Opto-Electronic Advances

Supplementary information

2021, Vol. 4, No. 5

DOI: 10.29026/oea.2021.200016

Deep-learning-based ciphertext-only attack on optical double random phase encryption

Meihua Liao[1], Shanshan Zheng[2,3], Shuixin Pan[1], Dajiang Lu[1], Wenqi He[1], Guohai Situ[2,3,4]* and Xiang Peng[1]*

[1]College of Physics and Optoelectronic Engineering, Shenzhen University, Shenzhen 518060, China; [2]Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai, 201800, China; [3]Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing 100049, China; [4]Hangzhou Institute for Advanced Study, University of Chinese Academy of Sciences, Hangzhou, China.

*Correspondence: GH Situ, E-mail: ghsitu@siom.ac.cn; X Peng, E-mail: xpeng@szu.edu.cn

This file includes:

Supplementary information for this paper is available at https://doi.org/10.29026/oea.2021.200016

This document provides supplementary information to "Deep-learning-based ciphertext-only attack on optical double random phase encryption". We provide more data on the comparison with the other neural network (NN)-based method, the correlation coefficient (CC) under various levels of cropping and noise, as well as the test results of de-autocorrelation DNN without zero-padding.

Section 1: Comparison of neural network models

Seciotn 1.1: De-noising neural network

To select an appropriate neural network model for the task of de-noising, we trained two widely utilized neural network models (DCNN[1] and U-net[2]) and compared them with the same conditions. Figs. S1(b) and S1(c) show some of the outputs of DCNN and U-net, respectively. We calculated the CC values between the 1000 outputs of two models and the corresponding ground-truth images. The averaged CC values of DCNN and U-net are 0.942 and 0.937 respectively, while the training time of them are around 5 minutes and 11 minutes respectively. Therefore, DCNN is the better one for its shorter training time and good enough de-noising performance.

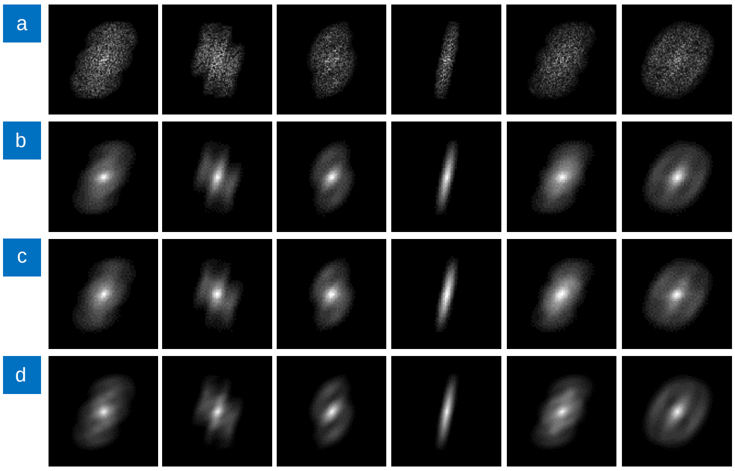

Fig. S1 | Comparison of de-noising neural network models. (**a**) The autocorrelations of ciphertexts. (**b**) Outputs of DCNN. (**c**) Outputs of U-net. (**d**) The autocorrelations of ground-truth plaintext images.

Seciotn 1.2: De-correlation neural network

We also trained two models of DCNN and U-net to perform the task of de-correlation. Both models were trained with the same amount of training dataset and follow the same training procedures. Figs. S2(b) and S2(c) show some of the

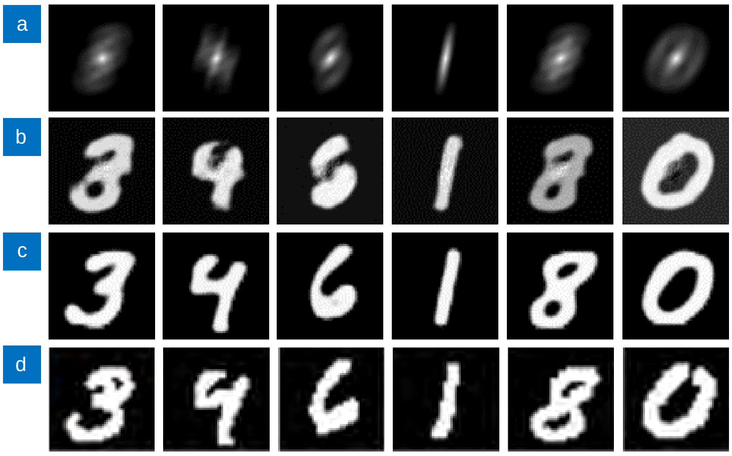

Fig. S2 | Comparison of de-correlation neural network models. (**a**) The autocorrelations of plaintext images. (**b**) Outputs of DCNN. (**c**) Outputs of U-net. (**d**) The ground-truth plaintext images.

outputs from DCNN and U-net, respectively. The averaged CC values (1000 test images in total) of DCNN and U-net are 0.823 and 0.931, respectively. Therefore, U-net can offer a better solution than DCNN to the de-correlation problem.

Section 2: Robustness tests against cropping and noise

We provide more data on robustness tests against cropping and two types of common noise (Gaussian noise and salt & pepper noise). We use the ciphertext under various levels of cropping and noise to perform our COA method, and the test results are shown in Fig. S3. The red points denote the measured CC values between the output images and the ground-truth plaintexts, the blue line represents the fitting trend.

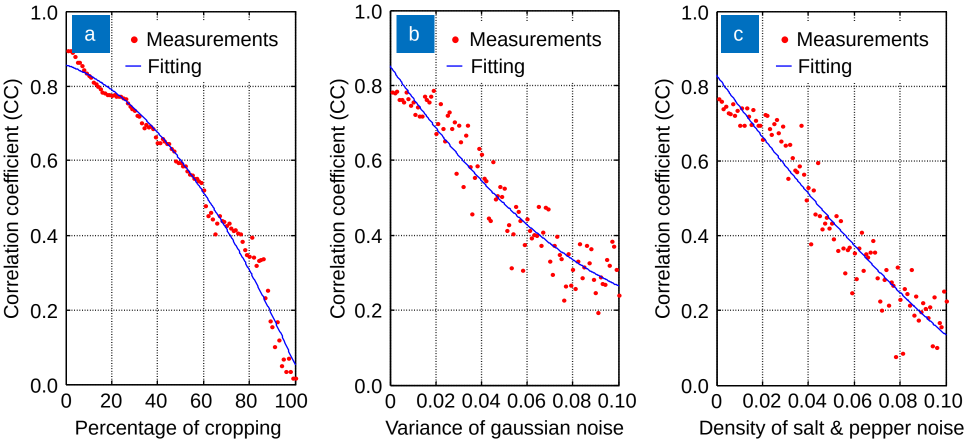

Fig. S3 | Robustness tests of the proposed COA method. (**a**) CC values under various percentages of cropping. (**b**) CC values under different variances of Gaussian noise. (**c**) CC values under different densities of salt & pepper noise.

Section 3: Test results of the de-correlation DNN without zero-padding

In order to validate the performance of the de-correlation DNN, we perform the test without zero-padding of images. During the training process, we use the autocorrelation function without zero-padding as the input of the de-correlation NN model and the test results are presented in Fig. S4.

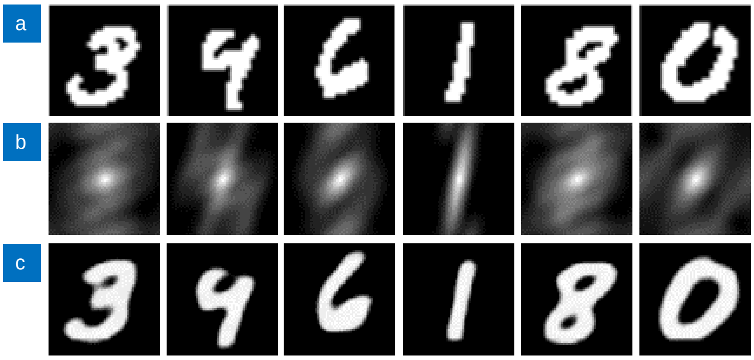

Fig. S4 | Test results of the de-correlation DNN without zero-padding. (**a**) The original images from the MNIST dataset. (**b**) The calculated autocorrelations without zero-padding. (**c**) The retrieved images from the trained de-correlation DNN.

References

1. Zhang K, Zuo WM, Chen YJ, Meng DY, Zhang L. Beyond a Gaussian denoiser: residual learning of deep CNN for image denoising. *IEEE Trans Image Process* **26**, 3142–3155 (2017).
2. Ronneberger O, Fischer P, Brox T. U-net: convolutional networks for biomedical image segmentation. In *Proceedings of the 18th International Conference on Medical Image Computing and Computer-Assisted Intervention* 234–241 (Springer, 2015).