The following publication Peifeng Wang, Yin Xiao, and Wen Chen "A simple authentication-based optical security method", Proc. SPIE 11205, Seventh International Conference on Optical and Photonic Engineering (icOPEN 2019), 1120519 (16 October 2019) is available at https://doi.org/10.1117/12.2542146.

A Simple Authentication-Based Optical Security Method

Peifeng Wang[a,b], Yin Xiao[a,b], and Wen Chen[a,b,*]
[a]Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
[b]The Hong Kong Polytechnic University Shenzhen Research Institute,
Shenzhen 518057, China
*Email: owen.chen@polyu.edu.hk

ABSTRACT

Optical security has attracted much attention in recent years, and much research work has been done to establish various optical security systems. It has been further found that when optical authentication is introduced into optical encryption systems, system security can be enhanced. Hence, authentication-based optical security has been widely studied. However, much previous work needs to use relatively complicated optical setups or algorithms to establish authentication-based optical security systems. In this paper, a simple method is presented by using direct wave propagation to generate a compressed phase-only mask as ciphertext, and the input image is compressed before the encoding. Results and analyses demonstrate that the proposed method is feasible and effective for authentication-based optical security. It is expected that the method presented can provide a promising approach for effectively enriching authentication-based optical security area.

Keywords: Optical security, direct wave propagation, optical encryption, optical authentication.

1. INTRODUCTION

After double random phase encoding [1] was proposed, numerous optical setups have been designed to establish different optical encryption infrastructures. For instance, different transform domains and algorithms [1–10] have been studied and integrated into optical setups for securing information. Various optical imaging methods [1–10], such as digital holography and diffractive imaging, have been studied and applied to enrich optical security field. Many parameters, e.g., random phase-only mask, wavelength, propagation distance and polarization, have been flexibly designed and applied as security keys. However, it has been found that some optical security systems cannot withstand potential attacks, such as known-plaintext attack and chosen-ciphertext attack [11–13]. Recently, it has been illustrated [14–22] that optical authentication can be further applied into optical encryption systems to enhance the security. The decoded image can be verified by using nonlinear correlation without visually rendering clear information about the plaintext. The original data or images can be stored in a remote database, and only an interface is provided to implement the authentication. This approach could open up a new research perspective or provide a new insight for optical security. Some authentication-based optical security systems have been studied and demonstrated. For instance, phase retrieval algorithm [15] can be applied to generate sparse phase-only patterns as ciphertext for authentication-based optical security, and a small number of measurements or realizations can be used in ghost imaging [20] to recover noisy objects for authentication-based optical security. Flexible application of data compression (or sparsity) and a large number of optical setups provide a sufficient condition for establishing various effective authentication-based optical security systems. However, previous work needs to use relatively complicated optical setups or algorithms to establish authentication-based optical security systems.

In this paper, a simple method is presented for authentication-based optical security by using direct wave propagation to generate a compressed phase-only mask as ciphertext. An input image is first compressed before the encoding, and then direct wave propagation is used. Only phase-only component is reserved, and amplitude component is directly removed. The generated phase-only mask is further compressed as ciphertext. The encoding process needs to be implemented by using a digital way, and an optical or digital method can be flexibly used for the decoding and authentication in practical applications. Computational results and analyses demonstrate that the proposed method is feasible and effective for authentication-based optical security. It is expected that the method presented can provide a promising approach for effectively enriching authentication-based optical security area.

2. PRINCIPLES

Figure 1 shows a schematic setup for the proposed authentication-based optical security method. A plane wave can be generated for the illumination. The input image is first compressed before the encoding, and then back propagation from the input image plane to the mask plane is numerically carried out to generate a compressed phase-only mask as ciphertext. In this study, fractional Fourier transform (FrFT) [23] is used as a typical example to illustrate the proposed method, and other transform domains [1–10] can also be applied in practical applications. The encoding process is described by using the FrFT, and phase-only mask $M(x,y)$ is described by

$$M(x,y)=\frac{\mathrm{FrFT}_{-\alpha,-\alpha}\left[H(\xi,\eta)\right]}{\left|\mathrm{FrFT}_{-\alpha,-\alpha}\left[H(\xi,\eta)\right]\right|}, \tag{1}$$

where α denotes FrFT function order [23], (x,y) and (ξ,η) respectively represent coordinates of the phase-only mask plane and the input image plane, symbol $|\,|$ denotes a modulus operation, and $H(\xi,\eta)$ denotes a sparse input image.

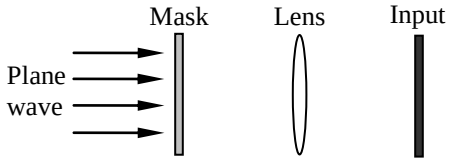


Figure 1. A schematic setup for the proposed method for the encoding.

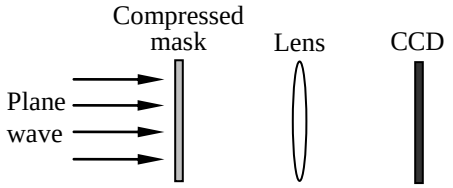


Figure 2. A schematic setup for the proposed method for optical decoding.

After phase-only mask *M* is obtained, the generated phase-only mask is further compressed as $M'(x,y)$ (i.e., acting as ciphertext). During the decoding the plane wave is used, and the input image plane is replaced by using a CCD camera as shown in Fig. 2. Hence, a decoded image can be correspondingly obtained by

$$D(\xi,\eta)=\left|\mathrm{FrFT}_{\alpha,\alpha}\left[M'(x,y)\right]\right|^2, \tag{2}$$

where $D(\xi,\eta)$ denotes a decoded image. The encoding process needs to be implemented by using a digital way, and an optical or digital method can be flexibly used for the decoding and authentication in practical applications.

In this study, data compression is applied, therefore the decoded image obtained by Eq. (2) cannot visually render clear information about original image. Nonlinear correlation is further implemented to generate correlation distribution between original image and the decoded image, which can be described by [14–22]

$$C(\xi,\eta)=\left|IFFT\left(\left|\left\{FFT\left[O(\xi,\eta)\right]\right\}\left\{FFT\left[D(\xi,\eta)\right]\right\}^*\right|^{\kappa}\frac{\left\{FFT\left[O(\xi,\eta)\right]\right\}\left\{FFT\left[D(\xi,\eta)\right]\right\}^*}{\left|\left\{FFT\left[O(\xi,\eta)\right]\right\}\left\{FFT\left[D(\xi,\eta)\right]\right\}^*\right|}\right)\right|^2, \tag{3}$$

where $C(\xi,\eta)$ denotes a correlation distribution, *FFT* and *IFFT* respectively denote 2-D Fourier transform and inverse 2-D Fourier transform, asterisk denotes complex conjugate, $O(\xi,\eta)$ represents original image stored in a database, and κ denotes the degree of nonlinearity strength (i.e., 0.30 used in this study). In nonlinear correlation algorithm, the judgment

to be made is that when only one sharp peak with low sidelobe is generated, the receiver could be confirmed as an authorized person who has correct security keys.

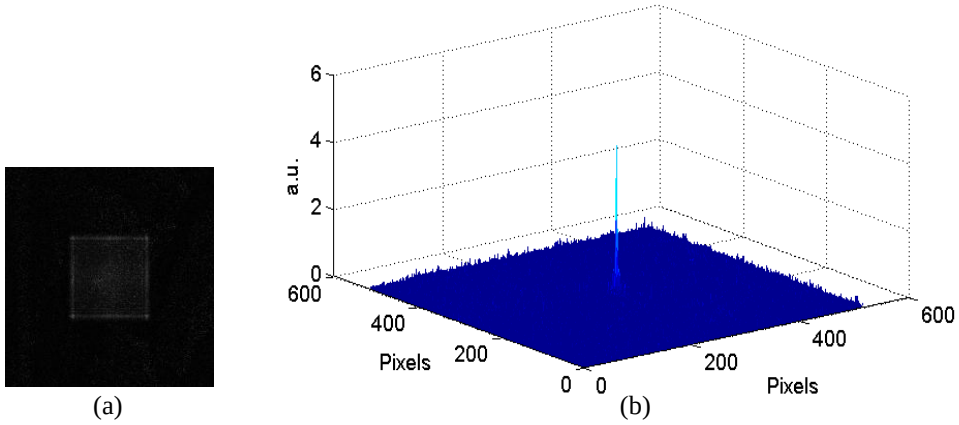
3. RESULTS AND DISCUSSION

Figure 1 shows a schematic setup for the proposed authentication-based optical security method, and numerical results are obtained to show its feasibility and effectiveness. The plane wave can be generated for the illumination during the encoding and decoding. The FrFT function order is set as 0.80, and different transform domains can be flexibly applied in practical applications. Figure 3(a) shows an input image (i.e., original image with size of 512x512 pixels), and only 7.0% pixels of the input image are randomly selected and reserved for the encoding. Using the proposed optical encoding method, a phase-only mask is correspondingly generated and shown in Fig. 3(b), and 80.0% pixels of the generated phase-only mask in Fig. 3(b) are randomly selected and reserved as ciphertext for the proposed method.

(a) (b)

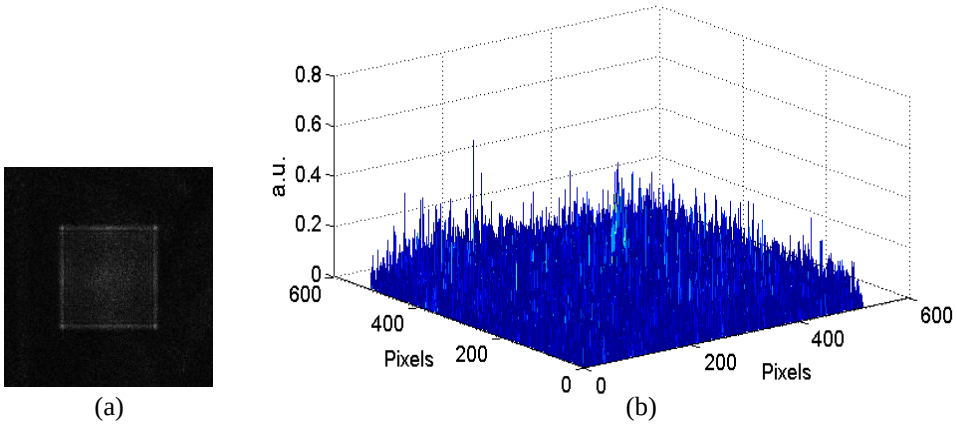
Figure 3. (a) An input image (i.e., original image, http://sipi.usc.edu/database/database.php?volume=misc), and (b) a generated phase-only mask.

During the decoding the plane wave can be used for the illumination, and the input image plane is replaced by using a CCD camera as shown in Fig. 2. Figure 4(a) shows a decoded image, when security keys are correctly applied. It can be seen in Fig. 4(a) that noisy distribution is generated, and information about original image cannot be clearly observed. In this study, data compression is applied, therefore the decoded image obtained by Eq. (2) cannot visually render clear information about the input image. Nonlinear correlation [14–22] is further implemented to generate correlation distribution between original image and the decoded image. Figure 4(b) shows a generated authentication distribution corresponding to that in Fig. 4(a). It can be seen in Fig. 4(b) that only one remarkable peak is obtained, which means the receiver has correct security keys. When FrFT function order α contains an error of 0.05 during the decoding, a decoded image and its corresponding authentication distribution are shown in Figs. 5(a) and 5(b), respectively. It can be seen in Fig. 5(b) that only noisy correlation distribution is obtained. It has been demonstrated that the proposed method is simple and feasible.



(a) (b)

Figure 4. (a) A decoded image obtained when security keys are correctly applied for the decoding, and (b) the corresponding authentication distribution.



(a) (b)

Figure 5. (a) A decoded image obtained when FrFT function order contains an error of 0.05 during the decoding, and (b) the corresponding authentication distribution.

4. CONCLUSION

In this paper, a simple method has been presented for authentication-based optical security by using direct wave propagation to generate a compressed phase-only mask as ciphertext. An input image is first compressed before the encoding, and then direct wave propagation is used. Only phase-only component is reserved, and amplitude component is directly removed. The generated phase-only mask is further compressed as ciphertext. The encoding process needs to be implemented by using a digital way, and an optical or digital method can be flexibly used for the decoding and authentication in practical applications. Numerical results and analyses have demonstrated that the proposed method is simple, feasible and effective for authentication-based optical security. It is expected that the method presented can provide a promising approach for effectively enriching authentication-based optical security area.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (NSFC) (Grant No. 61605165), the Hong Kong Research Grants Council Early Career Scheme under Grant No. 25201416, Shenzhen Science and Technology Innovation Commission through Basic Research Program (JCYJ20160531184426473), and The Hong Kong Polytechnic University (Fund Nos.: G-UAE2, 4-BCDY, G-YBVU, 4-ZZHM, 1-ZE5F).

REFERENCES

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767–769, (1995).

[2] Z. Liu, L. Xu, C. Lin and S. Liu, “Image encryption by encoding with a nonuniform optical beam in gyrator transform domains,” Appl. Opt. **49**, 5632–5637, (2010).

[3] H. E. Hwang, H. T. Chang and W. N. Lie, “Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain,” Opt. Lett. **34**, 3917–3919, (2009).

[4] W. Chen, B. Javidi and X. Chen, “Advances in optical security systems,” Adv. Opt. Photon. **6**, 120–155, (2014).

[5] W. Chen and X. Chen, “Interference-based optical image encryption using three-dimensional phase retrieval,” Appl. Opt. **51**, 6076–6083, (2012).

[6] Y. L. Xiao, X. Zhou, S. Yuan, Q. Liu and Y. C. Li, “Multiple-image optical encryption: an improved encoding approach,” Appl. Opt. **48**, 2686–2692, (2009).

[7] R. K. Wang, I. A. Watson and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng. **35**, 2464–2469, (1996).

[8] G. Situ and J. Zhang, "A cascaded iterative Fourier transform algorithm for optical security applications," Optik **114**, 473–477, (2003).

[9] H. E. Hwang, "Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain," Opt. Commun. **285**, 567–573, (2012).

[10] Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. **33**, 2443–2445, (2008).

[11] A. Carnicer, M. M. Usategui, S. Arcos and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**, 1644–1646, (2005).

[12] X. Peng, P. Zhang, H. Wei and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**, 1044–1046, (2006).

[13] X. Peng, H. Wei and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," Opt. Lett. **31**, 3261–3263, (2006).

[14] E. Pérez-Cabré, M. Cho and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22–24, (2011).

[15] W. Chen, X. Chen, A. Stern and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," IEEE Photon. J. **5**, 6900113, (2013).

[16] W. Chen, "3D Gerchberg-Saxton optical correlation," IEEE Photon. J. **10**, 7800409, (2018).

[17] W. Chen, "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," IEEE Photon. J. **8**, 6900209, (2016).

[18] W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL **110**, 44002, (2015).

[19] W. Chen and X. Chen, "Marked ghost imaging," Appl. Phys. Lett. **104**, 251109, (2014).

[20] W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett. **38**, 546–548, (2013).

[21] W. Chen, "Virtually optical information verification with a hierarchical structure," Opt. Eng. **57**, 010502, (2018).

[22] W. Chen, "Hierarchically optical double-image correlation using 3D phase retrieval algorithm in fractional Fourier transform domain," Opt. Commun. **427**, 374–381, (2018).

[23] H. M. Ozaktas, Z. Zalevsky and M. A. Kutay, The fractional Fourier transform with applications in optics and signal processing, Wiley, 2001.