Security enhancement for double-random phase encryption using orthogonally encoded image and electronically synthesized key data

In-Ho Lee and Myungjin Cho*

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

**Corresponding author: mjcho@hknu.ac.kr*

Received September 9, 2014; accepted October 24, 2014; posted online December 12, 2014

We propose a security-enhanced double-random phase encryption (DRPE) scheme using orthogonally encoded image and electronically synthesized key data to cope with the security problem of DRPE technique caused by fixed double-random phase masks for encryption. In the proposed scheme, we adopt the electronically synthesized key to frequently update the phase mask using a spatial light modulator, and also employ the orthogonal encoding technique to encode the image and electronically synthesized key data, which can enhance the security of both data. We provide detailed procedures for encryption and decryption of the proposed scheme, and provide the simulation results to show the encryption effects of the proposed scheme.

OCIS codes: 060.4785, 200.4560.
doi: 10.3788/COL201513.010603.

Optical encryption techniques have been widely researched for data security since they can provide higher encryption speed than non-optical encryption techniques[1–23]. In particular, double-random phase encryption (DRPE), one of the main optical encryption techniques, has been well investigated and improved as follows: DRPE using digital holography[2,3], photon-counting DRPE[4,5], DRPE using fractional Fourier transform[6–8], and DRPE using orthogonal encoding[18,19].

The DRPE technique has security flaws caused by using fixed double-random phase masks for encryption[9]. Thus, advanced DRPE techniques have been developed to improve the security: DRPE using fractional Fourier transform adopts complicated parameters for encryption in order to achieve the security enhancement[6–8] and DRPE using orthogonal encoding employs a Hadamard matrix[24] with orthogonal property to encode the data encrypted by DRPE[18,19]. However, the fundamental security problem of DRPE can be resolved by frequently updating the key phase mask. Hence, in this letter, we propose a DRPE scheme with security enhancement using orthogonally encoded image and electronically synthesized key by spatial light modulator (SLM) to frequently update the key phase mask in DRPE systems. In the proposed scheme, SLM is used to facilitate the updating of the key phase mask used for DRPE. The input of SLM is the key data generated by statistical random generation and frequently (referred to as electronically synthesized key data in this letter), and the SLM generates the key phase mask corresponding to the input data. Then, the key phase mask generated by SLM is employed to encrypt an image, and the electronically synthesized key data used for the image encryption are encrypted by DRPE with the fixed key phase mask (referred to as the physical key phase mask in this letter). Finally, both encrypted image and the electronically synthesized key data are encoded with orthogonal encoding. It is noted that the conventional DRPE scheme uses only the physical key phase mask, whereas the proposed scheme uses both the physical and electronically synthesized key phase masks. Also, the key data of the physical key phase mask are not transmitted, but the electronically synthesized key data are encoded and transmitted with the image because the electronically synthesized key data

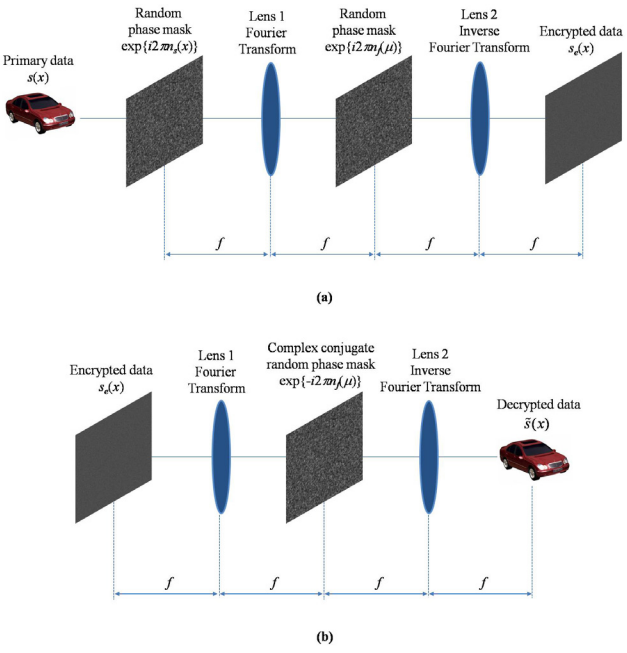

Fig. 1. Schematic setup of (a) encryption and (b) decryption for DRPE.

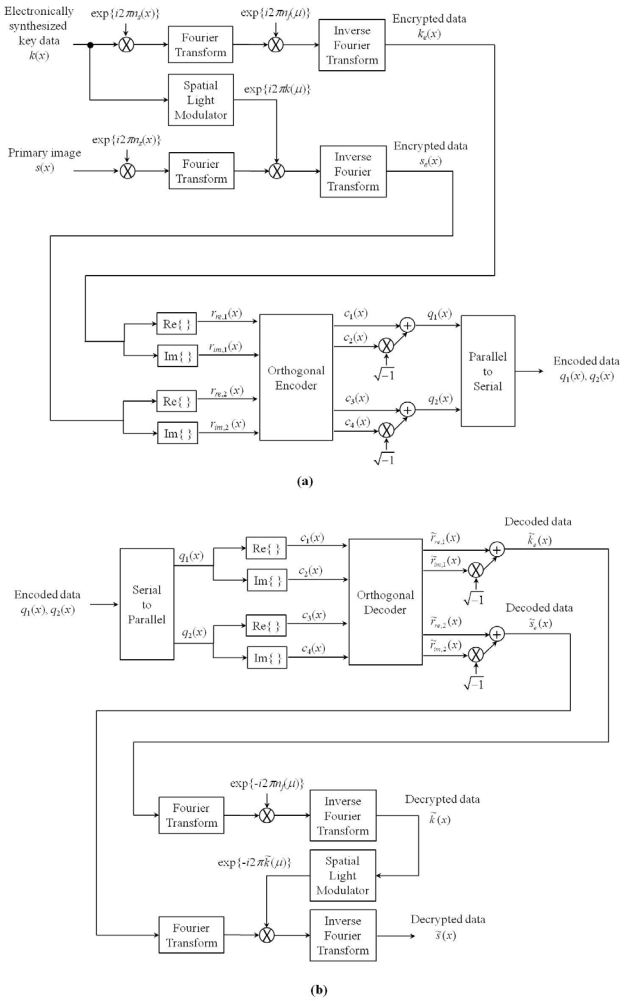

Fig. 2. Security-enhanced DRPE scheme with orthogonally encoded image and electronically synthesized key data for (a) encryption and (b) decryption.

are randomly generated at the encryption stage and unknown at the decryption stage. In this letter, we provide detailed procedures for encryption and decryption of the proposed DRPE scheme, and through simulation for DRPE, we verify that the proposed scheme can improve the security of DRPE systems.

Optical encryption has many advantages such as the parallel processing of optical systems, the fast processing time, and the data handling in various domains. In DRPE, two separated random phase masks are used for encryption. For the ease of understanding, we consider one-dimensional signal only. Encryption procedure is presented in Fig. 1(a). Let $s(x)$ be the primary data. Then, for encryption, we use two uniformly distributed random noises over [0, 1] which are $n_s(x)$ in spatial domain and $n_f(\mu)$ in spatial frequency domain. Firstly, we multiply the random phase mask, $\exp[\mathrm{i}2\pi n_s(x)]$ by the primary data, $s(x)$ in spatial domain. Secondly, the data pass through lens 1 which means Fourier transform of $s(x)\exp[\mathrm{i}2\pi n_s(x)]$, and are multiplied by the random phase mask $\exp[\mathrm{i}2\pi n_f(\mu)]$ in spatial frequency domain. Finally, the inverse Fourier transform of these data can be recorded through lens 2. In other words, the encrypted data by DRPE, $s_e(x)$ is a complex-valued function[4]

$$s_e(x) = \Im^{-1}\left[\Im\left\{s(x)\exp\left[\mathrm{i}2\pi n_s(x)\right]\right\}\exp\left\{\mathrm{i}2\pi n_f(\mu)\right\}\right], \quad (1)$$

where $\Im$ and $\Im^{-1}$ denote Fourier transform and inverse Fourier transform, respectively. Since the encrypted data are complex-valued functions, they have amplitude and phase, that is, $s_e(x) = |s_e(x)|\exp[\mathrm{i}\phi_e(x)]$.

However, unless the encryption stage, the only complex conjugate of the physical key phase mask in spatial frequency domain, $\exp[\mathrm{i}2\pi n_f(\mu)]$ is used at the decryption stage of DRPE as shown in Fig. 1(b). Thus, the decryption is implemented by multiplying the encrypted data by complex conjugate of the physical key phase mask used for encryption as[4]

$$\tilde{s}(x) = \left|\Im^{-1}\left\{\Im\left[s_e(x)\right]\exp\left[-\mathrm{i}2\pi n_f(\mu)\right]\right\}\right|. \quad (2)$$

Figure 2(a) shows the procedure for encryption of the enhanced DRPE scheme with orthogonally encoded image and the electronically synthesized key data. Firstly the electronically synthesized key data $k(x)$ are randomly generated by uniform distribution with support [0, 1], which can be frequently updated, and then the electronically synthesized phase mask $\exp[\mathrm{i}2\pi k(\mu)]$ is made by SLM, which is used for encryption of the primary image data $s(x)$. Thus, the encrypted data of the primary image $s_e(x)$ are obtained. The electronically synthesized key data are also encrypted with the physical key phase mask $\exp[\mathrm{i}2\pi n_f(\mu)]$. It is noted that when the primary image and the electronically synthesized key data are independently encrypted with DRPE, the first phase mask $\exp[\mathrm{i}2\pi n_s(x)]$ is the same, but the second phase masks (i.e., the physical and the electronically synthesized key phase masks) are different from

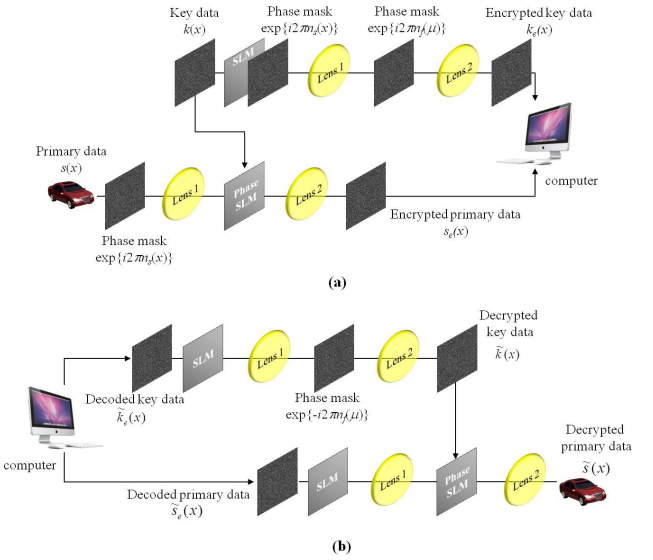

Fig. 3. Optical setup of security-enhanced DRPE scheme: (a) encryption and (b) decryption.

each other. The reason why we focus on the second phase masks in the DRPE system is that only the second phase masks are used for decryption (Fig. 2(b)). The encrypted data of the electronically synthesized key and primary image $k_e(x)$ and $s_e(x)$ are decomposed into real and imaginary parts, that is, $r_{re,1}(x)$, $r_{im,1}(x)$, $r_{re,2}(x)$, and $r_{im,2}(x)$, respectively. Then, the four real values are encoded together with orthogonal encoding as[19]

$$\begin{bmatrix} c_1(x) \\ c_2(x) \\ c_3(x) \\ c_4(x) \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} r_{re,1}(x) \\ r_{im,1}(x) \\ r_{re,2}(x) \\ r_{im,2}(x) \end{bmatrix} = \begin{bmatrix} \frac{1}{4}\left(r_{re,1}(x)+r_{im,1}(x)+r_{re,2}(x)+r_{im,2}(x)\right) \\ \frac{1}{4}\left(r_{re,1}(x)-r_{im,1}(x)+r_{re,2}(x)-r_{im,2}(x)\right) \\ \frac{1}{4}\left(r_{re,1}(x)+r_{im,1}(x)-r_{re,2}(x)-r_{im,2}(x)\right) \\ \frac{1}{4}\left(r_{re,1}(x)-r_{im,1}(x)-r_{re,2}(x)+r_{im,2}(x)\right) \end{bmatrix}, \tag{3}$$

where we employ the Hadamard matrix of order 4, which is given as [1 1 1 1; 1 −1 1 −1; 1 1 −1 −1; 1 −1 −1 1]. Finally, the complex encoded data $q_1(x)$ and $q_2(x)$ are made from the real-valued data $c_1(x)$, $c_2(x)$, $c_3(x)$, and $c_4(x)$, respectively (Fig. 2(a)).

Figure 2(b) shows the procedure for decryption of the enhanced DRPE scheme with orthogonally encoded image and electronically synthesized key data. Firstly the complex encoded data $q_1(x)$ and $q_2(x)$ are separated into the real and imaginary parts, that is, $c_1(x)$, $c_2(x)$, $c_3(x)$, and $c_4(x)$, respectively. Then, the four real values are decoded with orthogonal decoding as[19]

$$\begin{bmatrix} \tilde{r}_{re,1}(x) \\ \tilde{r}_{im,1}(x) \\ \tilde{r}_{re,2}(x) \\ \tilde{r}_{im,2}(x) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} c_1(x) \\ c_2(x) \\ c_3(x) \\ c_4(x) \end{bmatrix} = \begin{bmatrix} c_1(x)+c_2(x)+c_3(x)+c_4(x) \\ c_1(x)-c_2(x)+c_3(x)-c_4(x) \\ c_1(x)+c_2(x)-c_3(x)-c_4(x) \\ c_1(x)-c_2(x)-c_3(x)+c_4(x) \end{bmatrix}, \tag{4}$$

where it is noted that the Hadamard matrix used for encoding should be equally used for perfect decoding. Using the real decoded data $\tilde{r}_{re,1}(x)$, $\tilde{r}_{im,1}(x)$, $\tilde{r}_{re,2}(x)$, and $\tilde{r}_{im,2}(x)$, the complex decoded data $\tilde{k}_e(x)$ and $\tilde{s}_e(x)$ are obtained as $\tilde{k}_e(x) = \tilde{r}_{re,1}(x) + \mathrm{i}\tilde{r}_{im,1}(x)$, and $(x)+ \mathrm{i}\tilde{r}_{im.2}(x)$, $(x)+ \mathrm{i}\tilde{r}_{im.2}(x)$, respectively, where $\tilde{k}_e(x)$ and $\tilde{s}_e(x)$ represent the decoded data for the electronically synthesized key and the primary image, respectively. The complex decoded data for the electronically synthesized key are decrypted using the complex conjugate of the physical key phase mask $\exp[-\mathrm{i}2\pi n_f(\mu)]$. Then the decrypted data $\tilde{k}(x)$ are obtained, and the complex conjugate of the electronically synthesized key phase mask $\exp[-\mathrm{i}2\pi\tilde{k}(\mu)]$ is obtained by using the decrypted data in SLM. Finally, the complex decoded data for the primary image are decrypted with the obtained key phase mask, and the decrypted data for the primary image $\tilde{s}(x)$ are obtained. It is noted that the key phase mask used for decryption of the electronically synthesized key data is fixed and given, but the key phase mask used for decryption of the primary image is randomly generated by the decrypted data for the electronically synthesized key. Figures 3(a) and (b) show the optical setup of encryption and decryption of the enhanced DRPE scheme, respectively. In the proposed scheme, the modulated error of SLM is a critical issue. Since SLM is used to generate the key phase mask for decryption of the primary data, the modulated error of SLM can cause the error of key phase information used for decryption, and hence the decrypted primary data can be corrupted by the modulated error. Therefore, the reliability of SLM should be required for the proposed scheme. Also, SLMs for random phase masks should be the same since 4f system which has unity magnification ratio is used in DRPE.

For simulation of DRPE, we consider the electronically synthesized key data and the primary image with 500(H)×500(V) pixels as shown in Figs. 4(a) and (b), respectively, where the electronically synthesized key data are randomly generated by uniform distribution

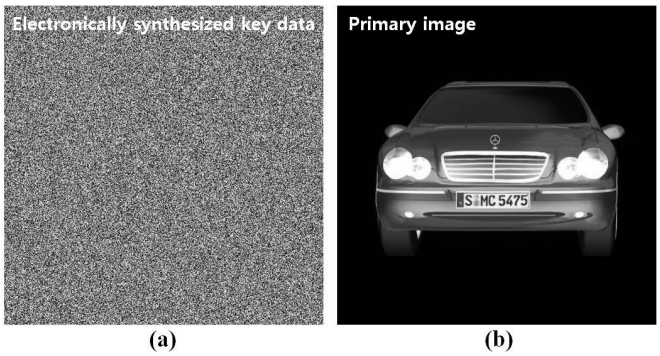

Fig. 4. Two images used for simulation: (a) electronically synthesized key data and (b) primary image.

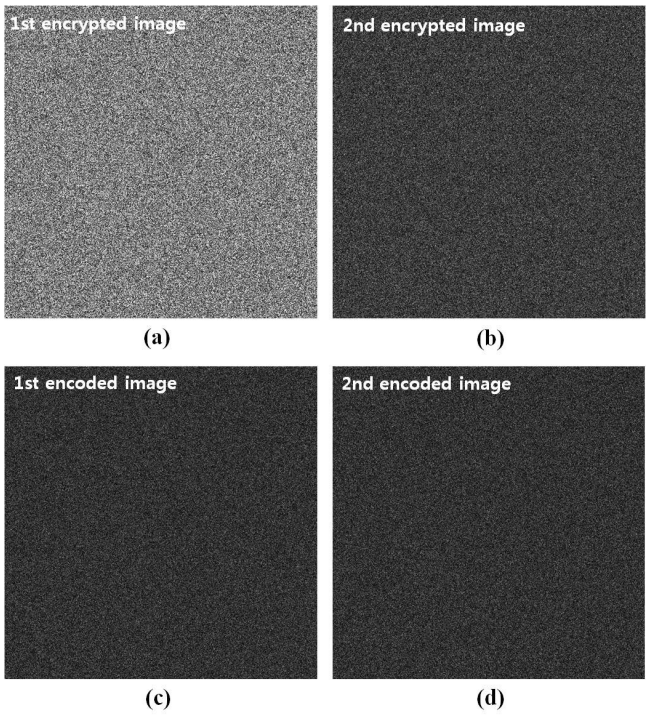

Fig. 5. Simulation results for encryption of the proposed DRPE scheme: (a) the 1st encrypted image, (b) the 2nd encrypted image, (c) the 1st encoded image, and (d) the 2nd encoded image.

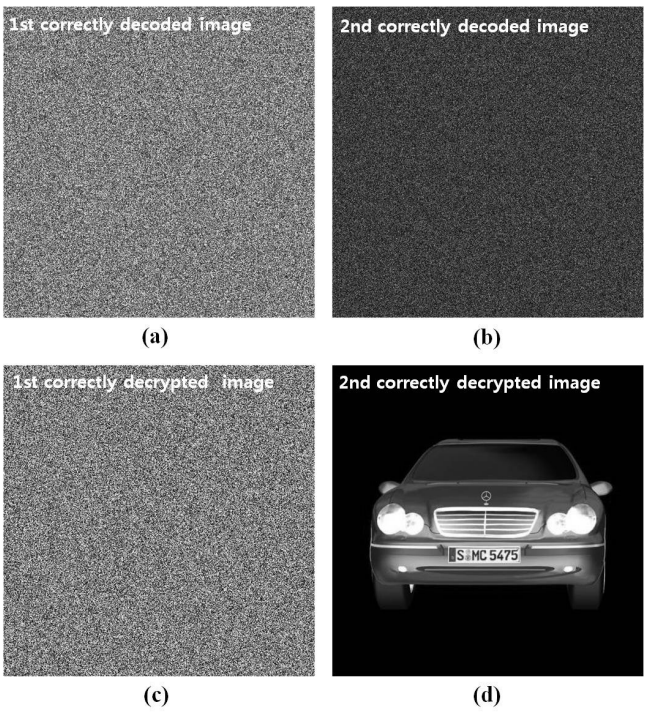

Fig. 6. Simulation results for correct decoding and decryption of the proposed DRPE scheme: (a) the 1st decoded image, (b) the 1st decoded image, (c) the 1st decrypted image, and (d) the 2nd decrypted image.

with support [0, 1]. Figure 5 shows simulation results for encryption of the enhanced DRPE scheme with orthogonally encoded image and electronically synthesized key data. The 1st and 2nd encrypted data in Figs. 5(a) and (b) correspond to the encrypted data of the electronically synthesized key and the primary image, respectively, that is, $k_e(x)$ and $s_e(x)$ in Fig. 2(a). The 1st and 2nd encoded data in Figs. 5(c) and (d) are obtained by orthogonally encoding the 1st and 2nd encrypted data, and those correspond to $q_1(x)$ and $q_2(x)$ in Fig. 2(a).

Figure 6 shows simulation results for correct decoding and decryption of the proposed DRPE scheme. For correct decoding and decryption, the orthogonal decoding of encoded data is done, and then the 1st decoded data in Fig. 6(a) corresponding to $\tilde{k}_e(x)$ in Fig. 2(b) are decrypted by DRPE decryption using complex conjugate of the physical key phase mask to obtain the electronically synthesized key data. The obtained key data are shown in Fig. 6(c) which are exactly the same as the data in Fig. 4(a), and those are used for DRPE decryption of the 2nd decoded data in Fig. 6(b) corresponding to $\tilde{s}_e(x)$ in Fig. 2(b). Thus, the correctly decrypted data for the primary image are obtained as shown in Fig. 6(d).

Figure 7 shows simulation results for wrong decoding and decryption of the proposed DRPE scheme. Wrong decoding means that no decoding is performed before DRPE decryption, and thus the results for wrong decoding are the same as the encoded data in Figs. 5(c) and (d). Also, wrong decryption means that only the complex conjugate of the physical key phase mask is used for the DRPE decryption of the 1st and 2nd decoded data, where it is noted that complex conjugates of the physical and electronically synthesized key phase masks are required for the correct DRPE decryption of the 1st and 2nd decoded data, respectively. Figures 7(a) and (b) demonstrate that all the decrypted images seem to be noise-like image when wrong decoding and decryption are employed although complex conjugate of the physical key phase mask is known.

Figure 8 shows simulation results for correct decoding but wrong decryption of the proposed DRPE scheme. The results for correct decoding have been shown in Figs. 6(a) and (b). The meaning of wrong decryption

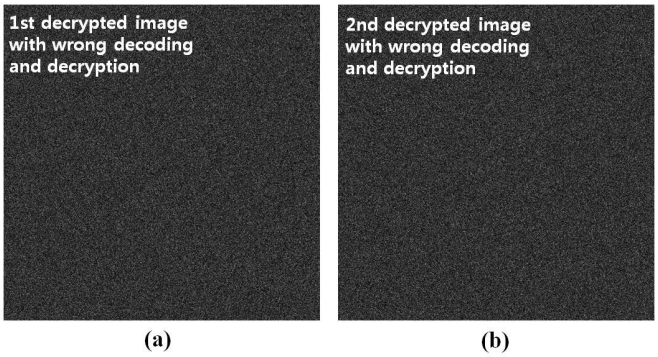

Fig. 7. Simulation results for wrong decoding and decryption of the proposed DRPE scheme: (a) the 1st decrypted image and (b) the 2nd decrypted image.

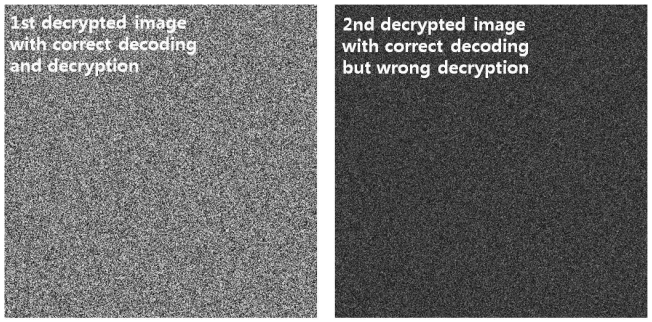

Fig. 8. Simulation results for correct decoding but wrong decryption of the proposed DRPE scheme: (a) the 1st decrypted image and (b) the 2nd decrypted image.

is the same as in Fig. 7. In Fig. 8(a), the 1st decrypted data are correct since the perfect orthogonal decoding and DRPE decryption are performed. Thus, the image in Fig. 8(a) is perfectly the same as that of the electronically synthesized key data shown in Fig. 4(a). However, the 2nd decrypted image shown in Fig. 8(b) seems to be noise-like image because the DRPE decryption is done with the wrong key phase mask (i.e., complex conjugate of the physical key phase mask, not the electronically synthesized key phase mask) even though the orthogonal decoding is correct. The results shown in Figs. 7 and 8 verify that the proposed DRPE scheme can enhance the security by using the electronically synthesized key.

In conclusion, we propose the enhanced DRPE scheme with orthogonally encoded image and electronically synthesized key data in order to resolve the fundamental security problem of DRPE technique. In the proposed scheme, the introduction of the electronically synthesized key enables the frequent updating of the key phase mask used for encryption and decryption, and the use of the orthogonal encoding technique to encode the image and electronically synthesized key data can improve the security of both data. The simulation results show that the proposed scheme produces noise-like images when decoding or decryption is incorrectly performed, even though complex conjugate of the physical key phase mask is known. Therefore, the proposed scheme can be regarded as one of the powerful encryption techniques.

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea Funded by the Ministry of Science, ICT & Future Planning (No. 2011-0030079) and the Ministry of Education (No. NRF-2013R1A1A2057549).

References

1. P. Refregier and B. Javidi, Opt. Lett. **20,** 767 (1995).
2. E. Tajahuerce and B. Javidi, Appl. Opt. **39,** 6595 (2000).
3. H. Y. Tu, J. S. Chiang, J. W. Chou, and C. J. Cheng, Jpn. J. Appl. Phys. **47,** 8838 (2008).
4. E. Perez-Cabre, M. Cho, and B. Javidi, Opt. Lett. **36,** 22 (2011).
5. M. Cho and B. Javidi, Opt. Lett. **38,** 3198 (2013).
6. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25,** 887 (2000).
7. M. Joshi, Chandrashakher, and K. Singh, Opt. Commun. **279,** 35 (2007).
8. M. Joshi, C. Shakher, and K. Singh, Opt. Commun. **283,** 2496 (2010).
9. Y. Frauel, A. Castro, T. Naughton, and B. Javidi, Opt. Express **15,** 10253 (2007).
10. T. Nomura and B. Javidi, Appl. Opt. **39,** 4783 (2000).
11. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, Appl. Opt. **46,** 6641 (2007).
12. M. Singh, A. Kumar, and K. Singh, Opt. Laser Technol. **40,** 619 (2008).
13. T. Sarkadi and P. Koppa, Appl. Opt. **51,** 745 (2012).
14. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, Opt. Express **18,** 13772 (2010).
15. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, Opt. Commun. **259,** 532 (2006).
16. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, Appl. Opt. **40,** 2310 (2001).
17. W. Chen and X. Chen, Opt. Express **18,** 27095 (2010).
18. I. H. Lee and M. Cho, J. Opt. Soc. Korea **18,** 129 (2014).
19. I. H. Lee and M. Cho, J. Opt. Soc. Korea **18,** 201 (2014).
20. O. Matoba and B. Javidi, Opt. Lett. **24,** 762 (1999).
21. W. Chen, B. Javidi, and X. Chen, Adv. Opt. Photon. **6,** 120 (2014).
22. O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, Proc. IEEE J. **97,** 1128 (2009).
23. D. Lu and W. Jin, Chin. Opt. Lett. **9,** 021002 (2011).
24. J. J. Sylvester, Philos. Mag. **34,** 461 (1867).