https://doi.org/10.1016/j.optlaseng.2019.105858

Vulnerability to machine learning attacks of optical encryption based on diffractive imaging

Lina Zhou[1], Yin Xiao[1], Wen Chen[1,2,*]

[1]Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
[2]The Hong Kong Polytechnic University Shenzhen Research Institute,
Shenzhen 518057, China

*Email: owen.chen@polyu.edu.hk

Abstract

In this paper, we experimentally demonstrate for the first time to our knowledge that optical encryption based on diffractive imaging is vulnerable to the attacks using learning methods. Using machine learning attack, an opponent is capable to retrieve unknown plaintexts from the given ciphertexts. The proposed method adopts end-to-end learning to extract a superior mapping relationship between the ciphertexts and the plaintexts. Without a direct retrieval or estimate of optical encryption keys, an unauthorized user can extract unknown plaintexts from the given ciphertexts by using the trained learning models. Simulations and optical experimental results demonstrate that the proposed learning method is feasible and effective to analyze the vulnerability of optical encryption schemes. The universality of the trained learning model is also illustrated, and it is verified that the machine learning model trained by using a database is robust to be used for attacking different databases. Compared with conventional cryptanalytic methods, the proposed machine learning attacks can retrieve unknown plaintexts from the given ciphertexts using the trained learning models without a direct usage of various different optical encryption keys, which provides a different strategy for the cryptanalysis of optical encryption systems. @ Elsevier, 2019.

Keywords: Machine learning; vulnerability detection; experimental demonstration; diffractive imaging

1. Introduction

The intention to securely store or transmit data has stimulated the emergence of information security and spawned a myriad of research work to explore encryption systems [1–3]. With the rapid development of optical information processing, optical techniques have provided new methods and apparatuses for securing information. Prevalence of optical techniques used for the encryption can be ascribed to their unique advantages, e.g., intrinsic parallelism and multidimensional capabilities [4–11]. The seminal work of Refregier and Javidi [11], i.e., double random phase encoding (DRPE), was presented to encode an image to unrecognized speckle and has drawn a vast amount of attention to applying the scheme in many fields [12–22]. There are also many variations of the DRPE scheme to further develop this approach. The optical encryption has been implemented in many different domains, e.g., Fresnel transform domain [15], fractional Fourier transform domain [16], Gyrator transform domain [21] and canonical transform domain [22]. Reasons for the explosion of interest of DRPE architecture could be due to its high feasibility and high flexibility. Besides the advances of DRPE scheme, studies on other optical encryption techniques, e.g., ghost imaging, diffractive imaging and interference [5,12], have also been carried out. In comparison with interference-based optical encryption, diffractive-imaging-based optical encryption [5] uses a single wave-propagation path. Until now, optical encryption techniques have unveiled their potentials in many aspects, e.g., data communications, identification, and data storage.

Despite the great capability of optical encryption techniques, how to refrain from the unauthorized use remains a huge challenge. The majority of research of optical encryption to date still focuses on promoting the development of optical cryptography. Nowadays, there is also a growing awareness of the need to carry out the cryptanalysis of optical encryption schemes. A pioneering work reported by Carnicer et al. used chosen-ciphertext attack to prove the vulnerability of DRPE system [23]. Meanwhile, chosen-plaintext attack was also proven to be effective [24]. Later, Peng et al. [25] verified that optical encryption cannot withstand the known-plaintext attack. Liao et al. [26] utilized the ciphertext-only attack (COA) to retrieve plaintext from the ciphertext by using phase retrieval algorithms. Another study based on the COA method proposed a hybrid iterative phase retrieval algorithm to extract the plaintext [27]. In addition, a potential security risk has also been analyzed by Li and Shi [6]. In the previous studies the attempts have been made to make assumptions of the plaintext using many preconditions, and conventional cryptanalytic methods always focused on retrieving or estimating various different optical encryption keys. Hence, it is still an unexplored field or a demand for the cryptanalysis to extract unknown plaintexts from the given ciphertexts without a direct retrieval of various different optical encryption keys.

In this paper, we experimentally demonstrate for the first time to our knowledge that machine learning is feasible and effective to implement the attacks to diffractive-imaging-based optical encryption scheme without a direct retrieval of various optical encryption keys. Vulnerability of optical encryption based on diffractive imaging is analyzed here. Recently, machine learning methods receive the growing interest, since they can discover the representations of the given data without additional information [28]. Owing to its striking characteristics, machine learning method is a promising alternative to extracting unknown plaintexts from the given ciphertexts without any prerequisite.

2. Principles

Figure 1 shows an optical encryption setup based on diffractive imaging using a single optical path in the Fresnel domain. The optical encryption procedure is briefly described as follows: The first random mask $M_1(x,y)$ is placed right behind and bonded with a plaintext $f(x,y)$ to be encrypted. Then, it propagates through the second random mask $M_2(k,l)$ described by

$$\varphi(k,l) = \{\mathrm{FrT}_{d_1,\lambda}[f(x,y)M_1(x,y)]\}M_2(k,l), \tag{1}$$

where FrT represents free-space wave propagation in the Fresnel domain, d_1 denotes axial distance between the first random mask and the second random mask, and λ denotes the wavelength. The free-space wave propagation with axial distance of d_2 is further carried out, and then ciphertext $\mathrm{I}(\xi,\eta)$ recorded at the CCD plane can be described by

$$\mathrm{I}(\xi,\eta) = |\mathrm{FrT}_{d_2,\lambda}(\{\mathrm{FrT}_{d_1,\lambda}[f(x,y)M_1(x,y)]\}M_2(k,l))|^2. \tag{2}$$

In the diffractive-imaging-based optical encryption system, the decryption process is usually conducted by using iterative retrieval algorithms [5,6]. Although those phase retrieval algorithms are feasible to extract the plaintexts from the ciphertexts, they have a prerequisite of knowledge about accurate security keys, e.g., wavelength, axial distances and random masks. Otherwise, it is difficult to implement those iterative retrieval algorithms. Here, machine learning attacks are proposed and designed to resolve the inspiring task in the cryptanalysis without a need of direct retrieval of various optical encryption keys. We found that optical encryption scheme based on diffractive imaging can be attacked by employing machine learning without a need of the direct retrieval of various optical encryption keys.

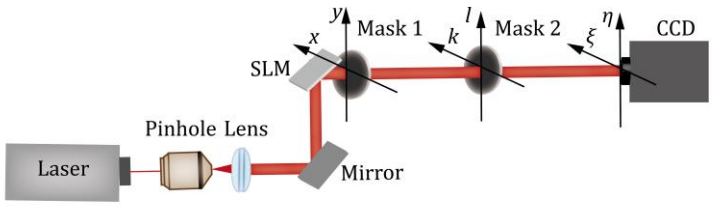

Fig. 1. An experimental setup for optical encryption based on diffractive imaging. SLM: spatial light modulator; CCD: charge-coupled device.

Inspired by the extensive penetration of machine learning methods into many application disciplines [29–32], we explore how the attack using machine learning becomes a threat to diffractive-imaging-based optical encryption without the direct retrieval of geometrical parameters and random masks. Figure 2 shows flow charts for the attacks to diffractive-imaging-based optical encryption system using a learning architecture. A certain number of plaintexts are sent to optical cryptographic system, and the same number of optically encoded images (i.e., ciphertexts) is obtained correspondingly. Then, the pairs of the ciphertexts and plaintexts are sent to a learning structure respectively as the inputs and outputs as shown in Fig. 2(a). After the training, the learning model is capable to make predictions of unknown plaintexts from the given ciphertexts. Finally, the trained learning model can be used to retrieve the plaintexts as shown in Fig. 2(b). The attack to diffractive-imaging-based optical encryption system can be implemented by utilizing the trained machine learning model.

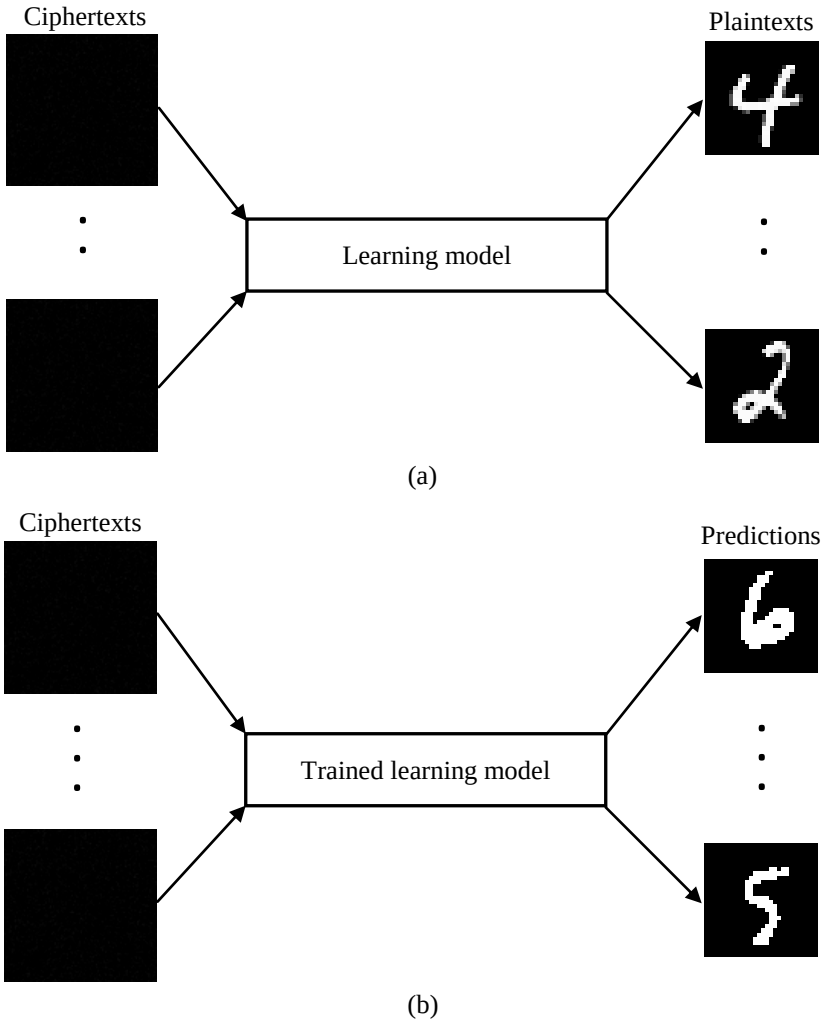

Fig. 2. Flow charts for the attack to diffractive-imaging-based optical encryption using a learning architecture. (a) Training phase: pairs of ciphertexts and plaintexts obtained from optical encryption scheme based on diffractive imaging are fed to the inputs and outputs of a learning model, respectively. (b) Testing phase: using the trained learning model to predict unknown plaintexts from the given ciphertexts.

2.1 The designed CNN architecture

A He-Ne laser with wavelength of 632.8nm is collimated, and illuminates onto a spatial light modulator (SLM) as shown in Fig. 1. The SLM functions as an object (i.e., plaintext). The plaintexts are respectively from MNIST database which consists of grayscale handwritten-digit images [33] and from the Fashion MNIST database which consists of grayscale fashion images [34]. From each database, 5000 grayscale images are used here. The modulated laser beam sequentially propagates through mask 1 and mask 2, and mask 1 is bonded with the SLM. Axial propagation distances of d_1 and d_2 are 5.2 cm and 5.4 cm, respectively. During optical encryption, the ciphertexts are sequentially recorded by using a CCD. The next step is to send the ciphertext-plaintext pairs to the designed learning model. Here, an end-to-end

learning model is built. Architecture of the learning model is shown in Fig. 3(a). The inputs fed to the learning model are the ciphertexts. To lower computational load of the proposed learning method, the inputs are preprocessed by resizing from 512×512 to 100×100. Then, the resized input convolves with 20 kernels (size of 5×5) forming the first convolution layer (size of $96\times96\times20$). Next, the first convolution layer is followed by the pooling processing forming the first pooling layer (size of $48\times48\times20$). Objective of the convolution procedure is to extract effective characterizations from the input (i.e., ciphertexts), and the pooling procedure is used to reduce parameters of the network. Subsequently, the first pooling layer is further processed by convolution and pooling to form the second pooling layer (size of $22\times22\times20$). After that, the second pooling layer is reshaped and fully connected to the corresponding plaintext. The constructed learning model is designed based on convolutional neural network (CNN) [31], which has 7 hidden layers, 20 neurons per convolution layer and 20 neurons per pooling layer. Weights and biases are initialized randomly, and the activation function used in each convolution layer is sigmoid function. The loss function used to measure the difference between the predicted plaintext and original one is mean squared error, and the optimization function applied to update the weights and biases is stochastic gradient descent. The learning rate is set to 10^{-6}, and the training epoch is 5. The learning model is executed by using Matlab 2009 on a PC with Intel Core i7@8GHz, 64GB RAM and Nvidia GTX1080Ti. In this study, 4800 images from each database are used as the plaintexts to be optically encoded for each training phase, and parameters in the designed learning model are optimized correspondingly. Another 200 ciphertexts are recorded and applied for the testing phase, and the unknown plaintexts can be further retrieved from the given ciphertexts by using the trained learning model as typically illustrated in Fig. 3(b). The total time used to train a learning model using each database is about 4 hours, and the trained model is ready to make predictions of unknown plaintexts from the given ciphertexts in real time.

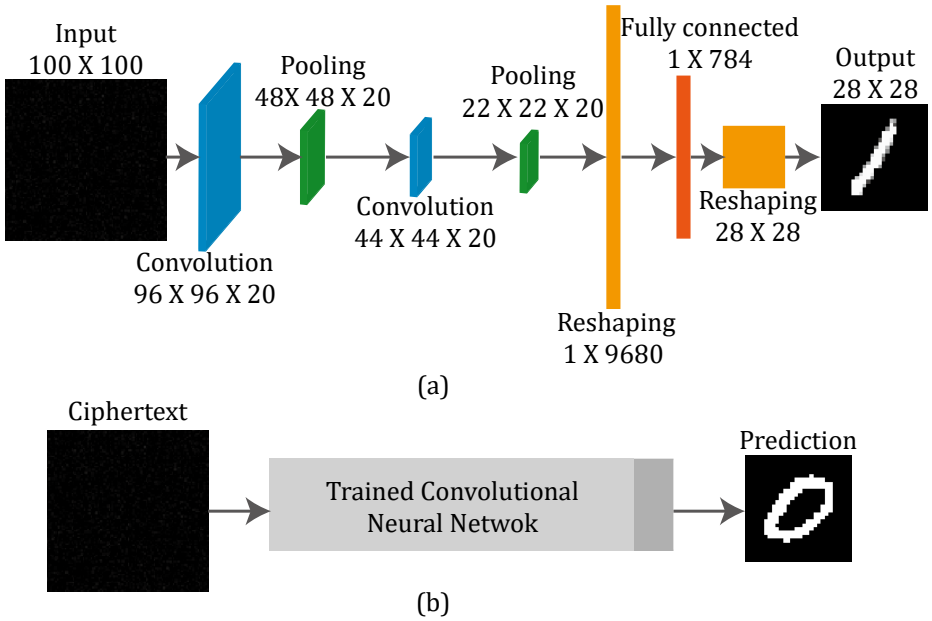

Fig. 3. The proposed learning architecture for attacking optical cryptography based on diffractive imaging. (a) A schematic of the designed CNN infrastructure, and (b) a typical example: retrieval of unknown plaintext from the given ciphertext by using the trained learning model.

2.2 Data processing

The 4800 pairs of ciphertexts and plaintexts are used in the training phase, and another 200 ciphertexts are obtained for the testing. The input, i.e., ciphertext, is preprocessed by subtracting its mean value to remove the DC component (i.e., direct current component). The loss function used in the designed CNN model is mean squared error (MSE), and optimization function applied to update weights and bias of the network to minimize the MSE value is stochastic gradient descent (SGD) [35]. The MSE is described by

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2, \tag{3}$$

where n denotes pixel number of the predicted plaintext, Y_i represents pixel value of the original plaintext (i.e., ground truth), $\hat{Y}_i$ represents pixel value of the predicted plaintext, and '$\sum$' denotes the summation. The updating rule of the SGD can be described by

$$w = w - v, \tag{4}$$

$$v = mv + \alpha\nabla J(w,b); \tag{5}$$

$$b = b - v, \tag{6}$$

$$v = mv + \alpha\nabla J(w,b), \tag{7}$$

where velocity v is 0 at the initial stage and then updated by using momentum m (i.e., -9.5×10^{-4}) and a learning rate α. The initial value of learning rate is 10^{-5}, and it is accelerated by doubling every 200 inputs sent to the network. The symbols w and b respectively denote the weight and bias to be updated by using the continuously-updated velocity. The symbol $\nabla J(w,b)$ represents the gradient at w and b. The weight is initialized to be 10^{-3} at the first convolve layer, then to be 10^{3} at the second convolve layer, and to be 10^{-3} at the fully-connected layer. The bias is initiated to 0. The MSE values become smaller approaching the optimal value after 5 epochs of iterations. The designed CNN model is trained and costs 4 hours, and then the unknown plaintexts can be retrieved from the given ciphertexts in real time by using the trained learning model without the usage of various different optical encryption keys and various complex phase retrieval algorithms.

2.3 Simulations

Figure 4 shows simulation results about the retrieved plaintexts by using the trained learning model without a need of direct usage of various optical encryption keys. Several ciphertexts shown in Figs. 4(a), 4(c), 4(e), 4(g), 4(i) and 4(k) are used as typical examples for the testing, and are respectively sent to the trained learning models. Figures 4(b), 4(d), 4(f), 4(h), 4(j) and 4(l) show the retrieved plaintexts obtained by using the trained machine learning attacks without access to optical encryption keys respectively corresponding to Figs. 4(a), 4(c), 4(e), 4(g), 4(i) and 4(k), which are advantageous over conventional cryptanalytic methods. To evaluate performance of the proposed method, peak signal-to-noise ratio (PSNR) is used to describe quality of the retrieved plaintexts. PSNR values of the images in Figs. 4(b), 4(d), 4(f), 4(h), 4(j) and 4(l) are 33.17 dB, 28.45 dB, 27.61 dB, 26.52 dB, 34.96 dB and 23.40 dB, respectively. The quality is high, and it is feasible for the attackers to fully recognize the plaintexts. For the objects comprised by Chinese characters, double digits and English letters which are different from the database used in the training phase, the pre-trained learning model can also retrieve the plaintexts from their correspondingly encoded ciphertexts. Typical ciphertexts of these objects are respectively shown in Figs. 4(m), 4(o) and 4(q). Figures 4(n),

4(p) and 4(r) show the retrieved plaintexts obtained from the machine learning model trained by the MNIST database, and PSNR values of the recovered images are 23.24 dB, 32.78 dB and 34.96 dB, respectively. These results effectively illustrate that the diffractive-imaging-based optical encryption system is vulnerable to the proposed machine learning attacks without a direct retrieval or estimate of optical encryption keys. It provides a different research perspective for conducting the cryptanalysis of optical encryption schemes. Moreover, it is also illustrated that the proposed attacks are also applicable for attacking the different databases using the trained learning model. There are two main reasons for the availability and universality of the trained learning model. The first is that the trained learning model has learned the mapping relationship between the input ciphertexts and output plaintexts. The second is that the ciphertexts encrypted by the diffractive-imaging-based cryptosystem share some similarities and correlations. Hence, the machine learning model trained by a database can be re-used for the attacking to retrieve the plaintexts which are from different databases. From the results aforementioned, it is also verified that the trained machine learning model is robust for attacking different databases.

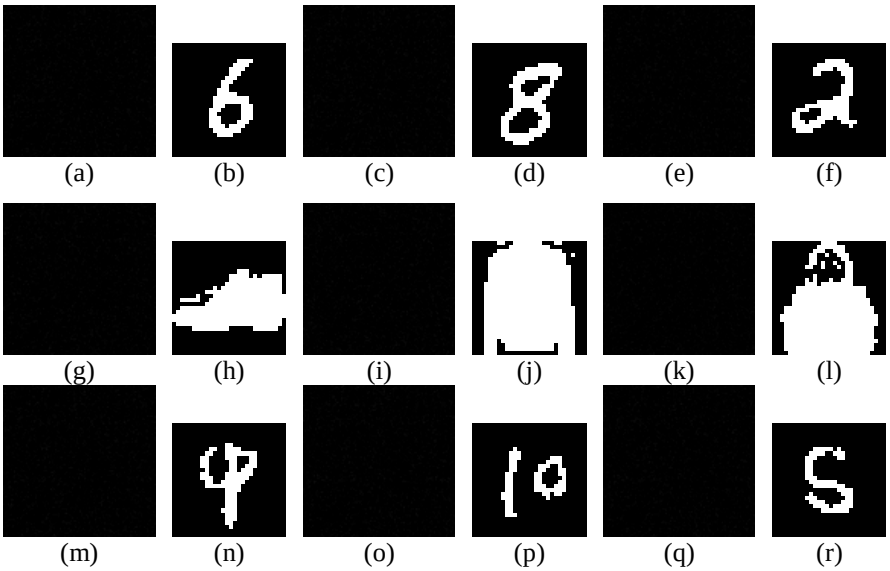

Fig. 4. Simulation results of the proposed machine learning attacks to the diffractive-imaging-based optical encryption. Testing phase: (a), (c), (e), (g), (i), (k), (m), (o) and (q) ciphertexts obtained by using optical encoding system (further sent to the corresponding trained learning models). (b), (d), (f), (h), (j) and (l) The retrieved plaintexts obtained respectively by using their corresponding trained learning models respectively corresponding to (a), (c), (e), (g), (i) and (k). (n), (p) and (r) The retrieved plaintexts (i.e., from different databases) obtained by using the learning model trained by the MNIST database.

3. Experimental demonstration and discussions

Experimental validation of machine learning attacks to optical encryption system based on diffractive imaging has also been implemented. A series of plaintexts are sequentially used and embedded into the SLM in the optical encryption setup, and their corresponding ciphertexts are sequentially recorded by using a CCD. It is worth noting that the recorded patterns are of 1280×1024 pixels in this study. To reduce computational load of the designed

learning model, the recorded patterns are resized to 100×100. These experimentally-obtained ciphertext-plaintext pairs are fed to the proposed learning model for the training. After that, a trained learning model is constructed. Typical examples for testing the trained learning method are shown in Fig. 5. We can observe that the experimentally obtained ciphertexts in Figs. 5(a), 5(c), 5(e), 5(g), 5(i) and 5(k) are successfully decoded respectively by using their corresponding trained learning models, and the retrieved plaintexts are respectively shown in Figs. 5(b), 5(d), 5(f), 5(h), 5(j) and 5(l). PSNR values of the retrieved plaintexts are 26.08 dB, 23.85 dB, 28.03 dB, 18.06 dB, 25.85 dB and 21.63 dB, respectively. Different from conventional cryptanalytic methods, without the direct retrieval of various optical encryption keys the proposed machine learning attacks are feasible to extract unknown plaintexts from the given ciphertexts. Hence, it is also demonstrated that the proposed machine learning attacks are effective as verified by the simulations and optical experiments.

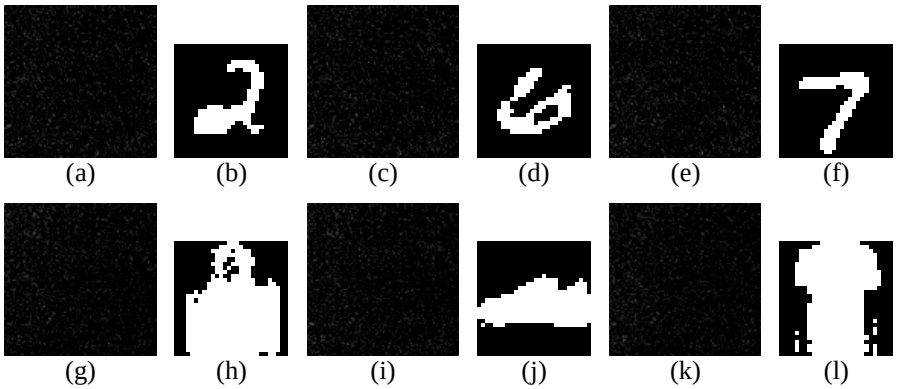

Fig. 5. Experimental results of the proposed machine learning attacks to the diffractive-imaging-based optical encryption. Testing phase: (a), (c), (e), (g), (i) and (k) ciphertexts obtained by using optical encoding system. (b), (d), (f), (h), (j) and (l) The retrieved plaintexts obtained respectively by using their corresponding trained learning models respectively corresponding to (a), (c), (e), (g), (i) and (k).

In addition, we further experimentally investigate the proposed machine learning attacks to the diffractive-imaging-based optical encryption system with multiple cascaded random masks. Optical setup with triple random masks used in the diffractive-imaging-based optical encryption system is studied as a typical example and shown in Fig. 6. Axial propagation distances of d_1, d_2 and d_3 are 5.2 cm, 5.4 cm, and 5.0 cm, respectively. Typical experimental results are shown in Fig. 7. Figures 7(b), 7(d), 7(f), 7(h), 7(j) and 7(l) show the retrieved plaintexts respectively from the given ciphertexts in Figs. 7(a), 7(c), 7(e), 7(g), 7(i) and 7(k) by using their corresponding trained learning models. The PSNR values are 29.46 dB, 24.47 dB, 24.65 dB, 19.30 dB, 17.97 dB and 22.18 dB, respectively. The proposed machine learning attacks are feasible and applicable, when multiple cascaded random masks are used in the diffractive-imaging-based optical encryption. Although it has been illustrated [5,10] that more random masks and geometric parameters render the higher security, the unauthorized users can still make use of the proposed machine learning attacks to extract unknown plaintexts from the given ciphertexts without a need of direct retrieval of various optical encryption keys. In essence, the proposed learning-based attacking method seems to estimate transfer function of the diffractive-imaging-based optical encryption systems.

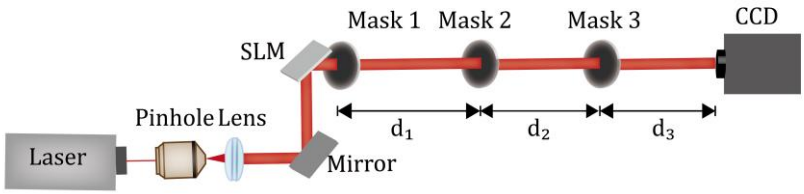

Fig. 6. Optical experimental setup for diffractive-imaging-based optical encryption using multiple cascaded random masks.

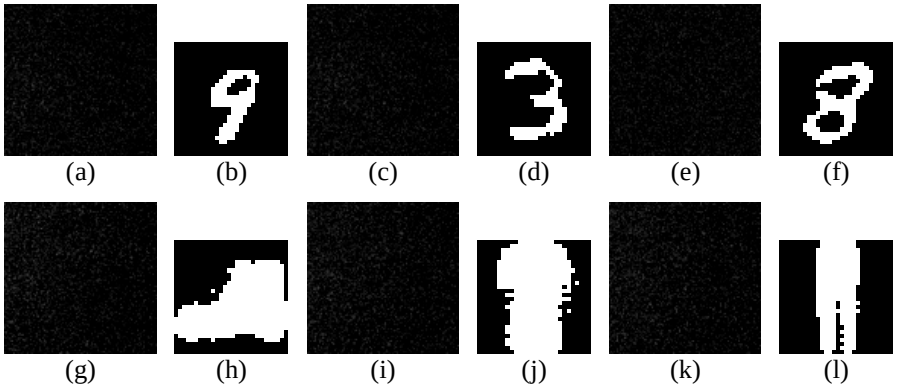

Fig. 7. Experimental results of the proposed machine learning attacks to diffractive-imaging-based optical encryption using multiple cascaded random masks. Testing phase: (a), (c), (e), (g), (i) and (k) ciphertexts obtained by using optical encoding system. (b), (d), (f), (h), (j) and (l) The retrieved plaintexts predicted respectively by using their corresponding trained learning models respectively corresponding to (a), (c), (e), (g), (i) and (k).

4. Conclusions

In this paper, we have experimentally demonstrated that optical encryption based on diffractive imaging is vulnerable to machine learning attacks. Optical encryption based on diffractive imaging is analyzed here, which cannot withstand the proposed machine learning attacks. The trained learning model can extract unknown plaintexts from the given ciphertexts in real time without the direct retrieval or estimate of various different optical encryption keys. The simulations and optical experiments have been conducted to verify feasibility and effectiveness of the proposed method. Moreover, the proposed machine learning method for attacking is also applied to successfully analyze the vulnerability of diffractive-imaging-based optical encryption systems with multiple cascaded random masks. A generalized learning model trained by using the data composed of various conditions (e.g., different axial distances, different random masks and different types of plaintexts) can be established which features extraordinary convenience and applicability to retrieve unknown plaintexts from the given ciphertexts. The proposed machine learning attacks would urge the further investigation of optical encryption schemes to enhance their security, and can also hold the promise for further developments of the cryptanalysis of optical encryption.

Acknowledgements

This work was financially supported by National Natural Science Foundation of China (NSFC) (61605165), The Hong Kong Polytechnic University (G-YBVU), and Hong Kong Research Grants Council (25201416).

References

[1] Javidi B. Securing information with optical technologies. Phys. Today 1997; 50: 27–32. https://doi.org/10.1063/1.881692.

[2] Petitcolas F A, Anderson R J, Kuhn M G. Information hiding-a survey. Proc. IEEE 1999; 87: 1062–1078. https://doi.org/10.1109/5.771065.

[3] Alfalou A, Brosseau C. Optical image compression and encryption methods. Adv. Opt. Photon. 2009; 1: 589–636. https://doi.org/10.1364/AOP.1.000589.

[4] Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt. Lett. 1999; 24: 762–764. https://doi.org/10.1364/OL.24.000762.

[5] Chen W, Chen X, Sheppard C J. Optical image encryption based on diffractive imaging. Opt. Lett. 2010; 35: 3817–3819. https://doi.org/10.1364/OL.35.003817.

[6] Li T, Shi Y. Security risk of diffractive-imaging-based optical cryptosystem. Opt. express 2015; 23: 21384–21391. https://doi.org/10.1364/OE.23.021384.

[7] Zhang Y, Zheng C H, Tanno N. Optical encryption based on iterative fractional Fourier transform. Opt. Commun. 2002; 202: 277–285. https://doi.org/10.1016/S0030-4018(02)01113-6.

[8] Barrera J F, Mira A, Torroba R. Optical encryption and QR codes: secure and noise-free information retrieval. Opt. Express 2013; 21: 5373–5378. https://doi.org/10.1364/OE.21.005373.

[9] Chen W, Chen X. Optical cryptography topology based on a three-dimensional particle-like distribution and diffractive imaging. Opt. express 2011; 19: 9008-9019. https://doi.org/10.1364/OE.19.009008.

[10] Chen W, Javidi B, Chen X. Advances in optical security systems. Adv. Opt. Photon. 2014; 6: 120–155. https://doi.org/10.1364/AOP.6.000120.

[11] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 1995; 20: 767–769. https://doi.org/10.1364/OL.20.000767.

[12] Zhang Y, Wang B. Optical image encryption based on interference. Opt. Lett. 2008; 33: 2443–2445. https://doi.org/10.1364/OL.33.002443.

[13] Matoba O, Javidi B. Encrypted optical storage with wavelength-key and random phase codes. Appl. Opt. 1999; 38: 6785–6790. https://doi.org/10.1364/AO.38.006785.

[14] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett. 2000; 25: 887–889. https://doi.org/10.1364/OL.25.000887.

[15] Situ G, Zhang J. Double random-phase encoding in the Fresnel domain. Opt. Lett. 2004; 29: 1584–1586. https://doi.org/10.1364/OL.29.001584.

[16] Unnikrishnan G, Singh K. Double random fractional Fourier domain encoding for optical security. Opt. Eng. 2000; 39: 2853–2859. https://doi.org/10.1117/1.1313498.

[17] Tao R, Xin Y, Wang Y. Double image encryption based on random phase encoding in the fractional Fourier domain. Opt. Express 2007; 15: 16067–16079. https://doi.org/10.1364/OE.15.016067.

[18] Liu Z, Liu S. Double image encryption based on iterative fractional Fourier transform. Opt. Commun. 2007; 275: 324–329. https://doi.org/10.1016/j.optcom.2007.03.039.

[19] Chen L, Zhao D. Optical image encryption with Hartley transforms. Opt. Lett. 2006; 31: 3438–3440. https://doi.org/10.1364/OL.31.003438.

[20] Liu Z, Li Q, Dai J, Sun X, Liu S, Ahmad M A. A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains. Opt. Commun. 2009; 282: 1536–1540. https://doi.org/10.1016/j.optcom.2009.01.002.

[21] Abuturab M R. Color image security system based on discrete Hartley transform in gyrator transform domain. Opt. Lasers Eng. 2013; 51: 317–324. https://doi.org/10.1016/j.optlaseng.2012.09.008.

[22] Singh N, Sinha A. Chaos based multiple image encryption using multiple canonical transforms. Opt. Laser Technol. 2010; 42: 724–731. https://doi.org/10.1016/j.optlastec.2009.11.016.

[23] Carnicer A, Montes-Usategui M, Arcos S, Juvells I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. 2005; 30: 1644–1646. https://doi.org/10.1364/OL.30.001644.

[24] Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt. Lett. 2006; 31: 3261–3263. https://doi.org/10.1364/OL.31.003261.

[25] Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. 2006; 31: 1044–1046. https://doi.org/10.1364/OL.31.001044.

[26] Liao M, He W, Lu D, Peng X. Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium. Sci. Rep. 2017; 7: 41789. https://doi.org/ 10.1038/srep41789.

[27] Liu X, Wu J, He W, Liao M, Zhang C, Peng X. Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding. Opt. Express 2015; 23: 18955–18968. https://doi.org/10.1364/OE.23.018955.

[28] LeCun Y, Bengio Y, Hinton G. Deep learning. Nature 2015; 521: 436–444. https://doi.org/10.1038/nature14539.

[29] Zhang K, Zuo W, Gu S, Zhang L. Learning deep CNN denoiser prior for image restoration. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2017; 3929–3938.

[30] Nasrabadi N M. Pattern recognition and machine learning. J. Electron. Imaging 2007; 16: 049901.

[31] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems 2012; 1097–1105.

[32] Chen X D. Computational Methods for Electromagnetic Inverse Scattering. 1st ed. Singapore: John Wiley & Sons; 2018.

[33] LeCun Y, Bottou L, Bengio Y, Haffner P. Gradient-based learning applied to document recognition. Proc. IEEE 1998; 86: 2278–2324. https://doi.org/10.1109/5.726791.

[34] Xiao H, Rasul K, Vollgraf R. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms. arXiv preprint arXiv:1708.07747 (2017).

[35] Sutskever I, Martens J, Dahl G E, Hinton G E. On the importance of initialization and momentum in deep learning. Proceedings of the 30th International Conference on Machine Learning, PMLR 2013; 28: 1139–1147.