Optical Encoding System using Sparse Pinhole Arrays for Optical Information Processing

Wen Chen[1,2]

[1]The Hong Kong Polytechnic University Shenzhen Research Institute,
Shenzhen 518057, China
[2]Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
Emails: owen.chen@polyu.edu.hk; chenwen327@gmail.com

Abstract—Optical security has attracted much attention nowadays, and relevant research has been widely conducted. Although optical encoding and decoding technique can be useful for securing information, its security is still a major concern in practical applications and more effort should be made to enhance system security. Recently, optical information authentication method has been developed and can be considered as a promising strategy to further enhance system security. The optical information authentication approaches are usually established based on optical encoding setups, and decoded images can be effectively verified without plaintext disclosure. It has also been found that high flexibility can be achieved in the optical information authentication system, and various optical imaging setups, such as phase retrieval, digital holography and computer-generated hologram, can be designed and applied in practice. To some extent, a new research perspective has been opened up for optical information security due to the development of optical information authentication strategy. It is expected that more optical information authentication systems can be established in the future. In this paper, one optical information processing method, i.e., for optical image authentication, is presented based on phase-truncated encoding system using sparse pinhole arrays. During optical encoding, phase-truncated strategy is employed, and sparse pinhole arrays are applied in spatial frequency domain and CCD plane, respectively. Since plaintext cannot be clearly observed during the decryption even using correct security keys, optical authentication method is further applied to verify the decrypted image. High security is achieved, and an effective security layer can be established for phase-truncated optical encoding system.

1. INTRODUCTION

Since double random phase encryption was developed [1], information security with optical means has attracted much attention [2–4]. A number of optical cryptosystems [5–13] have been developed. However, it is found that due to linear characteristics, some optical cryptosystems cannot withstand the attacks [14,15], such as known-plaintext attack. Recently, several advanced optical cryptosystems [16,17], such as phase-truncated optical encoding [17], have been developed for breaking the linear property. However, special attack and collision algorithms [18,19] might still be applicable to attack the cryptosystem. Hence, it is desirable that new strategies can be developed for phase-truncated optical cryptosystem to achieve the higher security.

In this paper, optical information authentication is presented based on phase-truncated encoding system using sparse pinhole arrays. During the encoding, phase-truncated strategy is employed, and sparse pinhole arrays are applied in spatial frequency domain and CCD plane, respectively. Since plaintext cannot be clearly observed during the decryption, optical authentication method is applied to verify the decrypted image. It will be illustrated that the higher security can be achieved.

2. PRINCIPLES

Figure 1 shows a schematic optical setup. The plane wave illuminates an input image, and two random phase-only masks M1 and M2 are used. Let $\exp[i\,\alpha(x,y)]$ and $\exp[i\beta(\mu,\nu)]$ denote phase-only masks M1 and M2 respectively located in the input image plane and spatial frequency domain, where $i=\sqrt{-1}$, and $\alpha(x,y)$ and $\beta(\mu,\nu)$ denote 2D maps randomly distributed in the range of $[0,\ 2\pi]$. In this study, sparse pinhole arrays S1 and S2 are placed just before phase-only mask M2 and CCD camera, respectively. Complex amplitude just before the pinhole array S1 can be described by

$$C(\mu,\nu)=\mathrm{FrFT}_{\gamma_1}\left\{k(x,y)\exp\left[i\,\alpha(x,y)\right]\right\}, \tag{1}$$

where $k(x,y)$ denotes an input image, and FrFT_{γ_1} denotes fractional Fourier transform (FrFT) [5,20] with function order of γ_1. Real amplitude and phase maps in the FrFT domain just before phase-only mask M2 can be extracted and respectively denoted as $A_c(\mu,\nu)$ and $P_c(\mu,\nu)$.

$$A_c(\mu,\nu)=\mathrm{abs}\left[C(\mu,\nu)S_1(\mu,\nu)\right], \tag{2}$$

$$P_c(\mu,\nu)=\arg\left[C(\mu,\nu)S_1(\mu,\nu)\right], \tag{3}$$

where $S_1(\mu,\nu)$ denotes sparse pinhole array S1, and abs and arg denote the extraction of amplitude and phase parts, respectively. In phase-truncated optical encoding system, phase part is truncated as decryption key, and only amplitude component is further encoded.

Subsequently, wave propagation between the FrFT domain and the CCD plane can be expressed as

$$O(\xi,\eta)=\mathrm{FrFT}_{\gamma_2}\left\{A_c(\mu,\nu)\exp\left[i\,\beta(\mu,\nu)\right]\right\}, \tag{4}$$

where γ_2 denotes FrFT function order. Similarly, real amplitude and phase maps in the CCD plane can be extracted and respectively denoted as $A_o(\xi,\eta)$ and $P_o(\xi,\eta)$.

$$A_o(\xi,\eta)=\mathrm{abs}\left[O(\xi,\eta)S_2(\xi,\eta)\right], \tag{5}$$

$$P_o(\xi,\eta)=\arg\left[O(\xi,\eta)S_2(\xi,\eta)\right], \tag{6}$$

where $S_2(\xi,\eta)$ denotes sparse pinhole array S2. Real amplitude $A_o(\xi,\eta)$ is used as ciphertext for the storage or transmission. Phase-only distributions $P_c(\mu,\nu)$ and $P_o(\xi,\eta)$ are generated as decryption keys, which are different from encryption keys (i.e., M1 and M2). Different from conventional cryptosystem [17], sparse pinhole arrays S1 and S2 are applied in the FrFT domain and CCD plane, respectively.

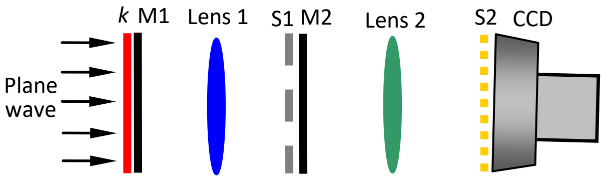


Figure 1: Schematic setup for the simulation: *k*, plaintext; M, phase-only mask; S, sparse pinhole array; CCD, charge-coupled device.

During optical decryption, a decrypted image can be retrieved by

$$\begin{aligned} k'(x,y)=\Big|\mathrm{FrFT}_{-\gamma_1}\Big\{&\Big(\Big|\mathrm{FrFT}_{-\gamma_2}\left\{A_o(\xi,\eta)\exp\left[i\,P_o(\xi,\eta)\right]\right\}\Big|\Big)\\ &\times\exp\left[i\,P_c(\mu,\nu)\right]\Big\}\Big|, \end{aligned} \tag{7}$$

where $k'(x,y)$ denotes a decrypted image, | | denotes modulus operation, and $\mathrm{FrFT}_{-\gamma_1}$ and $\mathrm{FrFT}_{-\gamma_2}$ denote inverse FrFT [5,20]. It can be seen in Eq. (7) that decryption keys $P_o(\xi,\eta)$ and $P_c(\mu,\nu)$ are applied, and pinhole arrays S1 and S2 are not required during the decryption. Evaluation parameters can be used to evaluate quality of decrypted images, and mean-square error (MSE) [21] is calculated in this study.

$$\mathrm{MSE}=\frac{1}{\mathrm{T}}\sum_x\sum_y\left[k(x,y)-k'(x,y)\right]^2, \tag{8}$$

where $x=1,2,3...$, $y=1,2,3...$, and T denotes the total image pixels.

Since sparse pinhole arrays S1 and S2 are used, the decrypted image does not visually render the plaintext. Optical correlation algorithm, such as nonlinear correlation [22–37], is further applied to authenticate the decrypted image, and optical authentication process can be described by

$$f_1(\mu,\nu)=\mathrm{FFT}\left[k(x,y)\right], \tag{9}$$

$$f_2(\mu,\nu)=\mathrm{FFT}\left[k'(x,y)\right], \tag{10}$$

$$N(x,y)=\left|\mathrm{IFT}\left[\left|f_1^*(\mu,\nu)f_2(\mu,\nu)\right|^{m-1}f_1^*(\mu,\nu)f_2(\mu,\nu)\right]\right|^2, \tag{11}$$

where $N(x,y)$ denotes nonlinear correlation output, *m* denotes strength of applied nonlinearity [22–37], asterisk denotes complex conjugate, and FFT and IFT respectively denote Fourier transform and inverse Fourier transform.

3. RESULTS

Numerical simulations are conducted to illustrate the validity in this paper. A collimated plane wave with wavelength of 630.0 nm is used during the encoding. The FrFT function orders γ_1 and γ_2 are 0.60 and 0.80, respectively. Figures 2(a) and 2(b) show phase-only masks M1 and M2, which are employed as encryption keys and are randomly distributed in the range of $[0, 2\pi]$. In this study, sparse pinhole arrays S1 and S2 shown in Figs. 2(c) and 2(d) are placed just before phase-only mask M2 and CCD camera, respectively. The insets in Figs. 2(c) and 2(d) show the enlarged parts, which clearly illustrate sparse pinholes. Each pinhole array S1 or S2 contains only 10.0% of 512×512 pixels, however position distributions of effect pixels (i.e., value of 1) are different in these two pinhole arrays. In practical applications, the number of sparse pinholes in each array can be flexibly designed to satisfy the encoding requirements, and the generated pinhole arrays may be embedded into amplitude-only spatial light modulator. During the encoding, pixel size of 4.65 μm and pixel number of 512×512 are used to record the ciphertext. An input image in Fig. 2(e) is used as plaintext to illustrate the feasibility and effectiveness.

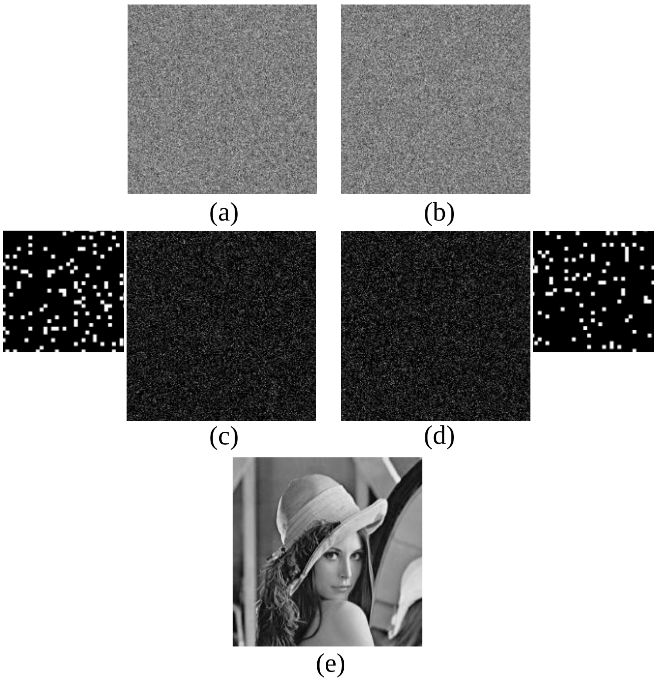
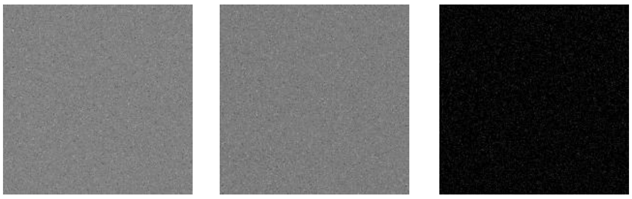


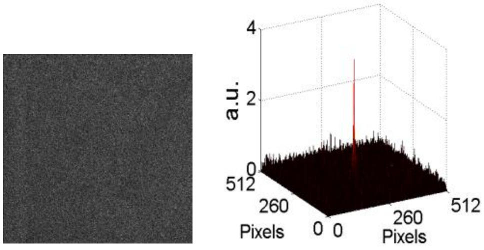
Figure 2: Phase-only masks (a) M1 and (b) M2; sparse pinhole arrays (c) S1 and (d) S2; and (e) an input image (i.e., grayscale "Lena" which can be found in http://sipi.usc.edu/database).

In phase-truncated optical cryptosystem, decryption keys (i.e., phase-only maps) are generated during the encoding, which are different from phase-only masks M1 and M2. Figures 3(a) and 3(b) show decryption keys $P_c(\mu,\nu)$ and $P_0(\xi,\eta)$ generated during the encoding, respectively. Figure 3(c) shows the ciphertext $A_0(\xi,\eta)$. It can be seen in Fig. 3(c) that the input image has been encoded. Figure 4(a) shows a decrypted image, when correct keys are used during the decryption. The MSE value for Fig. 4(a) is 1.6419×10^4. It can be seen in Fig. 4(a) that due to sparse pinhole arrays, plaintext cannot be clearly rendered during the decryption. Hence, when special attack and collision algorithms [18,19] are used, no plaintext information can be clearly extracted. The method using sparse pinhole arrays provides an additional and effective security layer for phase-truncated optical encoding system. Since the decrypted image still contains some invisible but useful plaintext information, correlation algorithm, such as nonlinear [22–37], can be further applied to conduct the authentication. Figure 4(b) shows the authentication result, when the decrypted image in Fig. 4(a) is nonlinearly correlated with the input image [see Fig. 2(e)]. The strength of applied nonlinearity is set as 0.30. It can be seen in Fig. 4(b) that only one remarkable peak is generated over noisy background. It indicates that the decrypted image in Fig. 4(a) is authentic. In practice, many parameters, such as peak to background noise ratio, can be further extracted from correlation distributions for the verification. Sparse pinhole arrays can be flexibly adjusted for encoding different input images in optical information authentication system to further optimize the outputs.



(a) (b) (c)

Figure 3: (a) $P_c(\mu,\nu)$, (b) $P_o(\xi,\eta)$, and (c) ciphertext.



(a) (b)

Figure 4: (a) A decrypted image using correct keys, and (b) authentication result.

4. CONCLUSIONS

In this paper, optical information authentication has been presented based on phase-truncated encoding approach using sparse pinhole arrays. Since plaintext cannot be clearly observed during the decoding, optical authentication method is further applied to verify the decrypted image. The simulation results have illustrated that decrypted images can be effectively authenticated. It has also been demonstrated that an additional and effective security layer can be established for phase-truncated optical encoding system.

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 under Grant No. JCYJ20160531184426473, and The Hong Kong Polytechnic University (Fund No. 1-ZE5F).

REFERENCES

1. Refregier, P., and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, Vol. 20, 767–769, 1995.
2. Javidi, B., "Securing information with optical technologies," *Physics Today*, Vol. 50, 27–32, 1997.
3. Matoba, O., T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," *Proceedings of the IEEE*, Vol. 97, 1128–1148, 2009.
4. Matoba, O., and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, Vol. 24, 762–764, 1999.
5. Unnikrishnan, G., J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, Vol. 25, 887–889, 2000.
6. Situ, G., and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, Vol. 29, 1584–1586, 2004.
7. Naughton, T. J., B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," *Journal of the Optical Society of America A*, Vol. 25, 2608–2617, 2008.
8. Hwang, H. E., 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," *Optics Letters*, Vol. 34, 3917–3919, 2009.
9. Rajput, S.K., and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," *Applied Optics*, Vol. 51, 5377–5386, 2012.
10. Peng, X., L. Yu, and L. Cai, "Double-lock for image encryption with virtual optical wavelength," *Optics Express*, Vol. 10, 41–45, 2002.

11. Zhang, Y., and B. Wang, "Optical image encryption based on interference," *Optics Letters*, Vol. 33, 2443–2445, 2008.

12. Kumar, P., J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Applied Optics*, Vol. 50, 1805–1811, 2011.

13. Chen, W., X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," *Optics Letters*, Vol. 35, 3817–3819, 2010.

14. Carnicer, A., M. M. Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Optics Letters*, Vol. 30, 1644–1646, 2005.

15. Peng, X., P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Optics Letters*, Vol. 31, 1044–1046, 2006.

16. Peng, X., H. Wei, and P. Zhang, "Asymmetric cryptography based on wavefront sensing," *Optics Letters*, Vol. 31, 3579–3581, 2006.

17. Qin, W., and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Optics Letters*, Vol. 35, 118–120, 2010.

18. Wang, X., and D. Zhao, "Double images encryption method with resistance against the specific attack based on an asymmetric algorithm," *Optics Express*, Vol. 20, 11994–12003, 2012.

19. Mehra, I., S. K. Rajput, and N. K. Nishchal, "Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification," *Optical Engineering*, Vol. 52, 028202, 2013.

20. Ozaktas, H.M., Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing* (Wiley, 2001).

21. Chen, W., X. Chen, A. Anand, and B. Javidi, "Optical encryption using multiple intensity samplings in the axial domain," *Journal of the Optical Society of America A*, Vol. 30, 806–812, 2013.

22. Sadjadi, F., and B. Javidi, *Physics of the Automatic Target Recognition* (Springer, 2007).

23. Chen, W., X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," *IEEE Photonics Journal*, Vol. **5**, 6900113, 2013.

24. Pérez-Cabré, E., M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Optics Letters*, Vol. 36, 22–24, 2011.

25. Pérez-Cabré, E., H. C Abril, M. S Millan, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *Journal of Optics*, Vol. 14, 094001, 2012.

26. Chen, W., "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," *IEEE Photonics Journal*, Vol. 8, 6900209, 2016.

27. Chen, W., and X. Chen, "Digital holography-secured scheme using only binary phase or amplitude as ciphertext," *Applied Optics*, Vol. 55, 6740–6746, 2016.

28. Chen, W., "Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification," *Applied Optics*, Vol. 54, 10711–10716, 2015.

29. Chen, W., and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," *EPL (Europhysics Letters)*, Vol. 110, 44002, 2015.

30. Chen, W., and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," *Optics and Lasers in Engineering*, Vol. 73, 123–127, 2015.

31. Chen, W., and X. Chen, "Marked ghost imaging," *Applied Physics Letters*, Vol. 104, 251109, 2014.

32. Chen, W., and X. Chen, "Optical color-image verification using multiple-pinhole phase retrieval," *Journal of Optics*, Vol. 16, 075403, 2014.

33. Chen, J. X., Z. L. Zhu, C. Fu, H. Yu, and L. B. Zhang, "Gyrator transform based double random phase encoding with sparse representation for information authentication," *Optics & Laser Technology*, Vol. 70, 50–58, 2015.

34. Chen, W., and X. Chen, "Optical multiple-image authentication based on modified Gerchberg-Saxton algorithm with random sampling," *Optics Communications*, Vol. 318, 128–132, 2014.

35. Yi, F., Y. Jeoung, and I. Moon, "Three-dimensional image authentication scheme using sparse phase information in double random phase encoded integral imaging," *Applied Optics*, Vol. 56, 4381–4387, 2017.

36. Javidi, B., 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, and A. Markman, "Roadmap on optical security," *Journal of Optics*, Vol. 18, 083001, 2016.

37. Chen, W., "Ghost identification based on single-pixel imaging in big data environment," *Optics Express*, Accepted and In press, 2017.