Journal of the Optical Society of Korea
Vol. 18, No. 4, August 2014, pp. 401-405

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2014.18.4.401

Accumulation Encoding Technique Based on Double Random Phase Encryption for Transmission of Multiple Images

In-Ho Lee*

Department of Electrical, Electronic, and Control Engineering, IITC, Hankyong National University, Ansung 456-749, Korea

(Received July 7, 2014 : revised July 25, 2014 : accepted July 25, 2014)

In this paper, we propose an accumulation encoding scheme based on double random phase encryption (DRPE) for multiple-image transmission. The proposed scheme can be used for a low-complexity DRPE system due to the simple structure of the accumulation encoder and decoder. For accumulation encoding of multiple images, all of the previously encrypted data are added, and hence the accumulation encoding can improve the security of the DRPE-encrypted data. We present a scheme for encryption and decryption for DRPE-based accumulation encoding, and a method for accumulation encoding and decoding. Finally, simulation results verify that the DRPE-based accumulation encoding scheme for multiple images is powerful in terms of data security.

Keywords : Optical encryption, Double random phase encryption, Accumulation encoding, Image transmissions
OCIS codes : (060.4785) Optical security and encryption; (200.4560) Optical data processing

I. INTRODUCTION

Information security is one of the most important issues in data transmission. Optical encryption has been widely investigated for information security because of its high encryption speed [1-23]. As a representative optical encryption technique, double random phase encryption (DRPE) has been well studied [1-21] and improvements have been developed, such as DRPE using the Fresnel domain [2], DRPE using a full-phase processor [3], DRPE using digital holography [4, 5], photon-counting DRPE [6, 7], and DRPE using fractional Fourier transform [8-10].

Since DRPE uses double random phase masks for encryption, a security defect can be introduced [11], so updating the phase masks is required to resolve the security problem. However, such a resolution may lead to a cost problem. Therefore, advanced DRPE techniques without phasemask updating have been introduced [8-10, 18-21]. In particular, DRPE using fractional Fourier transform has been presented [8-10] to enhance the security of DRPE systems, where security is improved by increasing the number of encryption parameters. However, DRPE systems using fractional Fourier transform can be more complicated because of many encryption parameters. Hence, DRPE using orthogonal encoding has been presented as a low-complexity DRPE system in which the orthogonal encoder contains simple linear functions [20, 21].

In this paper we propose a DRPE-based accumulation encoding scheme for multiple-image transmission. It can be considered a low-complexity DRPE scheme because of the simple structure of its accumulation encoder and decoder. In addition, data security can be enhanced by introducing accumulation encoding into DRPE. We provide a detailed method for DRPE-based accumulation encoding and decoding, and show simulation results verifying that decryption of the image encrypted by the DRPE-based accumulation encoding scheme becomes more difficult as the number of accumulated images increases, even when the phase key used in DRPE is known.

The paper is organized as follows. Section II presents the concepts behind DRPE. The DRPE-based accumulation encoding scheme for multiple-image transmission is described in Section III. To verify this optical encryption scheme, simulation results produced by DRPE using accumulation

*Corresponding author: ihlee@hknu.ac.kr
Color versions of one or more of the figures in this paper are available online.

encoding are provided in Section IV. Finally, we conclude the paper in Section V.

II. DOUBLE RANDOM PHASE ENCRYPTION

DRPE, an optical encryption technique, uses double random phase masks to encrypt data. Data encrypted by DRPE look like noise. For decryption, the key random phase mask used for encryption is required. For the sake of simplicity, in this paper we consider the encryption of one-dimensional data.

Let $p(x)$ denote the primary data in the spatial domain, and let $m_s(x)$ and $m_f(w)$ represent the random phases in the spatial and spatial frequency domains respectively. $m_s(x)$ and $m_f(w)$ are uniformly distributed over [0, 1]. Figures 1(a) and (b) depict the schematic setup of encryption and decryption for DRPE respectively, where f is the focal length and two lenses are used for Fourier transform and inverse Fourier transform. As shown in Fig. 1(a), for encryption first the primary data is multiplied by the random phase mask $\exp[i2\pi m_s(x)]$ in the spatial domain. After passing the signal through the first lens we obtain $\mathfrak{I}\{p(x)\exp[i2\pi m_s(x)]\}$, where $\mathfrak{I}$ denotes the Fourier transform. Next it is multiplied by the random phase mask $\exp[i2\pi m_f(w)]$ in the spatial frequency domain. After passing through the second lens, the data encrypted by DRPE, $s_e(x)$, are obtained as follows [6]:

$$s_e(x) = \mathfrak{I}^{-1}\left[\mathfrak{I}\left\{p(x)\exp\left[i2\pi m_s(x)\right]\right\}\exp\left\{i2\pi m_f(w)\right\}\right] \quad (1)$$

where $\mathfrak{I}^{-1}$ represent the inverse Fourier transform. Exploiting the characteristics of a complex-valued function, the encrypted data can be expressed as amplitude and phase parts, i.e. $s_e(x) = |s_e(x)|\exp[i\phi_e(x)]$.

As shown in Fig. 1(b), for decryption the encrypted data are multiplied by the complex conjugate of the key information, i.e. $\exp[-i2\pi m_f(w)]$. The decrypted data are then obtained as follows [6]:

$$d(x) = \left|\mathfrak{I}^{-1}\left[\mathfrak{I}[s_e(x)]\exp\left\{-i2\pi m_f(w)\right\}\right]\right| \quad (2)$$

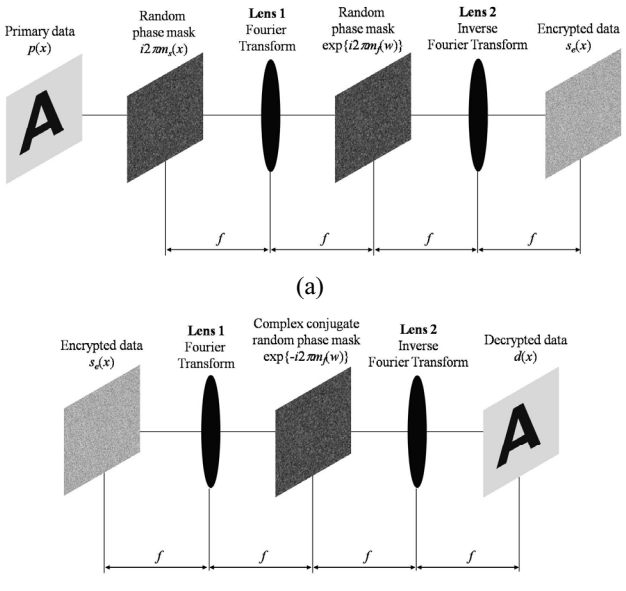

FIG. 1. Schematic setup of (a) encryption and (b) decryption for DRPE.

III. DRPE-BASED ACCUMULATION ENCODING AND DECODING

Figures 2(a) and (b) depict the schemes for DRPE-based accumulation encoding and decoding for encryption and decryption, respectively. As shown in Fig. 2(a), the n^{th} primary image $p_n(x)$ is encrypted and encoded for transmission. It is noted that DRPE with the same random phase mask is used for encryption of all the primary images. The data encrypted by DRPE, $s_{e,n}(x)$, are encoded with the accumulation encoding scheme as follows:

$$y_{e,n}(x) = \begin{cases} s_{e,1}(x) & \text{for } n = 1 \\ s_{e,n}(x) + y_{e,n-1}(x) & \text{for } n \geq 2 \end{cases} \quad (3)$$

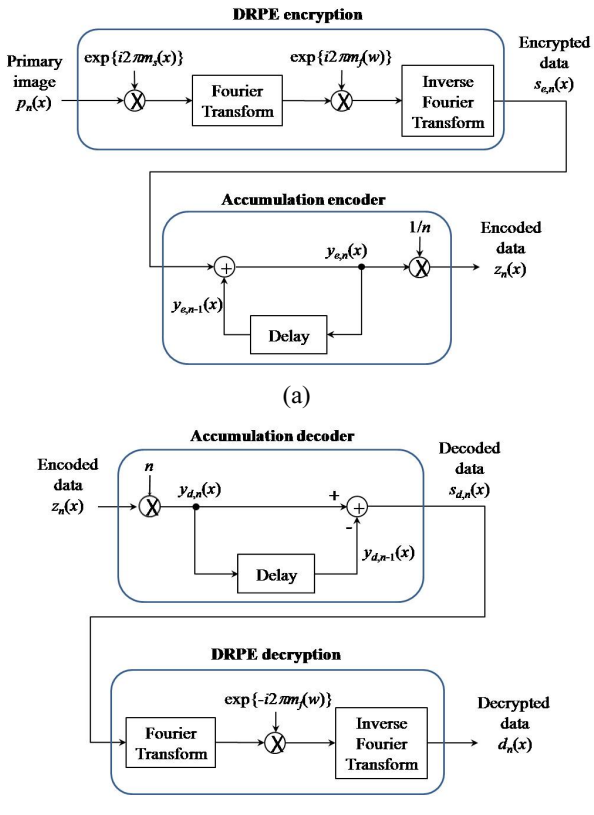

FIG. 2. Scheme for DRPE-based accumulation encoding: (a) encryption and (b) decryption.

where $y_{e,n}(x)$ represents the n^{th} encoded data. As seen in Eq. (3), for accumulation encoding all the previous encrypted data are added, which can enhance the security of the DRPE-encrypted data. Eq. (3) can be simply rewritten as

$$y_{e,n}(x) = \sum_{i=1}^{n} s_{e,i}(x) \tag{4}$$

After accumulation encoding of the n^{th} encrypted data, the n^{th} encoded data are normalized by the factor $1/n$, and finally the n^{th} encoded data $z_n(x)$ are obtained as follows:

$$z_n(x) = \frac{1}{n} y_{e,n} = \frac{1}{n} \sum_{i=1}^{n} s_{e,i}(x) \tag{5}$$

For perfect decryption of the accumulation-encoded data, as shown in Fig. 2(b), the encoded data are multiplied by n to scale it. Then the accumulation decoding is performed as follows:

$$s_{d,n}(x) = \begin{cases} y_{d,1}(x) & \text{for } n = 1 \\ y_{d,n}(x) - y_{d,n-1}(x) & \text{for } 2 \le n \le N \end{cases} \tag{6}$$

where $s_{d,n}(x)$ denotes the n^{th} decoded data and $y_{d,n}(x) = nz_n(x)$. By inserting Eq. (5) into Eq. (6), we obtain $s_{d,n}(x) = s_{e,n}(x)$, which means that the encoded data are perfectly decoded. The n^{th} decoded data are then decrypted by DRPE using the same random phase mask as for encryption. Finally the n^{th} decrypted data $d_n(x)$ are obtained as $d_n(x) = p_n(x)$.

The accumulation encoder and decoder require only a simple linear operation and storage to store the data with the size of a single image, as seen in Eqs. (3) and (6). Therefore, the addition of the accumulation encoder and decoder to the DRPE system requires low cost and effort.

IV. SIMULATION RESULTS

To evaluate the performance of DRPE-based accumulation encoding we consider 20 primary images with 500(H)× 500(V) pixels, as shown in Fig. 3. Figures 4(a)-(t) show the simulated results of DRPE-based accumulation encoding, meaning $z_n(x)$ in Fig. 2(a). From the figures we can see that the accumulation-encoded images are perfectly encrypted because they look like noise. Figures 5 and 6 show the decrypted images without and with accumulation decoding respectively, where it is assumed that the DRPE key information is perfectly known for decryption. When no decoding is used, the encoded data are not decoded with the accumulation decoder but are directly decrypted by DRPE decryption; thus, $s_{d,n}(x) = z_n(x)$. From Figs. 5(a)-(t), it is observed that when no decoding is used the image recognition becomes worse as the index of accumulation encoding n increases, even though perfect DRPE key informationis known for decryption. This also, means that

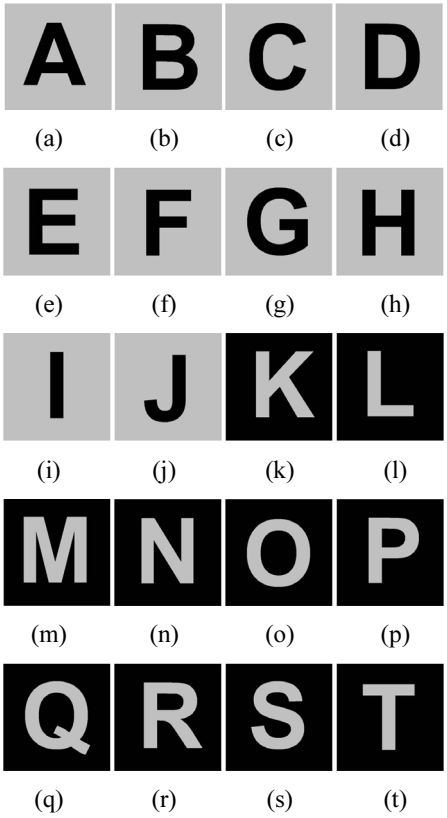

FIG. 3. Primary images.

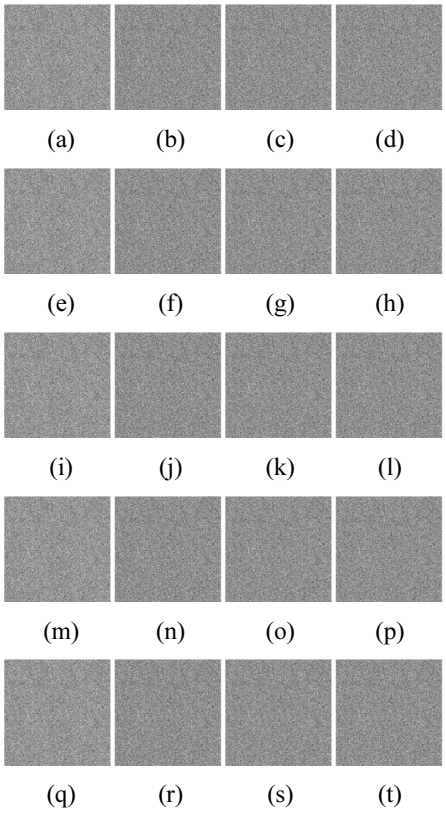

FIG. 4. Simulated results of DRPE-based accumulation encoding: (a)-(t) the 1st-20th encoded images.

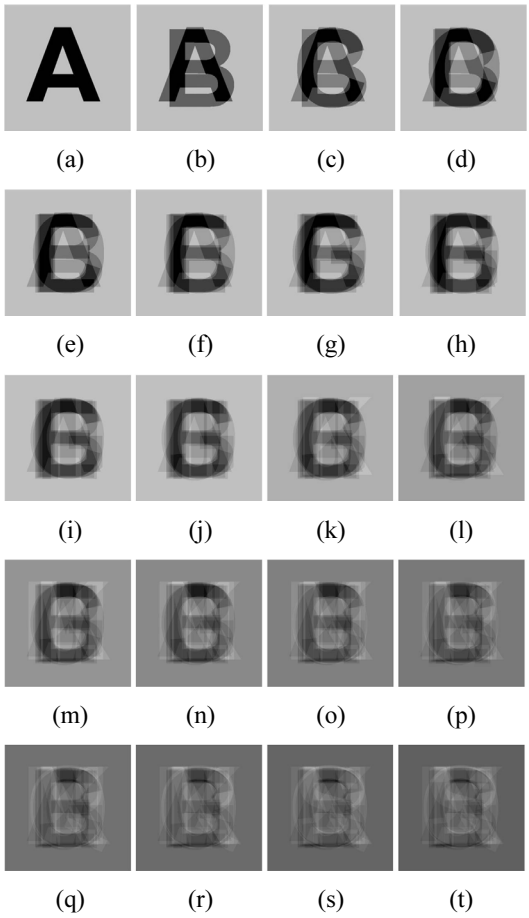

FIG. 5. Simulated results of decryption of DRPE-based accumulation encoding when no decoding is used: (a)-(t) 1st-20th decrypted images.

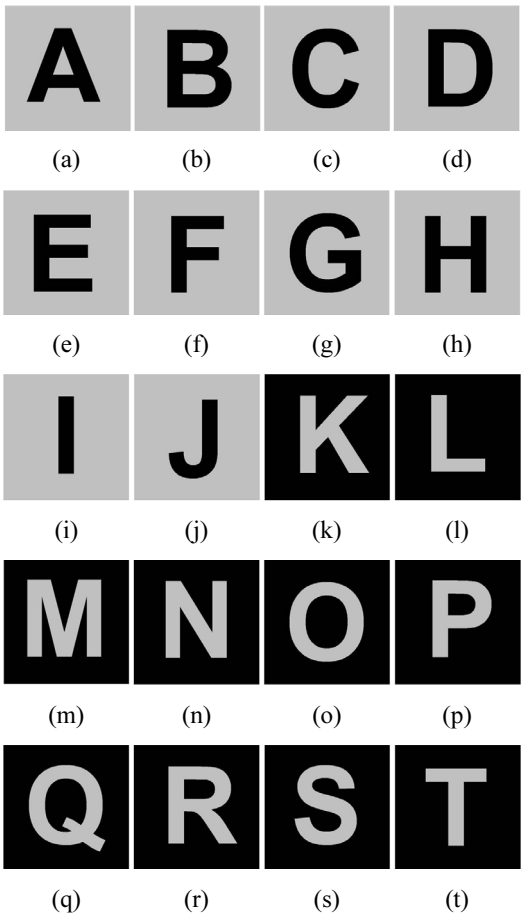

FIG. 6. Simulated results of decryption of DRPE-based accumulation encoding when decoding is used: (a)-(t) 1st-20th decrypted images.

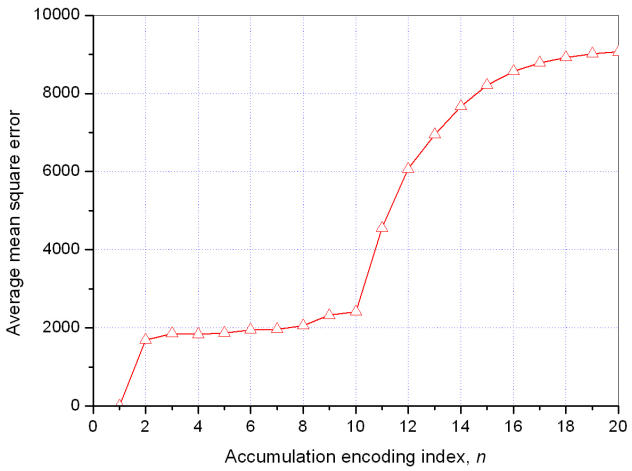

FIG. 7. MSE results for primary versus decrypted images, without decoding.

accumulation encoding is able to improve the security of DRPE-encrypted data even when the DRPE key information is known. Figures 6(a)-(t) indicate that the encoded images are perfectly decrypted when correct decoding and decryption are performed.

To quantify the differences between the primary images in Figs. 3(a)-(t) and the decrypted images without decoding in Figs. 5(a)-(t) respectively, mean square error (MSE) results are calculated, as shown in Fig. 7, where we assume that the image pixel values are integers ranging from 0 to 255. In Fig. 7 the average MSE for the n^{th} accumulation encoding is obtained as follows:

$$AMSE_n = \frac{1}{n}\sum_{i=1}^{n}\left[\frac{1}{500\times 500}\sum_{x=1}^{500\times 500}\left(d_n(x)-p_i(x)\right)^2\right] \quad (7)$$

When no decoding is used, the n^{th} decrypted data $d_n(x)$ contain the data for the 1st through n^{th} primary images, as described in Eq. (5). Thus we show the average of MSE results between the n^{th} decrypted image and the 1st through n^{th} primary images, as in Eq. (7). Figure 7 demonstrates that the average MSE increases with the accumulation encoding index n. Especially when $n \geq 11$ the average MSE increases greatly because the 11th through 20th primary images have a different color pattern than the 1st through 10th primary images. From these results it can be

seen that the encoded data become more secure as the accumulation encoding index rises, even though the DRPE key is known in decryption. However, for the first accumulation encoding the MSE result is zero, as the decrypted data contain only the data for the first primary image.

V. CONCLUSIONS

We propose a DRPE-based accumulation encoding technique for multiple-image transmission. In particular, we present the schemes for encryption and decryption for DRPE-based accumulation encoding and decoding, respectively, and methods for accumulation encoding and decoding. The simulation results verify that DRPE-based accumulation encoding for multiple-image transmission can enhance the security of DRPE-encrypted data when the key information of DRPE is perfectly known in decryption. Furthermore, since the accumulation encoder and decoder require only a simple linear operation and enough storage to hold a dataset of a single image, the DRPE system with accumulation encoding can be implemented with little cost and effort.

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. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762-764 (1999).
3. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915-1927 (1999).
4. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595-6601 (2000).
5. H.-Y. Tu, J.-S. Chiang, J.-W. Chou, and C.-J. Cheng, "Full phase encoding for digital holographic encryption using liquid crystal spatial light modulators," Jpn. J. Appl. Phys. **47**, 8838-8843 (2008).
6. E. Perez-Cabre, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22-24 (2011).
7. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett. **38**, 3198-3201 (2013).
8. M. Joshi, C. Shakher, and K. Singh, "Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys," Opt. Commun. **283**, 2496-2505 (2010).
9. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887-889 (2000).
10. M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," Opt. Commun. **279**, 35-42 (2007).
11. Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253-10265 (2007).
12. T. Nomura and B. Javidi, "Optical encryption system with a binary key code," Appl. Opt. **39**, 4783-4787 (2000).
13. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," Appl. Opt. **46**, 6641-6647 (2007).
14. M. Singh, A. Kumar, and K. Singh, "Secure optical system that uses fully phase-based encryption and lithium niobate crystal as phase contrast filter for decryption," Opt. Laser Technol. **40**, 619-624 (2008).
15. T. Sarkadi and P. Koppa, "Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys," Appl. Opt. **51**, 745-750 (2012).
16. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack," Opt. Express **18**, 13772-13781 (2010).
17. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," Opt. Commun. **259**, 532-536 (2006).
18. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," Appl. Opt. **40**, 2310-2315 (2001).
19. W. Chen and X. Chen, "Space-based optical image encryption," Opt. Express **18**, 27095-27104 (2010).
20. I.-H. Lee and M. Cho, "Double random phase encryption based orthogonal encoding technique for color images," J. Opt. Soc. Korea **18**, 129-133 (2014).
21. I.-H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," J. Opt. Soc. Korea **18**, 201-206 (2014).
22. S. H. Jeon and S. K. Gil, "Dual optical encryption for binary data and secret key using phase-shifting digital holography," J. Opt. Soc. Korea **16**, 263-269 (2012).
23. S. K. Gil, "2-step quadrature phase-shifting digital holographic optical encryption using orthogonal polarization and error analysis," J. Opt. Soc. Korea **16**, 354-364 (2012).