. 2019, doi: 10.1364/Oe.27.021204.

[21] L. N. Zhou, Y. Xiao, and W. Chen, "Machine-learning attacks on interference-based optical encryption: Experimental demonstration," *Opt. Exp.*, vol. 27, no. 18, pp. 26143–26154, Sep. 2019, doi: 10.1364/Oe.27.026143.

[22] W. Q. He, S. X. Pan, M. H. Liao, D. J. Lu, Q. Xing, and X. Peng, "A learning-based method of attack on optical asymmetric cryptosystems," *Opt. Laser Eng.*, vol. 138, Mar. 2021, Art. no. 106415, doi: 10.1016/j.optlaseng.2020.106415.

[23] L. F. Chen, B. Y. Peng, W. W. Gan, and Y. Q. Liu, "Plaintext attack on joint transform correlation encryption system by convolutional neural network," *Opt. Exp.*, vol. 28, no. 19, pp. 28154–28163, Sep. 2020, doi: 10.1364/Oe.402958.

[24] L. Zhang, Y. Wang, D. H. Li, Q. Li, W. X. Zhao, and X. W. Li, "Cryptanalysis for a light-field 3D cryptosystem based on M-cGAN," *Opt. Lett.*, vol. 46, no. 19, pp. 4916–4919, Oct. 2021, doi: 10.1364/Ol.436049.

[25] Y. Wang, Z. Q. Ren, L. Zhang, D. H. Li, and X. W. Li, "3D image hiding using deep demosaicking and computational integral imaging," *Opt. Laser Eng*, vol. 148, Jan. 2022, Art. no. 106772, doi: 10.1016/j.optlaseng.2021.106772.

[26] R. J. Ni, F. Wang, J. Wang, and Y. H. Hu, "Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain," *IEEE Photon. J.*, vol. 13, no. 3, Jun. 2021, Art. no. 7800116, doi: 10.1109/Jphot.2021.3076480.

[27] Q. Li, X. F. Meng, Y. K. Yin, and H. Z. Wu, "A multi-image encryption based on sinusoidal coding frequency multiplexing and deep learning," *Sensors-Basel*, vol. 21, no. 18, Sep. 2021, Art. no. 106772, doi: 10.3390/s21186178.

[28] H. Xiao, K. Rasul, and R. Vollgraf," Fashion-MNIST: A novel image dataset for benchmarking machine learning algorithms," 2017. [Online]. Available: http://arxiv.org/abs/1708.07747

[29] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," vol. 9351, pp. 234–241, Oct. 2015, doi: 10.1007/978-3-319-24574-4_28.

[30] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," *Comput. Vis. Lab, Comput. Sci. Dept.*, Univ. Massachusetts, Amherst, MA, USA, 2007. [Online]. Available: http://vis-www.cs.umass.edu/lfw/

[31] J. Kingma and Ba, "Adam: A method for stochastic optimization," 2014, *arXiv 1412.6980*. [Online]. Available: https://arxiv.org/abs/1412.6980v9

[32] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/Tip.2003.819861.

[33] O. Russakovsky *et al.*, "ImageNet large scale visual recognition challenge," *Int. J. Comput. Vis.*, vol. 115, no. 3, pp. 211–252, Dec. 2015, doi: 10.1007/s11263-015-0816-y.