Optical Decoded-Image Correlation using Simultaneous Compression of Input Image and the Phase in the Recording Plane

Wen Chen
Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
E-mail: owen.chen@polyu.edu.hk

***Abstract*—The 2D optical decoded-image correlation is presented by using simultaneous compression of input image and the phase in the recording plane. The compressed input image is encrypted via double random phase encoding. In the recording plane, complex-valued wavefront is extracted, and only phase part is retained and compressed as ciphertext. During the decoding, either digital or optical approach can be applied, and due to the designed strategy the decoded image cannot visually render information related to input image. The decoded-image correlation is conducted to verify whether the receiver possesses correct keys or is an authorized person. The method using simultaneous compression of input image and the phase in the recording plane can be used as a complementary alternative for optical information correlation.**

Keywords—optical decoded-image correlation; compressed image; compressed phase pattern; 2D information verification.

I. INTRODUCTION

Optical encryption [1]–[12] has attracted much current attention, since it possesses several remarkable characteristics, such as parallel processing. The input image can be converted into stationary white noise, and various domains [1]–[12], such as gyrator transform [7] and fractional Fourier transform [8], have been applied. In addition, some optical infrastructures, such as holography and ghost imaging, have been studied, and system robustness and security are also investigated [1]–[12].

Since double random phase encoding [1] was developed, its vulnerability has also been studied [13]–[15]. For instance, Carnicer et al. [13] used chosen-cyphertext attack to extract phase-only patterns in the optical security system. Peng et al. [14],[15] applied known-plaintext attack and chosen-plaintext attack algorithms to estimate phase keys.

To enhance security of optical encryption systems, researchers [16]–[20] have developed some methods. For instance, Hennelly and Sheridan [17] introduced pixel scrambling algorithm to enhance the security, and the work in Ref. [18] illustrated that phase retrieval algorithm can be applied as an effective alternative to enhance system security. Qin and Peng [20] studied an asymmetric approach based on phase truncation to generate decryption keys which are different from the encryption keys.

In recent years, optical correlation [21]–[32] has been developed based on optical image encryption setup. For instance, Pérez-Cabré et al. [21] applied sparse wavefront in the CCD plane for the decoding and authentication. Other methods [23]–[32], such as phase hologram and ghost imaging, have also been explored, and optical encoding and correlation are simultaneously conducted.

Here, 2D optical decoded-image correlation is presented by using simultaneous compression of input image and phase in the recording plane. The compressed input image is encrypted via double random phase encoding. In the recording plane, complex-valued wavefront is extracted, and only phase part is retained and compressed as ciphertext [23],[28]. During the decoding, either digital or optical approach can be applied, and due to the designed strategy the decoded image cannot visually render information related to input image. The decoded-image correlation is conducted to verify whether the receiver possesses correct keys or is an authorized person [21]–[32]. The method using simultaneous compression of input image and the phase in the CCD plane is extended and presented based on previous works in Refs. [23],[28], and can be employed as a complementary alternative for the 2D encryption-based optical information correlation [21]–[32].

II. THEORETICAL ANALYSES

Figure 1 shows a schematic setup for double random phase encoding in fractional Fourier domain [8]. In this setup, a random phase-only mask M1 is placed just behind the compressed input image, which can make the input image white but nonstationary [1]–[12]. A random phase-only mask M2 will maintain the whiteness but makes it stationary [1]–[12]. Let M1 and M2 denote random phase-only patterns respectively located in the input image plane and spatial frequency domain, and phase values are randomly distributed in the range of $[0, 2\pi]$. Here, (x,y), (ξ,η) and (μ,ν) are

This work was supported by the startup grant (1-ZE5F) from The Hong Kong Polytechnic University, and Science and Technology Innovation Commission of Shenzhen Municipality through Basic Research Program under the Grant JCYJ20160531184426473.

employed to denote coordinates of the input image plane, spatial frequency plane and CCD plane, respectively. It is straightforward to describe complex-valued wavefront in the recording plane [4],[23],[28] as follows:

$$O(\mu,\nu)=\mathrm{FrFT}_{\beta}\left(\left\{\mathrm{FrFT}_{\alpha}\left[P_s(x,y)\mathrm{M1}(x,y)\right]\right\}\mathrm{M2}(\xi,\eta)\right), \quad (1)$$

where $P_s(x,y)$ denotes a compressed input image, $O(\mu,\nu)$ denotes complex-valued wavefront extracted in the recording plane, α and β denote function orders, and FrFT denotes fractional Fourier transform [4],[8] described by

$$\mathrm{FrFT}_{\alpha}\left[P_s(x)\mathrm{M1}(x)\right]=\int_{-\infty}^{+\infty}P_s(x)\mathrm{M1}(x)\,T_{\alpha}(\xi_{\alpha},x)\,dx, \quad (2)$$

where

$$T_{\alpha}(\xi_{\alpha},x)=\begin{cases}U\,\exp\left\{j\pi\left[\xi_{\alpha}^2\cot(\alpha\pi/2)+x^2\cot(\alpha\pi/2)-2\xi_{\alpha}x\csc(\alpha\pi/2)\right]\right\} & \text{if } \alpha\neq 2w\\ \delta(\xi_{\alpha}-x) & \text{if } \alpha=4w\\ \delta(\xi_{\alpha}+x) & \text{if } \alpha=4w\pm 2\end{cases},$$

$U=\sqrt{1-j\cot(\alpha\pi/2)}$, $j=\sqrt{-1}$, and w denotes an integer. For the sake of brevity only 1D form is described, and it is straightforward to describe the 2D FrFT [4],[8].

Some methods, such as digital holography [4],[33],[34] and phase retrieval [35]–[37], can be applied to extract complex-valued wavefront $O(\mu,\nu)$ in the recording plane. In this study, only phase part of the extracted complex-valued wavefront is retained [23],[28], and is denoted as $P(\mu,\nu)$. To achieve the decoded-image correlation without information visualization, the extracted phase map is also compressed (i.e., unselected pixels are directly set as zero), i.e., $P_s(\mu,\nu)$ as ciphertext.

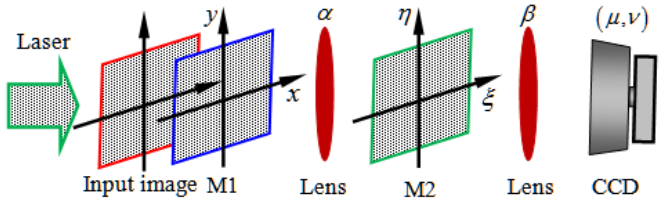

Fig. 1. A schematic setup [4],[23],[28],[38] for the optical decoded-image correlation method using the compressed input image and the compressed phase in the recording plane. Random phase-only pattern M1 is placed just behind the compressed input image. Symbols α and β denote the FrFT function orders. The plane wave is generated for the illumination.

For the decoding, the compressed phase pattern $P_s(\mu,\nu)$ is used as ciphertext, and the FrFT function orders and random phase-only pattern M2 are used as security keys. When ciphertext and security keys are available, a decoded image can be described by [4],[23],[28]

$$\hat{P}(x,y)=\left|\mathrm{FrFT}_{-\alpha}\left(\left\{\mathrm{FrFT}_{-\beta}\left[P_s(\mu,\nu)\right]\right\}\left[\mathrm{M2}(\xi,\eta)\right]^{*}\right)\right|^2, \quad (3)$$

where $\mathrm{FrFT}_{-\alpha}$ and $\mathrm{FrFT}_{-\beta}$ denote inverse fractional Fourier transform [4],[8], $|\ |$ denotes the modulus operation, asterisk denotes complex conjugate, and $\hat{P}(x,y)$ denotes a decoded image. Since the compressed input image $P_s(x,y)$ and the compressed phase $P_s(\mu,\nu)$ are simultaneously used, the decoded image $\hat{P}(x,y)$ does not visually render information related to the input image. Similarly to previous works in Refs. [21]–[32],[38],[39], nonlinear correlation is conducted between the decoded image and the originally whole input image (such as stored in a remote database) to verify whether the receiver possesses correct keys or is an authorized person [31],[32]. To show the whole process, a flow chart is given in Fig. 2.

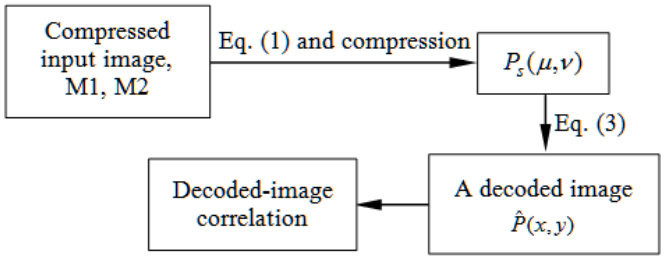

Fig. 2. Flow chart for illustrating the whole process.

III. SIMULATION RESULTS AND DISCUSSION

The setup in Fig. 1 is numerically conducted to show the validity. In Fig. 1, double random phase encoding is applied, and random phase-only pattern M1 is placed just behind the compressed input image. The FrFT function orders α and β are 0.3 and 0.7, respectively. An input image, i.e., "Lena" with 512×512 pixels (http://sipi.usc.edu/database), is compressed, and is encoded by using the setup in Fig. 1. Only phase part in the CCD plane is retained, and is further compressed as ciphertext $P_s(\mu,\nu)$.

The random phase-only patterns M1 and M2 are shown in Figs. 3(a) and 3(b), respectively. The compressed image $P_s(x,y)$ is shown in Fig. 3(c), and only 35.0% of the original image are randomly selected and retained (unselected pixels are directly set as zero). The phase ciphertext, i.e., $P_s(\mu,\nu)$, is shown in Fig. 3(d), and only 45.0% of the original phase map $P(\mu,\nu)$ are randomly selected and retained (others are directly set as zero).

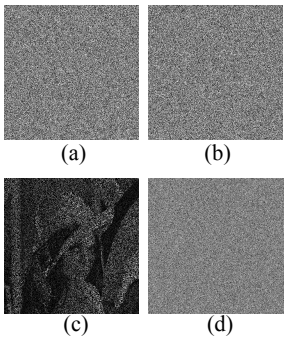

Fig. 3. Phase pattern (a) M1 and (b) M2, (c) the compressed input image $P_s(x,y)$, and (d) the compressed phase $P_s(\mu,\nu)$.

Figure 4(a) shows a decoded image, when all keys are correctly used. The peak signal-to-noise ratio (PSNR) for Fig. 4(a) is 9.91 dB. It can be seen in Fig. 4(a) that the decoded image does not visually render the information. Figure 4(b) shows a correlation distribution generated between that in Fig. 4(a) and the originally whole input image. It can be seen in Fig. 4(b) that only one remarkable peak is observed to verify the receiver, i.e., an authorized person or has correct keys.

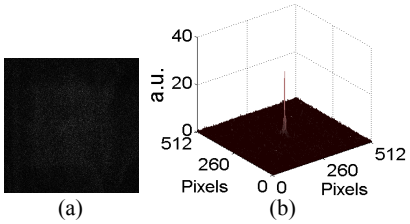

Fig. 4. (a) A decoded image obtained when all keys are correctly used, and (b) the correspondingly generated correlation distribution.

When only phase pattern M2 is incorrectly applied during the decoding, a decoded image is obtained in Fig. 5(a). The PSNR for Fig. 5(a) is 9.893 dB. The correspondingly generated correlation map is shown in Fig. 5(b). When only FrFT function order β has an error of 0.01 during the decoding, a decoded image is obtained in Fig. 5(c). The PSNR for Fig. 5(c) is 9.894 dB. The correspondingly generated correlation map is shown in Fig. 5(d). It can be seen in Figs. 5(b) and 5(d) that only noisy correlation maps are generated, when wrong keys are applied for the decoding.

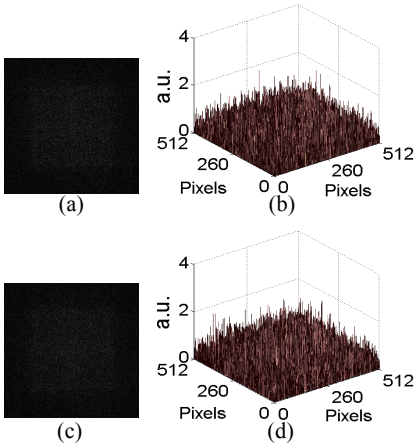

Fig. 5. (a) A decoded image obtained when only phase pattern M2 is incorrectly applied during the decoding, and (b) the correspondingly generated correlation map; (c) a decoded image obtained when only FrFT function order β has an error of 0.01 during the decoding, and (d) the correspondingly generated correlation map.

IV. CONCLUSIONS

The 2D optical decoded-image correlation is presented by using simultaneous compression of input image and the phase in the recording plane. The numerical results illustrate that the decoded image cannot visually render information related to input image due to the designed strategy. The decoded-image correlation can be effectively and correctly conducted to verify whether the receiver possesses correct keys or is an authorized person. The method using simultaneous compression of the plaintext and the phase in the CCD plane is extended and presented based on previous works in Refs. [23],[28],[38],[39], and can be used as a complementary alternative for optical correlation [21]–[32],[38],[39].

REFERENCES

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

[2] B. L. Volodin, B. Kippelen, K. Meerholz, B. Javidi, and N. Peyghambarian, "A polymeric optical pattern-recognition system for security verification," *Nature* vol. 383, pp. 58–60, 1996.

[3] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* vol. 33, pp. 1752–1756, 1994.

[4] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon*. vol. 6, pp. 120–155, 2014.

[5] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," *Opt. Lett.* vol. 35, pp. 3817–3819, 2010.

[6] W. Chen and X. Chen, "Space-based optical image encryption," *Opt. Express* vol. 18, pp. 27095–27104, 2010.

[7] Z. Liu, L. Xu, C. Lin, and S. Liu, "Image encryption by encoding with a nonuniform optical beam in gyrator transform domains," *Appl. Opt.* vol. 49, pp. 5632–5637, 2010.

[8] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.* vol. 25, pp. 887–889, 2000.

[9] X. F. Meng, L. Z. Cai, X. F. Xu, X. L. Yang, X. X. Shen, G. Y. Dong, and Y. R. Wang, "Two-step phase-shifting interferometry and its application in image encryption," *Opt. Lett.* vol. 31, pp. 1414–1416, 2006.

[10] X. Wang, D. Zhao, F. Jing, and X. Wei, "Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics," *Opt. Express* vol. 14, pp. 1476–1486, 2006.

[11] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photon.* vol. 1, pp. 589–636, 2009.

[12] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using fractional Fourier transform," *Opt. Eng.* vol. 42, pp. 1583–1588, 2003.

[13] 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.* vol. 30, pp. 1644–1646, 2005.

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

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

[16] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* vol. 15, pp. 10253–10265, 2007.

[17] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* vol. 28, pp. 269–271, 2003.

[18] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.* vol. 35, pp. 2464–2469, 1996.

[19] W. Liu, Z. Liu, and S. Liu, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm," *Opt. Lett.* vol. 38, pp. 1651–1653, 2013.

[20] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.* vol. 35, pp. 118–120, 2010.

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

[22] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.* vol. 38, pp. 3198–3201, 2013.

[23] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *J. Opt.* vol. 16, pp. 025402, 2014.

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

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

[26] W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," *Appl. Phys. Lett.* vol. 103, pp. 221106, 2013.

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

[28] W. Chen, "Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification," *Appl. Opt.* vol. 54, pp. 10711–10716, 2015.

[29] X. Wang, W. Chen, S. Mei, and X. Chen, "Optically secured information retrieval using two authenticated phase-only masks," *Sci. Rep.* vol. 5, pp. 15668, 2015.

[30] W. Chen, X. Wang, and X. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," *J. Opt.* vol. 17, pp. 035702, 2015.

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

[32] W. Chen, "Computer-generated hologram authentication via optical correlation," IEEE International Conference on Industrial Informatics (IEEE INDIN 2016), Poitiers, France, July 18–July 21 2016.

[33] I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," *Opt. Lett.* vol. 22, pp. 1268–1270, 1997.

[34] U. Schnars and W. Jueptner, *Digital Holography: Digital Hologram Recording, Numerical Reconstruction, and Related Techniques* (Springer, New York, 2005).

[35] W. Chen, G. Situ, and X. Chen, "High-flexibility optical encryption via aperture movement," *Opt. Express* vol. 21, pp. 24680–24691, 2013.

[36] W. Chen, X. Chen, A. Anand, and B. Javidi, "Optical encryption using multiple intensity samplings in the axial domain," *J. Opt. Soc. Am. A* vol. 30, pp. 806–812, 2013.

[37] W. Chen, C. Quan, and C. J. Tay, "Retrieval of complex object fields in coherent diffractive imaging using position shift of a phase mask," *Opt. Eng.* vol. 50, pp. 080502, 2011.

[38] W. Chen and X. Chen, "Digital holography-secured scheme using only binary phase or amplitude as ciphertext," *Appl. Opt.* vol. 55, pp. 6740–6746, 2016.

[39] W. Chen and X. Chen, "Optical multiple-image authentication based on modified Gerchberg-Saxton algorithm with random sampling," *Opt. Commun.* vol. 318, pp. 128–132, 2014.