Optica Applicata, Vol. LIV, No. 3, 2024
DOI: 10.37190/oa240309

Robust encryption in diffractive-imaging-based encryption scheme using deep learning

SHIBANG MA[#], YI QIN[#], QIONG GONG, HONGJUAN WANG

College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China

Corresponding author: Yi Qin, 641858757@qq.com

[#]The authors contribute equally to this manuscript

Noise attack is a potential threat to optical cryptosystems because the contaminated ciphertext always yields degraded decrypted result. What is more, such contamination can hardly be eliminated by traditional methods, as the ciphertext itself is also a noise-like image. In this paper, we propose a deep-learning-based approach to deal with this problem. The contaminated ciphertexts, which produce unrecognized decrypted images, can yield high quality ones after being repaired by a deep neural network. We take the diffractive-imaging-based encryption (DIBE) scheme as an example to illustrate our method. Numerical results are presented to show the feasibility and validity of the proposal.

Keywords: robust encryption, noise attack deep learning, diffractive-imaging-based encryption.

1. Introduction

Optical information security emerges as a new research field [1-4] since the invention of the double random phase encoding (DRPE) [5]. DRPE employs two random phase only masks at the input and the output planes of an optical 4*f* system to transform the plaintext into complex stationary white noise. After DRPE, a number of optical cryptosystems are reported. In particular, the diffractive-imaging-based encryption (DIBE) aroused wide attention due to its some advantages over DRPE. For example, only intensity maps need to be recorded to recover the plaintext; therefore, the optical arrangement of DIBE is rather simple [6, 7]. Furthermore, the ciphertext is obtained by nonlinear transformation of the plaintext, and this reinforces the security of DIBE to some extent [8].

Noise attack means the contamination of the ciphertext during the storage or transmission. It is a potential threat to optical cryptosystems, as it can significantly degrade the quality of the decrypted images [9, 10]. This problem becomes especially prominent when it comes to DIBE [6, 11, 12]. Recently, researchers set about coping with the noise problem. However, most current efforts focus on designing a proper "container" to protect the plaintext [9]. The first data container introduced to optical cryptosystem is the quick response (QR) code [9], and thereafter several its derivatives are developed and

applied [13, 14]. Employing data container exploits a feasible way to cope with the polluted ciphertext. However, due to their small capacity, the data container can only accommodate a small amount of information and therefore is unavailable for large-sized plaintext, such as gray scale image.

Deep learning, which is based on a multi-layered deep neural network (DNN), receives more and more attention as it offers general methods to numerous judgment-based applications [15]. In particular, it has been widely employed to resolve various inverse problems [16-18]. The training of the DNN can be regarded as a generic function approximation. In other words, if the DNN is trained with sufficient pairs of matched inputs and outputs of a hitherto-unknown system (*i.e.* training set), it can build a computational structure that translates the input from another set (*i.e.* test set) to their corresponding output. Recently, DNN is also introduced for cryptanalysis of optical cryptosystems [19, 20].

In this paper, we propose a solution, from another perspective, to resist the noise attack faced by DIBE. We focus on repairing the ciphertext via a well-trained DNN. In our proposal, the decryption process consists of two steps. In the first step, the polluted ciphertext is denoised with a well-trained model of the DNN. Secondly, the plaintexts are decrypted from the purified ciphertexts with the median-filter based phase retrieval algorithm. To the best of our knowledge, this is the first paper that reports restoring the contaminated ciphertext of an optical cryptosystem with DNN. Both theoretical analyses and numerical results are detailed to demonstrate the proposal.

2. Principle

2.1. Image encryption and decryption in DIBE

Figure 1 schematically shows an optical arrangement of DIBE. Basically, the scheme translates an input image (plaintext) into a noise-like image (ciphertext) through mod-

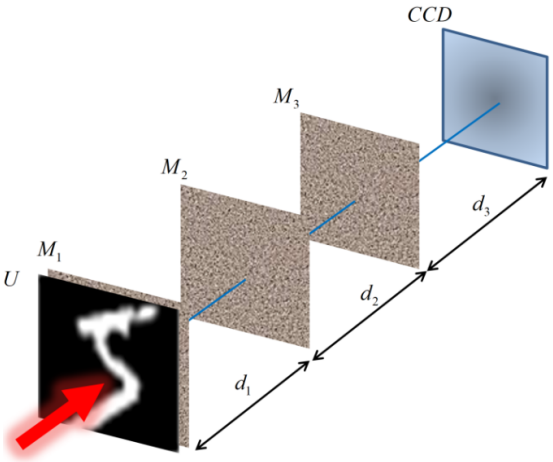

Fig. 1. The optical configuration of a representative DIBE scheme.

ulating its diffraction field with a series of random phase masks (RPMs). As shown in Fig. 1, all of the elements are optically coaxial. The input image (*i.e.* U) and the first RPM M1 are bonded together and are placed at the input plane; meanwhile, M2 and M3 locate at the distances of d_1 and $d_1 + d_2$ from them, respectively. The phase values of each RPM are randomly distributed within $[0, 2\pi]$. Furthermore, a CCD camera separating from M3 with a distance of d_3 locates at the output plane. A coherent light source with a wavelength of λ is employed to illuminate the input image. The light diffracting from the input image passes through the three RPMs and then reaches to the output plane, where the diffraction pattern is registered with a CCD camera.

Hereinafter, the coordinates of the input plane, M2, M3, and the output plane are respectively denoted by the symbols (x, y), (η, ξ), (p, q) and (μ, v). The wavefront immediately before M2 can be expressed as

$$O(\eta, \xi) = \mathrm{FSP}\Big[U(x, y)M_1(x, y);\, d_1\Big] \tag{1}$$

where FSP[P; d] stands for the free space propagation of P with a distance of d. Following this symbol, the intensity pattern on the CCD plane can be expressed as

$$I(\mu, v) = \left|\mathrm{FSP}\left[\mathrm{FSP}\left\{\mathrm{FSP}\Big[U(x, y)M_1(x, y);\, d_1\Big]M_2(\eta, \xi);\, d_2\right\}M_3(p, q);\, d_3\right]\right|^2 \tag{2}$$

where $|\cdot|$ means the modulus calculation. $I(\mu, v)$ is saved as the ciphertext, while the RPMs, the wavelength, and the axial distances are regarded as the secret keys. For decryption, a median-filtering-based phase retrieval algorithm (MF-PRA) can be employed [7]. The MF-PRA consists of two iterative cycles: the first cycle produces a preliminary recovery of the primary image, and the other one further optimizes it. In addition, two parameters, denoted by δ_1 and δ_2, are respectively adopted as the criterions to judge whether these cycles should be terminated. It is shown that the MF-PRA could accurately reconstruct the plaintext if all the correct secret keys are provided.

2.2. Noise attack and the proposal

Figure 2 illustrates the noise attack that a DIBE scheme may encounter. The plaintext is firstly encrypted by DIBE and then sent to the authorized receiver. However, the ciphertext is always transmitted via the public channel, which is of low security level. Consequently, the damage from an ill-disposed intruder or other irresistible factors may lead to the pollution of the ciphertext. The direct consequence of noise attack is that the authorized user can only obtain low-quality or even totally unrecognized decrypted images. Various optical cryptosystems have been demonstrated to be vulnerable to noise attack, and so does DIBE [6-8]. However, although many researchers have tested and demonstrated the vulnerability of their cryptosystems against noise attack, few of them engage to eliminate the noise existing in the ciphertext. In fact, the noise

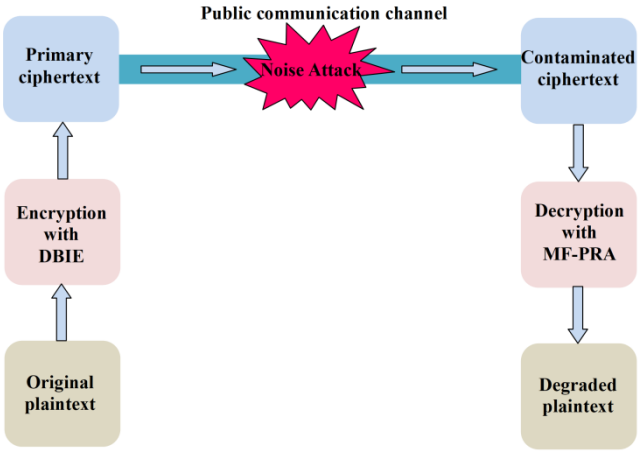

Fig. 2. The noise attack to the DIBE scheme.

in the ciphertext is rather difficult to be removed since the ciphertext itself also has a noise appearance. In this paper, we will mainly focus on the damaged ciphertext that is polluted by the multiplicative noise. The pollution of the ciphertext can be described as follows:

$$C_c = C_o(1 + \alpha N) \tag{3}$$

where C_o is the normalized original ciphertext (OCT), C_c is the contaminated ciphertext (CCT), α is the weight of the noise, and N is the uniform noise whose values are uniformly distributed in [0, 1].

It is known that, for any unknown systems, a proper DNN is capable of foretelling the response if the input is given, and this is because the DNN has learned the inherent relation between them from the experience accumulated during training [15]. Therefore, the DNN is potentially able to distinguish the noise in the CCT and can further remove it, although this task is extensively difficult for human or conventional methods. In order to cope with the noise attack, we propose to utilize the DNN to repair the CCT before the standard decryption procedure. The schematic diagram for expressing our intention is depicted in Fig. 3.

The structure of the designed DNN for repairing the CCT is schematically shown in Fig. 4. Besides the input and the output layers, the DNN comprises totally five hidden layers. The neurons of the output layer have linear transfer functions, whereas the other neurons in the input and hidden layers adopt Rectified Linear Unit (ReLU) transfer functions. It should be pointed out that the configuration of the number of the layers and neurons of a DNN is a complex problem, and there are several methods for solving it [21,22]. In our case, these parameters are obtained by testing a series of different configurations, and the current one exhibits better performance on both the training set as well as the testing set.

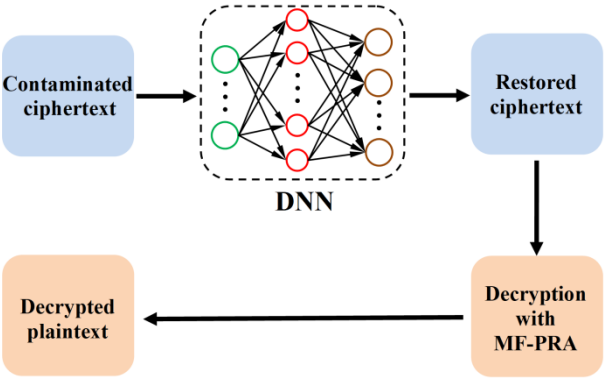

Fig. 3. The proposed approach for decryption in DIBE with contaminated ciphertext.

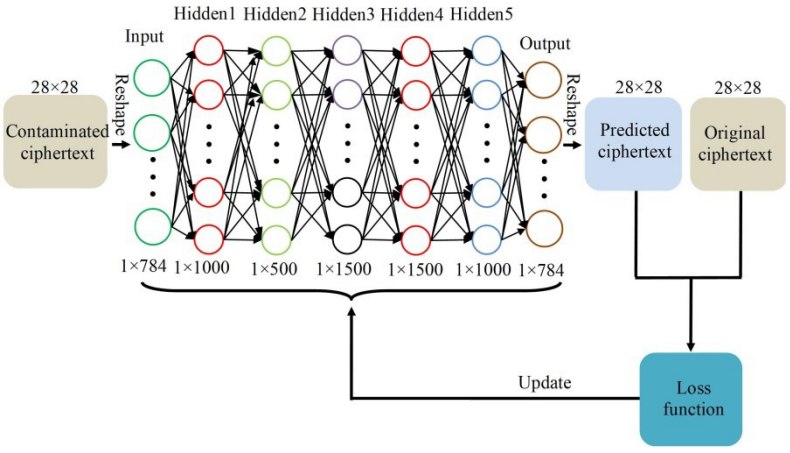

Fig. 4. Detailed schematic of our DNN architecture, indicating the number of layers, nodes in each layer, and the training process.

The mathematical relationship between two adjacent layers in the proposed DNN can be given by [15]

$$X_{(k+1)} = \sigma(W_{(k)}X_{(k)} + b_{(k)}) \tag{4}$$

where k represents the layer number, and $W_{(k)}$ and $b_{(k)}$ stand for respectively the weight matrix and the bias vectors. $\sigma(\cdot)$ denotes the active function, and its expression for the ReLU function is given by

$$\sigma(x) = \max(0, x) \tag{5}$$

For the subsequent training, 12 000 images, selected from the MNIST database, act as the plaintexts of DIBE to generate the OCTs. Meanwhile, these OCTs are polluted

in the manner illustrated by Eq. (3) to obtain their contaminated versions (*i.e.* CCTs). A total of 12000 OCT-CCT pairs are produced to train the DNN, of which 95% are employed as the training set and 5% as the testing set. Both the CCTs and PCTs are of 28×28 pixels, and the former is reshaped to 1×784 vectors before being fed into the DNN. The output of the DNN is also with the size of 1×784, and it is reshaped back to 28×28 pixels images to form the predicted ciphertext (PCT). The mean squared error (MSE) between PCT and CCT is employed as the loss function

$$\mathrm{MSE} = \frac{1}{N}\sum_{1}^{N}\left(\sum\sum(\mathrm{OCT\text{-}CCT})^2\right) \tag{6}$$

where N denotes the number of iteration. For training, the weight matrix is iteratively updated to minimize the MSE with the back-propagation algorithm [15]. During training, the Adam is assigned as the optimizer because it is almost the best in the context of the earlier algorithms. In Adam, momentum is introduced as an estimate of the first order moment. Moreover, Adam contains bias corrections to the estimates of both the first-order moments and the second order moments. Meanwhile, a minibatch of several samples from the training set are employed to generate the estimator every time, and the parameters obtained from these samples are employed to update the weight matrix and bias vectors. In addition, a fixed epoch number is preset to decide when to terminate the training. Finally, the model achieving the minimum of MSE is saved as the predicting model (PM). Generally, if the loss function could reach to a very small value, the PM will be capable of transforming the CCT to a clean version approximating to the PCT.

3. Results and discussions

Both MATLAB R2011a and Python 3.7 are employed to perform the numerical simulation. The former is used to read the MNIST dataset, generate the training data and testing data, and perform encryption and decryption in DIBE, while the latter is used mainly to train the DNN. Also, we adopt a GTX1070 graphics card (NVIDIA) to boost the calculation speed. To simulate DIBE, the wavelength of illumination light is set as $\lambda = 632.8$ nm. The axial distances d_1, d_2, and d_3 are all equal to 50 mm. In MF-PRA, the values of δ_1 and δ_2 are respectively set as 0.0001 and 0.00001. The data set for training and testing the DNN is generated in this simulated DIBE. By choosing 12000 images from the MNIST dataset as the plaintexts and encrypting them with the DIBE, we get a set of 12000 OCTs. Afterwards, the corresponding CCTs are produced by the method illustrated by Eq. (3). Among the 12000 OCT-CCT pairs, 11400 pairs are employed as the training set and the rest as the testing set. In order to simulate the noise with different intensities, the value of α is randomly selected within [0, 0.5] for each OCT. In a typical case, the configuration of $\alpha = 0.1$ is sufficient to describe the potential noise [5]. Here we set it to 0.5 to show the denoising ability of the DNN. The epoch number is set as 1000. Figure 5 depicts the relationship between the loss

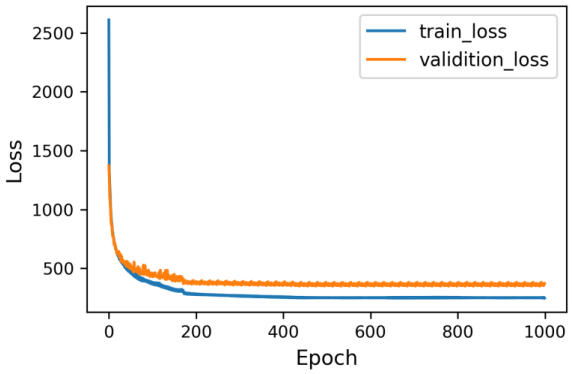

Fig. 5. The relationship between the loss function and the epoch number.

function and the epoch number during the training procedure. The minimum of the validation loss value is 345.89 and the model associated with it is saved as the predict model (PM) to repair the CCT.

In order to investigate the feasibility of the proposal, four images from the MNIST database, which are not used to generate the training data, are chosen as the plaintexts of the DIBE. The corresponding OCTs are shown in Fig. 6(a), and the decrypted results of Fig. 6(a) are shown in Fig. 6(e). The CC values for these images in Fig. 6(e) all equal 1.0000, and this means that the plaintexts can be completely restored from the uncontaminated cipertext by use of MF-PRA. Suppose the ciphertexts are contaminated by the noise with $\alpha = 0.3$, the quality of them will obviously degrade (see Fig. 6(b)).

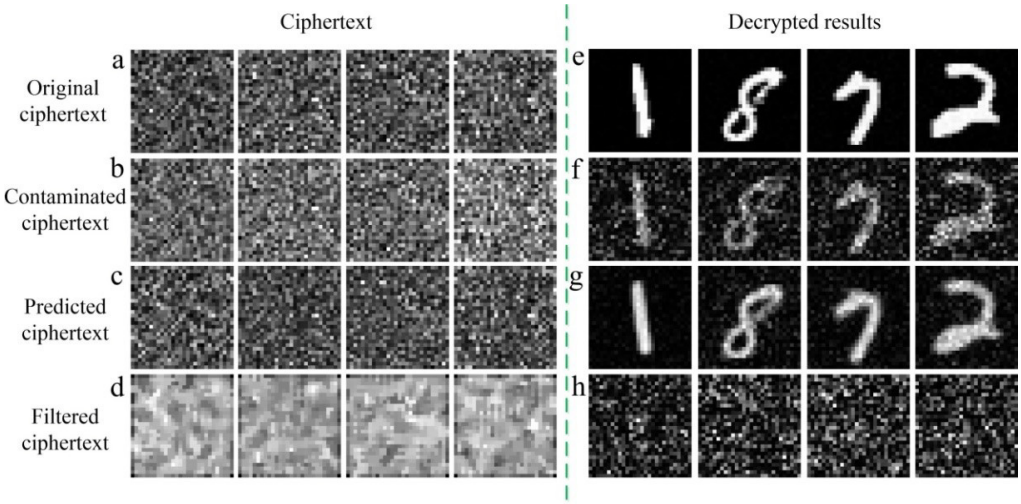

Fig. 6. Effectiveness of the proposal. (a) The original ciphertext; (b) the contaminated ciphertext; (c) the predicted ciphertext by the DNN; (d) the filtered ciphertext obtained with a 3×3 median filter; (e) the decrypted results of (a); (f) the decrypted results of (b); (g) the decrypted results of (c); (h) the decrypted results of (d).

In order to objectively evaluate the similarity between the original ciphertext (or plaintext) f and its degraded form f_{d}, the correlation coefficient (CC) between them is adopted as the metric:

$$\mathrm{CC} = \frac{E\left\{\left[f - E(f)\right]\left[f_{\mathrm{d}} - E(f_{\mathrm{d}})\right]\right\}}{\sqrt{E\left\{\left[f - E(f)\right]^2\right\} E\left\{\left[f_{\mathrm{d}} - E(f_{\mathrm{d}})\right]^2\right\}}} \tag{7}$$

where $E\{\cdot\}$ stands for the expectation value. The CC values for Fig. 6(b) are respectively 0.8232, 0.8649, 0.8621, 0.8790. The decrypted results of Fig. 6(b) are shown in Fig. 6(f). Figure 6(f) manifests that the quality of the decryption degrades severely, and only ambiguous profiles of the digits can be observed. This confirms the threat of noise attack to the DIBE scheme. Figure 6(c) shows the predicted ciphertexts by the DNN, and the CC values for them are respectively 0.9529, 0.9054, 0.9168, 0.9228, indicating that the DNN model can well repair the CCTs. The PCTs yield rather good decrypted images (see Fig. 6(g)), for which the CC values are 0.9746, 0.9276, 0.9511, and 0.9388. It is interesting to note that, although the CC values for the PCTs and the CCTs are close to each other, the decrypted results from the former are much better than those from the latter. This can be explained that the training procedure can enable the DNN to hold the substantive characters of the samples, and therefore the PCTs are inherently close to the OCTs. However, the CCTs only 'resemble' them. For comparison, we introduce a common denoising approach, referred to as median filtering, to improve the CCTs. The median-filtered ciphertexts (MCTs) are shown in Fig. 6(d), for which the CC values are 0.2430, 0.1650, 0.2262, 0.2302. These low-valued CCs indicate that the regular denoising method fails to suppress the noise in the CCTs, which are also noise-like images. Figure 6(h) is the decrypted images from the MCTs, which are totally unrecognized (CCs = 0.0431, 0.0712, 0.0362, 0.0434). It can be concluded from Fig. 6(h) that conventional methods are unsuitable for processing the noise in the CCT.

In order to further investigate the behavior of the proposal to noise attack, we increase the value of α from 0.1 to 0.8 with an interval of 0.1, and we obtain the corresponding decrypted results shown in Fig. 7. Figure 7(a) shows the relationship between the CC values of the decrypted results and α. As can be seen, the quality of the decrypted result of the CCT descends with the increase of α, while that of the PCT maintains a high quality over a wide range of α. Figures 7(b) and (c) show respectively the decrypted results that highly agree with the CC values. In Fig. 7(b), it is seen that slight pollution of the ciphertext causes negligible corruption on the decrypted image (first column). In addition, the digit '7' deteriorates with the increase of α and becomes thoroughly undistinguished when α exceeds 0.4. This indicates that the CCT will be unavailable if severe noise attack happens. In contrast, the decrypted images with our method (see Fig. 7(c)) can be well recognized even though α rises to 0.8.

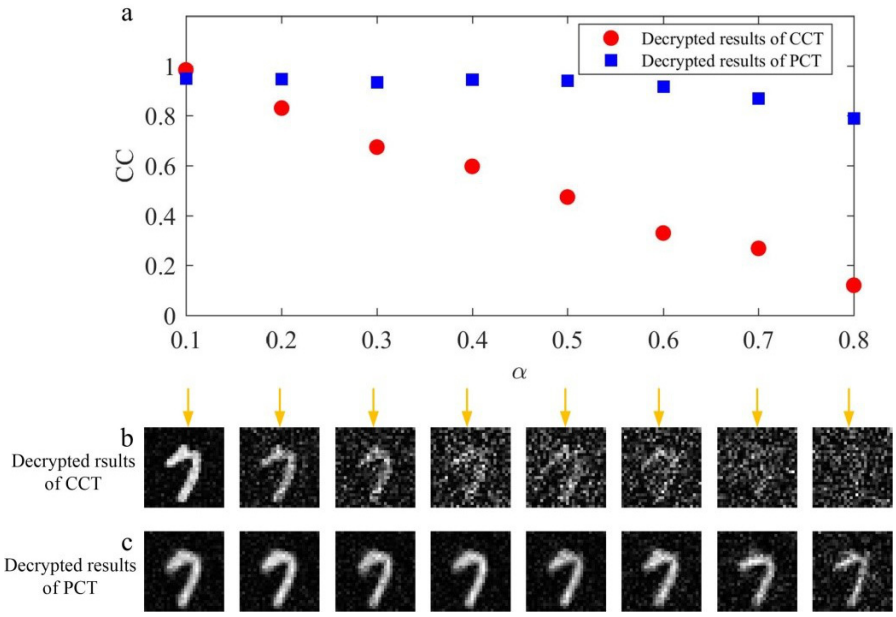

Fig. 7. The robustness of the proposal to different noise intensities. (a) The relationship between the CC values of the decrypted results and α; (b) the decrypted results of the CCTs; (c) the decrypted results obtained from the PCTs (our method).

In the above discussions, the ciphertext is supposed to be corrupted by the uniform noise; therefore, it is also significant to test the feasibility of the proposal when noises with different features, such as Gaussian noise and salt-and-pepper noise, are encountered. In the following simulations, the Gaussian noise has a zero mean and β variance, and the salt-and-pepper noise has a density of γ. In addition, both of the noises are directly added to the normalized ciphertext. Figure 8(a) shows the Gaussian-noise-polluted CCTs when β takes respectively the values of 0.01, 0.02, 0.03, and the CC values for them are 0.8568, 0.7248, 0.6554. The decrypted results of Fig. 8(a) are shown in Fig. 8(b), corresponding to CC values of 0.6514, 0.3586, 0.2693. Figure 8(b) indicates that the DIBE scheme is rather sensitive to Gaussian noise, as the decrypted result is totally unrecognizable in the case of $\beta = 0.02$. Figure 8(c) shows the PCTs corresponding to Fig. 8(a), for which the CC values are respectively 0.8929, 0.8817, 0.8808. The promoting in the CC values means that the DNN has successfully removed a certain amount of noise from the CCTs. The decrypted results of Fig. 8(c) are shown in Fig. 8(d), which have high CC values (CCs = 0.9230, 0.9190, 0.8850) and strongly resemble the primary images. Figure 8(e) shows the salt-and-pepper-noise-polluted CCTs when the values of γ are respectively 0.05, 0.10, 0.15, and the CC values for them are 0.7378, 0.5889, 0.4891, respectively. The decrypted results of Fig. 8(e) are all meaningless images (see Fig. 8(f)), for which the CC values are 0.4346, 0.1698, and 0.1247. Figure 8(g) shows the PCTs corresponding to Fig. 8(g), corresponding to the CC values

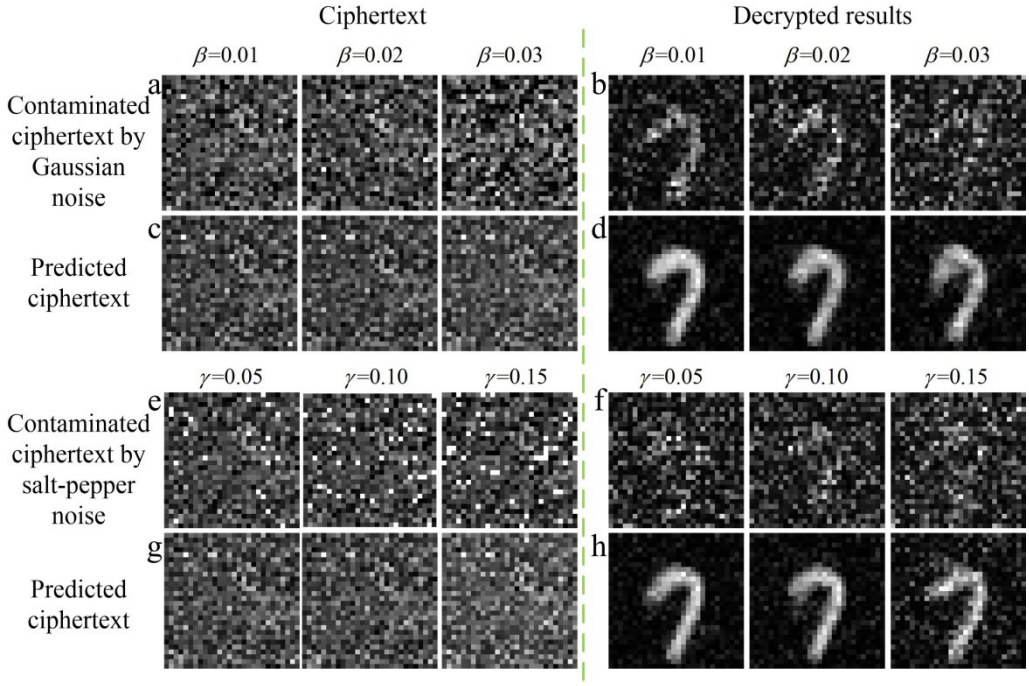

Fig. 8. Robustness of the proposal against to Gaussian noise and salt-and-pepper noise. (a) The Gaussian -noise-polluted CCTs with β = 0.01, 0.02, 0.03. (b) the decrypted results of (a); (c) The PCTs of (a) by the DNN; (d) the decrypted results of (c); (e) the salt-and-pepper-noise-polluted CCTs; (f) the decrypted results of (e); (g) The PCTs of (e) by the DNN; (h) the decrypted results of (g).

of 0.8852, 0.8590, 0.8499. The CC values manifest that our method results in substantially improvement in the quality of the ciphertext. The recovered plaintexts from Fig. 8(g) can be well recognized, as shown in Fig. 8(h). It can be learned from Fig. 8 that the proposal can effectively eliminate the common noises, regardless of their features. As a result, the proposal reinforces the robustness of DIBE against noise attack.

Additionally, it is interesting to test the DNN when the CCTs with different features, such as those generated by the images of the fashion-MNIST dataset, are fed into it. To do this, a set of four images from the fashion-MNIST dataset (see Fig. 9(a)) are used as the plaintexts. The ciphertexts are also polluted by the manner of Eq. (3), and α takes the value of 0.3. The corresponding CCTs are shown in Fig. 9(b). The PCTs given by the previous DNN model are shown in Fig. 9(c), for which the CC values are 0.5288, 0.5118, 0.6416, 0.7408, respectively. The low values of the CCs manifest that the DNN makes incorrect predictions of the CCTs, and the corresponding restored plaintexts (see Fig. 9(d), CCs = 0.3430, 0.2327, 0.6335, 0.7070) further support this judgement. Figures 9(c) and (d) show that the DNN is inapplicable for those CCTs with different character from the training set. This is because the applicability of a DNN model depends strongly on the training examples [21]. In other words, the CCTs to be denoised must resemble those that have been adopted for training in character. Ac-

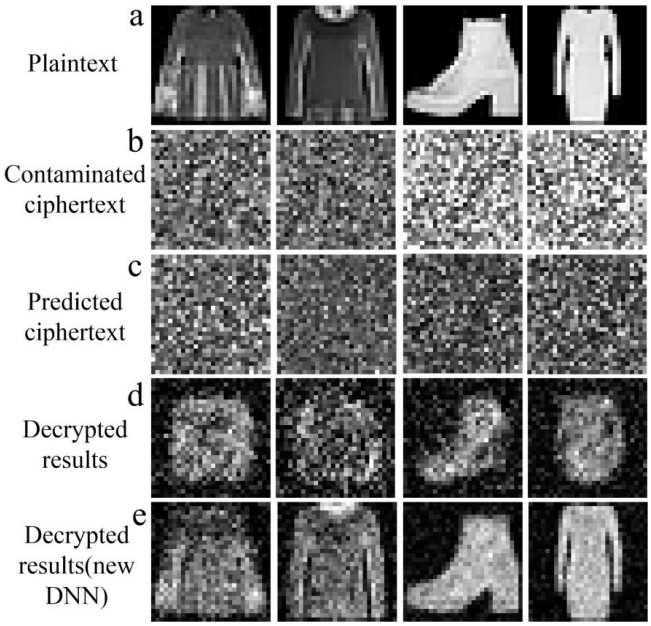

Fig. 9. The test of the generalization of the proposal. (a) The four images from the fashion-MNIST dataset; (b) the corresponding CCTs; (c) the PCTs of previous DNN trained with the MNIST dataset; (d) the corresponding restored images; (e) the restored images by using a new DNN trained with the fashion-MNIST dataset.

cordingly, the plaintexts producing the present CCTs must have the counterpart of them in those producing the training set. To confirm this, we retrain the DNN with the OCT-CCT pairs generated by the fashion-MNIST dataset and obtain a new DNN model. We repair the CCTs (see Fig. 9(b)) with this new DNN and obtain the corresponding PCTs. The finally decrypted results are shown in Fig. 9(e), for which the CC values are respectively 0.7537, 0.7957, 0.9563 and 0.9649. It is seen that the plaintexts have been well restored. Therefore, in order to extend the generalization of the proposal, the training set should be made as diverse as possible.

In real applications, our proposal is supposed to work under such a scenario: the information sender is in charge of generating the OCT-CCT pairs, performing the encryption and training the DNN, while the information receiver collects the ciphertext, secret keys and the DNN model. In other words, our proposal is totally the same as a common optical cryptosystem except the ciphertext denoising procedure. Meanwhile, since the DNN does not act as the secret key, it can be transferred from the sender to the receiver on a public channel.

4. Conclusions

In summary, we have presented a deep-learning-based approach to cope with the noise attack faced by optical cryptosystems. We take the DIBE scheme as an example to il-

lustrate our method. For decryption, the CCTs are first denoised by a well-trained DNN; thereafter, the obtained PCTs are decrypted with MF-PRA. The proposal ensures a high quality retrieval of the plaintext as it is able to effectively suppress the noise degrading the ciphertext. In particular, although the DNN is obtained under the assumption that the ciphertext is polluted by uniform noise, it exhibits excellent applicability for Gaussian noise and salt-and-pepper noise. Moreover, to enhance the applicability of the proposal, the dataset fed into the DNN should be as diverse as possible. In addition, the proposal indicates that a DNN can perceive and suppress the noise existing in a noise -like image (*i.e*. the ciphertext), and this is beyond the ability of the traditional methods (*e.g.* filtering). In this sense, our method offers new insight to the power of DNN in processing highly ill-posed problems in information optics.

Acknowledgements
This work is supported by the National Natural Science Foundation of China (NSFC) (Grant No. 61505091) and the Scientific Research Foundation of Nanyang Normal University (Grant No. 2024ZX031).

Author contributions
Conceptualization: Shibang Ma, Yi Qin; Funding acquisition: Yi Qin; Methodology: Yi Qin; Project administration: Yi Qin; Software: Shibang Ma; Validation: Qiong Gong; Writing – original draft: Qiong Gong and Hongjuan Wang; Writing – review and editing: Yi Qin.

References

[1] ALFALOU A., BROSSEAU C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009: 589-636. https://doi.org/10.1364/AOP.1.000589

[2] JAVIDI B., CARNICER A., YAMAGUCHI M., NOMURA T., PÉREZ-CABRÉ E., MILLÁN M.S., NISHCHAL N.K., TORROBA R., BARRERA J.F., HE W., PENG X., STERN A., RIVENSON Y., ALFALOU A., BROSSEAU C., GUO C., SHERIDAN J.T., SITU G., NARUSE M., MATSUMOTO T., JUVELLS I., TAJAHUERCE E., LANCIS J., CHEN W., CHEN X., PINKSE P.W.H., MOSK A.P., MARKMAN A., *Roadmap on optical security*, Journal of Optics **18**(8), 2016: 083001. https://doi.org/10.1088/2040-8978/18/8/083001

[3] SUI L., ZHANG X., HUANG C., TIAN A., ASUNDI A.K., *Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms*, Optics and Lasers in Engineering **113**, 2019: 29-37. https://doi.org/10.1016/j.optlaseng.2018.10.002

[4] SUI L., XIN M., TIAN A., *Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain*, Optics Letters **38**(11), 2013: 1996-1998. https://doi.org/10.1364/OL.38.001996

[5] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767

[6] CHEN W., CHEN X., SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010: 3817-3819. https://doi.org/10.1364/OL.35.003817

[7] QIN Y., GONG Q., WANG Z., *Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme*, Optics Express **22**(18), 2014: 21790-21799. https://doi.org/10.1364/OE.22.021790

[8] LI T., SHI Y., *Security risk of diffractive-imaging-based optical cryptosystem*, Optics Express **23**(16), 2015: 21384-21391. https://doi.org/10.1364/OE.23.021384

[9] BARRERA J.F., MIRA A., TORROBA R., *Optical encryption and QR codes: Secure and noise-free information retrieval*, Optics Express **21**(5), 2013: 5373-5378. https://doi.org/10.1364/OE.21.005373

[10] Goudail F, Bollaro F, Javidi B, Réfrégier P., *Influence of a perturbation in a double phase-encoding system*, Journal of the Optical Society of America A **15**(10), 1998: 2629-2638. https://doi.org/10.1364/JOSAA.15.002629

[11] Chen W., Chen X., Anand A., Javidi B., *Optical encryption using multiple intensity samplings in the axial domain*, Journal of the Optical Society of America A **30**(5), 2013: 806-812. https://doi.org/10.1364/JOSAA.30.000806

[12] Qin Y., Wang Z., Gong Q., *Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern*, Applied Optics **53**(19), 2014: 4094-4099. https://doi.org/10.1364/AO.53.004094

[13] Zea A.V., Barrera J.F., Torroba R., *Customized data container for improved performance in optical cryptosystems*, Journal of Optics **18**(12), 2016: 125702. https://doi.org/10.1088/2040-8978/18/12/125702

[14] Zhao S., Wang L., Liang W., Cheng W., Gong L., *High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique*, Optics Communications **353**, 2015: 90-95. https://doi.org/10.1016/j.optcom.2015.04.063

[15] LeCun Y., Bengio Y., Hinton G., *Deep learning*, Nature **521**, 2015: 436-444. https://doi.org/10.1038/nature14539

[16] Sinha A., Lee J., Li S., Barbastathis G., *Lensless computational imaging through deep learning*, Optica **4**(9), 2017: 1117-1125. https://doi.org/10.1364/OPTICA.4.001117

[17] Wu G., Nowotny T., Zhang Y., Yu H., Li D., *Artificial neural network approaches for fluorescence lifetime imaging techniques*, Optics Letters **41**(11), 2016: 2561-2564. https://doi.org/10.1364/OL.41.002561

[18] Lyu M., Wang W., Wang H., Wang H.C., Li G., Chen N., Situ G., *Deep-learning-based ghost imaging*, Scientific Reports **7**, 2017: 17865. https://doi.org/10.1038/s41598-017-18171-7

[19] Lina Zhou, Yin Xiao, Wen Chen, *Vulnerability to machine learning attacks of optical encryption based on diffractive imaging*, Optics and Lasers in Engineering **125**, 2020: 105858. https://doi.org/10.1016/j.optlaseng.2019.105858

[20] Hai H., Pan S., Liao M., Lu D., He W., Peng X., *Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning*, Optics Express **27**(15), 2019: 21204-21213. https://doi.org/10.1364/OE.27.021204

[21] Heaton J., *Artificial Intelligence for Humans: Deep Learning and Neural Networks and Deep Learning*, Vol. 3. Heaton Research Inc., St. Louis 2015: 190-198.

Received March 25, 2024
in revised form June 5, 2024