PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

Speckle-based optical cryptosystem for face recognition

Qi Zhao, Huanhao Li, Zhipeng Yu, Puxiang Lai

Qi Zhao, Huanhao Li, Zhipeng Yu, Puxiang Lai, "Speckle-based optical cryptosystem for face recognition," Proc. SPIE 12438, AI and Optical Data Sciences IV, 1243810 (15 March 2023); doi: 10.1117/12.2645932

SPIE.

Event: SPIE OPTO, 2023, San Francisco, California, United States

Speckle-based Optical Cryptosystem for Face Recognition

Qi Zhao, Huanhao Li, Zhipeng Yu, and Puxiang Lai*
The Hong Kong Polytechnic University, Hong Kong, China

ABSTRACT

Face recognition has been widely implemented in public places for security purposes. However, face photos are sensitive biometric data, and their privacy is a common concern, which often needs to be protected via cryptosystems. Popular software-based cryptosystems have limitations on short secret key lengths, posing a significant threat when facing high performance quantum computing. Recently, in order to achieve higher level security, hardware-based optical cryptosystems have been investigated. However, due to the complexity of optical system designs, it is difficult to integrate the extensively studied optical double random phase encryption into current face recognition systems. Speckle-based cryptosystems, on the contrary, affords high-level safety with high adaptivity, high speed, and low cost, using simpler optical setups. In this study, a speckle-based optical cryptosystem for face recognition is proposed, and encrypted face recognition is experimentally demonstrated. During encryption, a scattering ground glass is utilized as the only physical secret key with 17.2 gigabit length, so as to encrypt face images via random optical speckles at light speed. During decryption, a specially designed neural network is pre-trained to reconstruct face images from speckles with high fidelity, allowing for up to 98% accuracy in the subsequent face recognition process. Apart from face recognition, the proposed speckle-based optical cryptosystem can also be transferred to other high-security cryptosystems due to its high security, high adaptivity, fast speed, and low cost.

Keyword: deep learning, optical encryption, optical cryptosystem, speckle

INTRODUCTION

In modern society, public safety is becoming more and more important, and face recognition applications have been widely set up for safeguarding [1]. Note that human face is a personal identification and people can seldom modify their appearance. Thus, storing human face data in face recognition applications should be highly confidential. Once face recognition data leaks out, hackers can utilize these data to attack key sectors, including bank accounts [2]. Therefore, effective cryptosystems to protect face image data are critical for privacy protection [3].

To protect data privacy, various cryptosystems have been put forward, including software-based and hardware-based cryptosystems. As for software-based cryptosystems, their limited secret key length might be sufficient against conventional attacks by modern computers. But these cryptosystems are vulnerable to attacks from the rapidly evolving quantum computers, which have 10^8 times the computing power of the conventional ones [4]. In comparison, hardware-based cryptosystems can attain much longer secret key lengths and are hence far safer than software-based cryptosystems. Amongst the

AI and Optical Data Sciences IV, edited by Bahram Jalali, Ken-ichi Kitayama,
Proc. of SPIE Vol. 12438, 1243810 · © 2023 SPIE
0277-786X · doi: 10.1117/12.2645932

proposed hardware-based cryptosystems, optical cryptosystems are of extensive interest due to development of optical computing and computational imaging [5-6]. What's more, due to their high performance, optical cryptosystems can lead to breakthroughs in cryptosystems, such as high-speed, high security, low cost, etc. [7]. As one type of optical cryptosystems, speckle-based cryptosystems have been proposed, where optical speckles are utilized as ciphertext to encrypt plaintext. Compared with double-random-phase encryption, speckle-based cryptosystems are much easier to deploy due to simpler optical setups. In a fully developed optical scattering regime, original plaintext images are optically scrambled, and cameras can capture optical speckles as ciphertexts, which are featured by randomly distributed optical spots. The nonsensical and difficult-to-decipher random representations of the speckles indicate high-level security with high-speed encryption. Recently, various applications of speckle-based cryptosystems have been demonstrated in encrypting simple structural images (e.g., characters, garments, animals, etc.) [8-13]. However, complex tasks, such as encrypted face recognition, have rarely been explored using speckle-based optical cryptosystems. The main challenge here is to decrypt images from rapidly changing optical speckles and to recognize faces from the decrypted images. Moreover, decryption with high fidelity in key features and detailed structures is essential to achieve high accuracy in face recognition.

METHODS

In this work, we propose a cryptosystem that encrypts face photos with optical speckles and decrypts optical speckles with a deep neural network, and the decrypted images are then used for face recognition. The concept, as illustrated in Figure 1, can be divided into three stages: first, as for encryption, face images are optically scrambled into speckles by a scattering medium, in order to protect face image data during transmission and storage; then, a neural network is trained to decrypt optical speckles to get face images with high fidelity; last, the decrypted images are compared with the known face images and recognized. In the proposed cryptosystem, face images are encrypted into seemingly random speckles, and it is nearly impossible to decrypt speckles without the scattering medium as the physical key. Moreover, only speckles but no face images are stored in the database to protect private information.

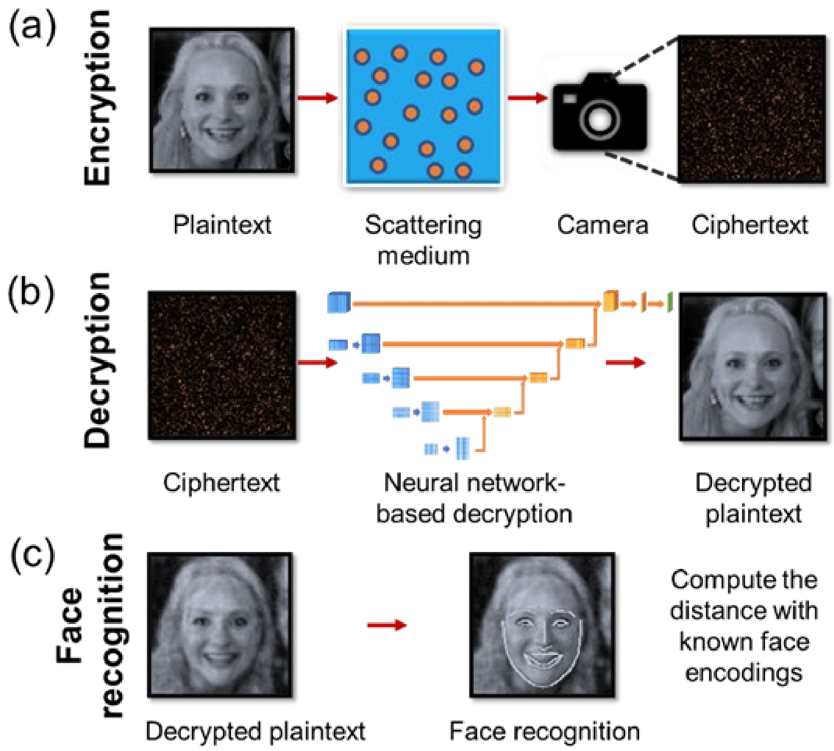

Figure 1. The flowchart of the speckle-based optical cryptosystem for face recognition. (a) Encryption: face images (plaintext) are loaded on a spatial light modulator (SLM) to generate the corresponding speckles (ciphertext) from a scattering medium (physical secret key). (b) Decryption: a neural network is pre-trained to decrypt speckle patterns (ciphertext), and the decrypted face images are then used for face recognition. (c) Face recognition: if the distance between the face encoding of decrypted images and known face encodings is less than a pre-set threshold, the face recognition result is "Match" (the same person), otherwise it is "Mismatch" (different people).

Note: The plaintext image in Figure 1a is from Lawrence Lessig at Second Home London, by Innotech Summit, Copyright 2015, Flickr (https://www.flickr.com/photos/115363358@N03/18260388752/). Reproduced under terms of the CC-BY 2.0 license. The original image is cropped and converted to gray-scale.

REFERENCE

[1] A. W. Senior, S. Pankanti, Handbook of Face Recognition, Springer London, London 2011.

[2] K. Chavis, Policing: A Journal of Policy and Practice 2021, 15 (1), 425.

[3] H. Berghel, Comp. 2017,50 (12), 72.

[4] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, H. Neven, Phys. Rev. X 2016, 6 (3), 031015.

[5] S. Liu, C. Guo, J. T. Sheridan, Opt. Laser Technol. 2014, 57, 327.

[6] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, A. Markman, J. Opt. (Bristol, U. K.) 2016,18 (8), 083001.

[7] A. Zhao, N. Jiang, S. Liu, Y. Zhang, K. Qiu, J. Lightwave Technol. 2021, 39 (8), 2288.

[8] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. 2000, 25 (12), 887.

[9] W. Chen, B. Javidi, X. Chen, Adv. Opt. Photon. 2014, 6 (2), 120.

[10] L. Zhou, Y. Xiao, W. Chen, Opt. Lett. 2020, 45 (18), 5279.

[11] Y. Liu, P. Yu, Y. Li, L. Gong, OSA Continuum 2020, 3 (11), 2968.

[12] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, J. Lancis, Opt. Lett. 2010,35 (14), 2391.

[13] G. Qu, W. Yang, Q. Song, Y. Liu, C.-W. Qiu, J. Han, D.-P. Tsai, S. Xiao, Nat. Commun. 2020, 11 (1), 5484.