Journal of the Optical Society of Korea
Vol. 18, No. 3, June 2014, pp. 201-206

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2014.18.3.201

Double Random Phase Encryption using Orthogonal Encoding for Multiple-Image Transmission

In-Ho Lee and Myungjin Cho*

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

(Received May 9, 2014 : June 3, 2014 : accepted June 10, 2014)

In this paper we extend double random phase encryption (DRPE) using orthogonal encoding from single-image transmission to multiple-image transmission. The orthogonal encoding for multiple images employs a larger Hadamard matrix than that for a single image, which can improve security. We provide a scheme for DRPE with an orthogonal codec, and a method for orthogonal encoding/decoding for multiple-image transmission. Finally, simulation results verify that the DRPE using orthogonal encoding for multiple images is more secure than both the conventional DRPE and the DRPE using orthogonal encoding for a single image.

Keywords : Multiple-image transmission, Optical encryption, Double-random-phase encryption, Orthogonal encoding
OCIS codes : (060.4785) Optical security and encryption; (200.4560) Optical data processing

I. INTRODUCTION

A significant issue in transmitting private or confidential information is information security. Encryption techniques for secure data transmission have been well developed [1-26], and lots of research has focused on optical encryption [3-26]. One widely used optical technique is double random phase encryption (DRPE) [3]. It provides high encryption speed, but requires updating of the key phase masks [4]. To improve the security of DRPE, fractional Fourier transform has been adopted in DRPE systems [25], but it requires much more information in the keys for encryption and decryption. An increase in the key information can make the DRPE systems more complicated, so DRPE using orthogonal encoding has been proposed for single-image transmission [26]. The orthogonal encoding technique for single-image transmission employs only simple, linear operations based on the Hadamard matrix of order 2 with the orthogonality property [27]. Thus, the use of orthogonal encoding can enhance the security of DRPE at the cost of a little complexity.

In this paper we extend DRPE using orthogonal encoding from single-image to multiple-image transmission. The orthogonal encoding for multiple images uses a larger Hadamard matrix than that for a single image, and hence is more secure. We provide a scheme for DRPE with an orthogonal codec for multiple-image transmission. Furthermore, we show simulation results verifying that the multiple images encrypted by DRPE using orthogonal encoding are not correctly decrypted even when the key information used in DRPE is known.

The paper is organized as follows. Section II presents the basic concept of DRPE. Then, DRPE using orthogonal encoding for multiple-image transmission is described in Section III. To verify this optical encryption method, simulation results produced by DRPE using orthogonal encoding are provided in Section IV. Finally, we conclude with a summary.

II. DOUBLE RANDOM PHASE ENCRYPTION TECHNIQUE

DRPE, an optical encryption technique, can provide high encryption and decryption speed. In addition, it can be implemented simply. It uses two random phase noises (i.e., random phase masks) for the encryption process. Then, noise like encrypted data can be obtained. For decryption, the

*Corresponding author: mjcho@hknu.ac.kr

Color versions of one or more of the figures in this paper are available online.

key random phase mask is convolved with the encrypted data. To understand the DRPE concept, we consider only one-dimensional data. Let us assume that the primary data is $s(x)$ and the two random phase noise signals for encryption, $n_s(x)$ in the spatial domain and $n_f(\mu)$ in the spatial frequency domain, are uniformly distributed over [0, 1]. Figure 1(a) illustrates an experimental optical setup for DRPE. Two imaging lenses with focal length f are used for the Fourier transform and inverse Fourier transform, respectively. For encryption, first the original data is multiplied by random noise, $\exp[i2\pi n_s(x)]$, in the spatial domain. Through the first imaging lens $\Im\{s(x)\exp[i2\pi n_s(x)]\}$ can be obtained, where $\Im$ indicates the Fourier transform. Then this is multiplied by random noise, $\exp[i2\pi n_f(\mu)]$ (the Fourier transform of $h(x)$), in the spatial frequency domain. After passing through the second imaging lens, the data encrypted (as a complex-valued function) by DRPE, $s_e(x)$, can be generated as the following [11]:

$$s_e(x) = \Im^{-1}\left[\Im\left\{s(x)\exp\left[i2\pi n_s(x)\right]\right\}\exp\left\{i2\pi n_f(\mu)\right\}\right] \tag{1}$$

where $\Im^{-1}$ indicates the inverse Fourier transform. This encrypted data can be separated into amplitude and phase, i.e. $s_e(x)=|s_e(x)|\exp[i\phi_e(x)]$ because of the characteristics of a complex-valued function.

For decryption, the complex conjugate of the key information (i.e. the Fourier transform of $h(x)$) is multiplied by the encrypted data as shown in Fig. 1(b). Therefore, the decrypted data can be obtained from the following equation [11]:

$$\tilde{s}(x) = \left|\Im^{-1}\left[\Im\left[s_e(x)\right]\exp\left\{-i2\pi n_f(\mu)\right\}\right]\right| \tag{2}$$

III. DOUBLE RANDOM PHASE ENCRYPTION USING ORTHOGONAL ENCODING

3.1. Procedure for DRPE using Orthogonal Encoding

In this paper we assume that K primary images are transmitted. Figures 2(a) and 2(b) depict the schemes for DRPE using orthogonal encoding for encryption and decryption, respectively. As shown in Fig. 2(a), the primary images $s_1(x)$, $s_2(x)$, ⋯, $s_K(x)$ are sequentially encrypted by DRPE with the same key information (i.e. the same phase masks). Then the encrypted data $s_{e,1}(x)$, $s_{e,2}(x)$, ⋯, $s_{e,K}(x)$ are obtained from the K primary images. Note that the encrypted data are complex-valued functions. By a serial-to-parallel converter, the encrypted data are converted from serial format to parallel format. Then each encrypted datum is separated into real and imaginary parts. The $2K$ values $r_{re,1}(x)$, $r_{im,1}(x)$, ⋯ , $r_{re,K}(x)$, $r_{im,K}(x)$ are encoded together with the orthogonal encoding technique, which will be introduced in Section 3.2. The reason why the real and imaginary parts are encoded is that these parts are independent from each other. Finally, the complex encoded data $q_1(x)$, $q_2(x)$, ⋯ , $q_{M/2}(x)$ are produced from the encoded real values $c_1(x)$, $c_2(x)$, ⋯ , $c_M(x)$ and successively transmitted after the parallel-to-serial converter, where $M = 2^{\lceil \log_2 2K \rceil}$ and $\lceil\,\rceil$ indicates the ceiling operation.

As shown in Fig. 2(b), to correctly decrypt the orthogo-

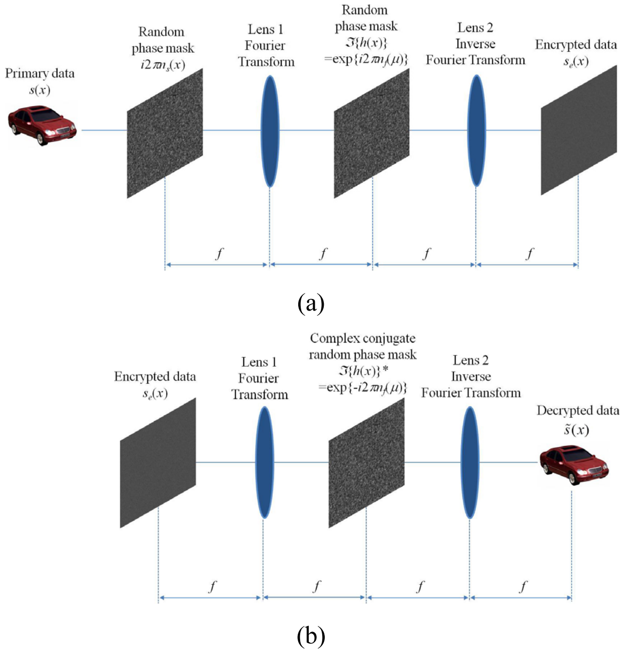


FIG. 1. Schematic setup of (a) encryption and (b) decryption for DRPE.

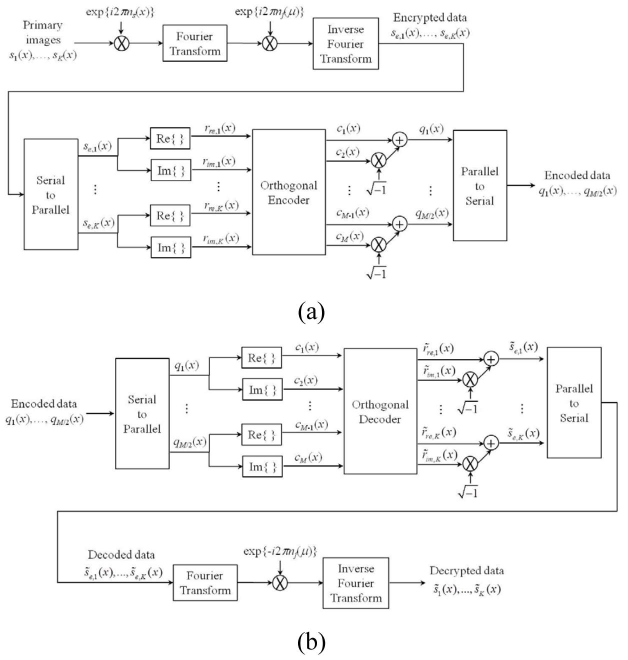


FIG. 2. Scheme for DRPE using orthogonal encoding: (a) encryption and (b) decryption.

nally encoded data, first the encoded data are converted from serial format to parallel format and decomposed into real and imaginary components. Then the real encoded data are decoded with the orthogonal matrix used in the encoder. From the real decoded data $\tilde{r}_{re,1}(x)$, $\tilde{r}_{im,1}(x)$, ⋯ , $\tilde{r}_{re,K}(x)$, $\tilde{r}_{im,K}(x)$ the complex decoded data $\tilde{s}_{e,1}(x)$, $\tilde{s}_{e,2}(x)$, ⋯ , $\tilde{s}_{e,K}(x)$ are found, and then sequentially decrypted with the DRPE decryption technique after the parallel-to-serial converter. Finally, the K decrypted data $\tilde{s}_1(x)$, $\tilde{s}_2(x)$, ⋯ , $\tilde{s}_K(x)$ are obtained.

3.2. Orthogonal Encoding and Decoding Technique

For orthogonal encoding and decoding of multiple images, we use the Hadamard matrix of order 2^n, denoted by $\mathbf{H}_{2^n \times L}$, with the following orthogonality property [27]:

$$\mathbf{H}_{2^n \times L}^T \mathbf{H}_{2^n \times L} = 2^n \mathbf{I}_{L \times L} \tag{3}$$

where n and L are positive integers, $2^n \geq L$, $\mathbf{I}_{L\times L}$ represents the $L\times L$ identity matrix, and $\mathbf{H}^T$ is the transpose of $\mathbf{H}$. The square Hadamard matrix of order 2^n is generated as follows:

$$\mathbf{H}_{2^n \times 2^n} = \begin{bmatrix} \mathbf{H}_{2^{n-1}\times 2^{n-1}} & \mathbf{H}_{2^{n-1}\times 2^{n-1}} \\ \mathbf{H}_{2^{n-1}\times 2^{n-1}} & -\mathbf{H}_{2^{n-1}\times 2^{n-1}} \end{bmatrix} \tag{4}$$

where $\mathbf{H}_2$=[1 1; 1 -1]. On the other hand, when $2^{n-1} < L < 2^n$, the non-square Hadamard matrix is obtained by choosing any L columns of the square Hadamard matrix of order 2^n, $\mathbf{H}_{2^n \times 2^n}$.

By using the Hadamard matrix in the orthogonal encoder, the real and imaginary components of the encrypted data for K images are encoded as follows:

$$\begin{bmatrix} c_1(x) \\ c_2(x) \\ \vdots \\ c_{M-1}(x) \\ c_M(x) \end{bmatrix} = \frac{1}{M} \mathbf{H}_{M\times 2K} \begin{bmatrix} r_{re,1}(x) \\ r_{im,1}(x) \\ \vdots \\ r_{re,K}(x) \\ r_{im,K}(x) \end{bmatrix} \tag{5}$$

where $M = 2^{\lceil \log_2 2K \rceil}$, $c_m(x)$ is the mth encoded datum, and $r_{re,k}(x)$ and $r_{im,k}(x)$ are the real and imaginary parts of the encrypted data for the kth image, respectively. $1/M$ is a normalization factor.

In the orthogonal decoder, the real and imaginary components of the encoded data $c_1(x)$, $c_2(x)$, ⋯ , $c_M(x)$ are decoded by using the Hadamard matrix of the encoder as follows:

$$\begin{bmatrix} \tilde{r}_{re,1}(x) \\ \tilde{r}_{im,1}(x) \\ \vdots \\ \tilde{r}_{re,K}(x) \\ \tilde{r}_{im,K}(x) \end{bmatrix} = \mathbf{H}_{M\times 2K}^T \begin{bmatrix} c_1(x) \\ c_2(x) \\ \vdots \\ c_{M-1}(x) \\ c_M(x) \end{bmatrix} \tag{6}$$

where $\tilde{r}_{re,k}(x)$ and $\tilde{r}_{im,k}(x)$ are the decoded data for the kth image. By inserting Eq. (5) into Eq. (6), we obtain $\tilde{r}_{re,k}(x) = r_{re,k}(x)$ and $\tilde{r}_{im,k}(x) = r_{im,k}(x)$.

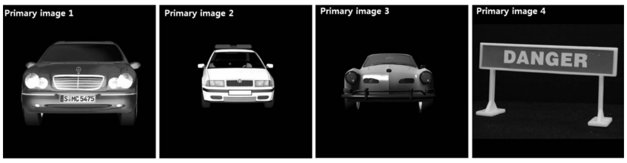
The orthogonal encoder and decoder consist of only simple linear operations, as described in Eqs. (4)-(6). Hence, the addition of the orthogonal encoder and decoder to the DRPE system does not require any high cost or effort.

IV. SIMULATION RESULTS

For performance evaluation of DRPE using orthogonal encoding, we use four primary images with 500 (H)×500 (V) pixels as shown in Fig. 3. We consider transmissions of two, three, and four images. For two-, three-, and four-image transmissions the primary images in Figs. 3(a) and 3(b), Figs. 3(a)-3(c), and Figs. 3(a)-3(d) are used respectively, and the following Hadamard matrices are used respectively.

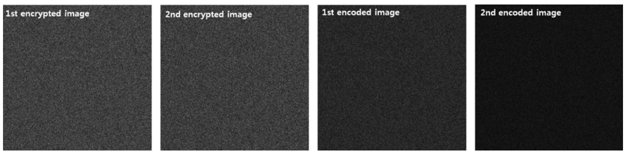
$$\mathbf{H}_{4\times 4} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{7}$$

$$\mathbf{H}_{8\times 6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix} \tag{8}$$



(a) (b) (c) (d)

FIG. 3. The four primary images.

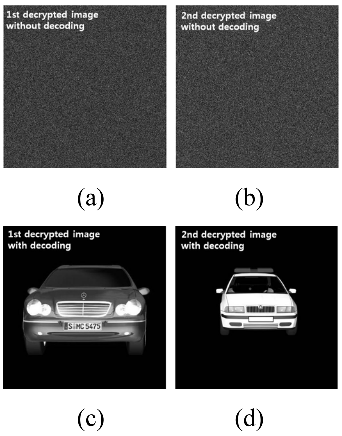


(a) (b) (c) (d)

FIG. 4. Simulation results for encryption by DRPE using orthogonal encoding for two images: (a) the first and (b) the second encrypted images, and (c) the first and (d) the second encoded images.

$$\mathbf{H}_{8\times8}=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix}\tag{9}$$

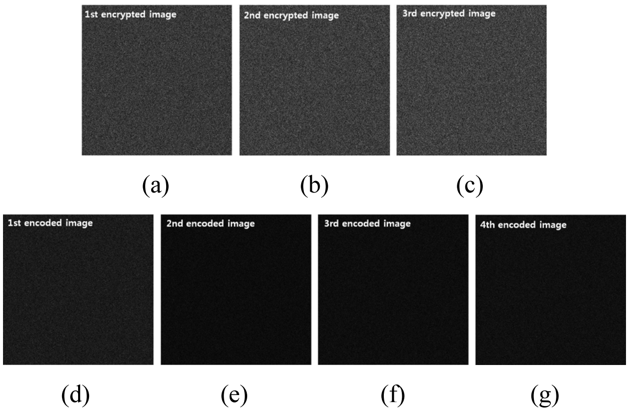
Figures 4-6 show the encrypted and encoded images for two-, three-, and four-image transmissions respectively. These figures indicate that the images encrypted by DRPE and encoded by orthogonal encoding are perfectly encrypted, and thus look like noise. It is noted that for three-image transmission, four encoded images are generated because the order of Hadamard matrix is eight. Figures 7-9 show


1st decrypted image without decoding
2nd decrypted image without decoding
1st decrypted image with decoding
2nd decrypted image with decoding
S·MC 5475

(a) (b)

(c) (d)

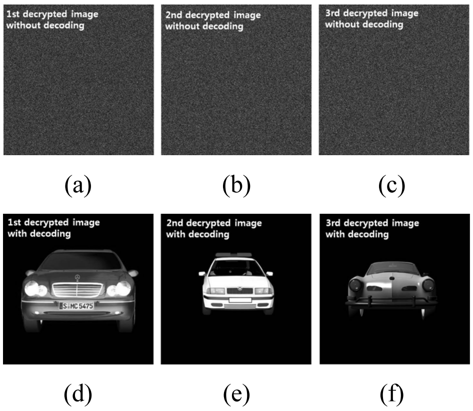
FIG. 7. Simulation results for decryption by DRPE using orthogonal encoding for two images: (a) the first and (b) the second decrypted images without decoding, and (c) the first and (d) the second decrypted images with decoding.



(a) (b) (c)

(d) (e) (f) (g)

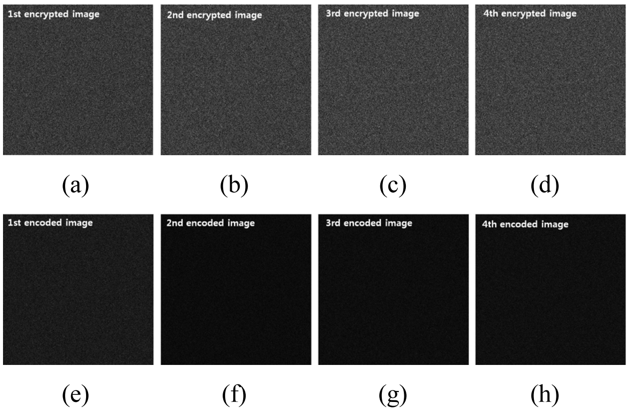
FIG. 5. Simulation results for encryption by DRPE using orthogonal encoding for three images: (a) the first, (b) the second, and (c) the third encrypted images, and (d) the first, (e) the second, (f) the third, and (g) the fourth encoded images.


1st decrypted image without decoding
2nd decrypted image without decoding
3rd decrypted image without decoding
1st decrypted image with decoding
2nd decrypted image with decoding
3rd decrypted image with decoding
S·MC 5475

(a) (b) (c)

(d) (e) (f)

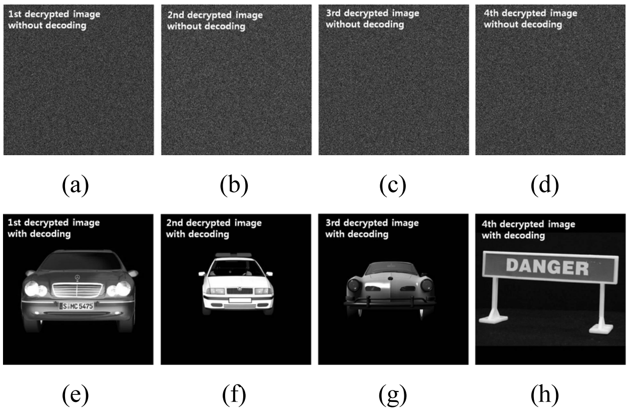
FIG. 8. Simulation results for decryption by DRPE using orthogonal encoding for three images: (a) the first, (b) the second, and (c) the third decrypted images without decoding, and (d) the first, (e) the second, and (f) the third decrypted images with decoding.



(a) (b) (c) (d)

(e) (f) (g) (h)

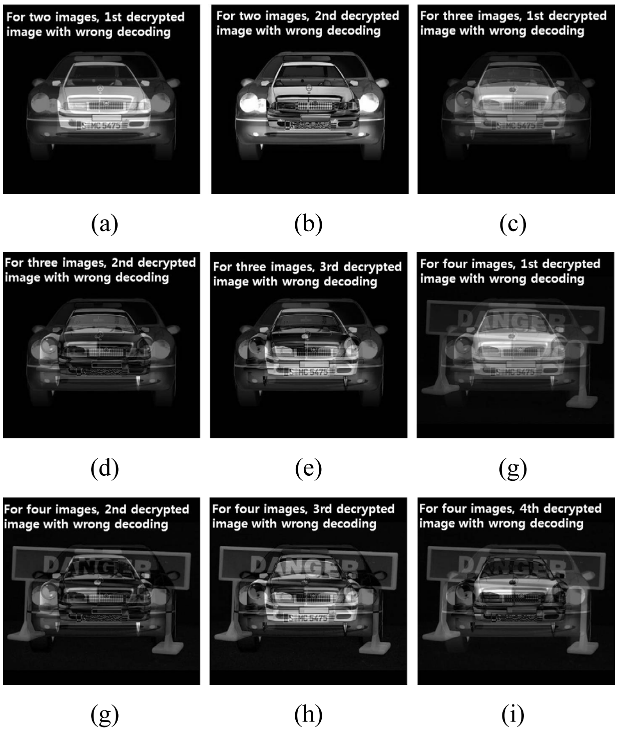
FIG. 6. Simulation results for encryption by DRPE using orthogonal encoding for four images: (a) the first, (b) the second, (c) the third, and (d) the fourth encrypted images, and (e) the first, (f) the second, (g) the third, and (h) the fourth encoded images.


1st decrypted image without decoding
2nd decrypted image without decoding
3rd decrypted image without decoding
4th decrypted image without decoding
1st decrypted image with decoding
2nd decrypted image with decoding
3rd decrypted image with decoding
4th decrypted image with decoding
S·MC 5475
DANGER

(a) (b) (c) (d)

(e) (f) (g) (h)

FIG. 9. Simulation results for decryption by DRPE using orthogonal encoding for four images: (a) the first, (b) the second, (c) the third, and (d) the fourth decrypted images without decoding, and (e) the first, (f) the second, (g) the third, and (h) the fourth decrypted images with decoding.


For two images, 1st decrypted image with wrong decoding
For two images, 2nd decrypted image with wrong decoding
For three images, 1st decrypted image with wrong decoding
For three images, 2nd decrypted image with wrong decoding
For three images, 3rd decrypted image with wrong decoding
For four images, 1st decrypted image with wrong decoding
For four images, 2nd decrypted image with wrong decoding
For four images, 3rd decrypted image with wrong decoding
For four images, 4th decrypted image with wrong decoding

(a) (b) (c)

(d) (e) (g)

(g) (h) (i)

FIG. 10. Simulation results for decryption by DRPE using orthogonal encoding when decoding for the single-image transmission is used: (a) the first and (b) the second decrypted images for two-image transmission, (c) the first, (d) the second, and (e) the third decrypted images for three-image transmission, and (f) the first, (g) the second, (h) the third, and (i) the fourth decrypted images for four-image transmission.

the decrypted images, with and without decoding, for two-, three-, and four-image transmissions respectively, when the key information of DRPE is perfectly known for decryption. In the case of no decoding, the complex encoded data are not decoded with the orthogonal decoder, but directly decrypted. Thus, $\tilde{s}_{e,k}(x) = q_k(x)$ for $k=1,2,\cdots, K$. From these figures, it is seen that the decrypted images without decoding resemble the encrypted images, even though perfect key information was applied for decryption. On the other hand, when the decryption is done with orthogonal decoding and perfect key information, the decrypted images in Fig. 3 match the primary images perfectly.

Figures 10(a)-10(i) show the decrypted images for two-, three-, and four-image transmissions respectively, when perfect key information of DRPE is used for decryption but the wrong decoding is employed. For the wrong decoding method we use the Hadamard matrix of order 2 that was adopted for decryption of the single-image transmission [26]. For encoding of two-, three-, and four-image transmissions, we use the Hadamard matrices of order 4, 8, and 8, respectively. Thus the Hadamard matrices used for encoding and decoding do not match. As seen in these figures, the decrypted images somewhat include the primary images, but overlapped, and image recognition becomes worse as the number of transmitted images increases, i.e. the size of the Hadamard matrix increases.

TABLE 1. MSE results of DRPE using orthogonal encoding when incorrect decoding is used

Cases	MSE for two-image transmission	MSE for three-image transmission	MSE for four-image transmission
Primary image1 and the 1st decrypted image	1001.4	1660.2	1806.8
Primary image2 and the 2nd decrypted image	3940.4	4060.7	4211.8
Primary image3 and the 3rd decrypted image	-	2277.2	2517.3
Primary image4 and the 4th decrypted image	-	-	2517.3

To quantify the difference between the primary images in Figs. 3(a)-3(d) and the decrypted images with incorrect decoding in Figs. 10(a)-10(i) respectively, the mean square error (MSE) is evaluated. MSE between the *k*th primary and decrypted images is calculated as follows:

$$MSE_k = \frac{1}{X}\sum_{x=1}^{X}\left|s_k(x) - \tilde{s}_k(x)\right|^2 \tag{10}$$

where $X=500\times500$, and $s_k(x)$ and $\tilde{s}_k(x)$ denote the *k*th primary and decrypted data respectively, as shown in Fig. 2. Assuming that the image pixel value's integer range is from 0 to 255, the MSE results are obtained as shown in Table 1. From the MSE results it is observed that the MSE increases with the number of transmitted images. Therefore, we can expect a significant improvement in information security by encoding many more images together.

V. CONCLUSIONS

We present a DRPE technique using orthogonal encoding for multiple-image transmission. Particularly we provide a scheme for DRPE using orthogonal encoding for encryption and decryption as well as the method for orthogonal encoding and decoding with the Hadamard matrix. From simulation results we verify that DRPE using orthogonal encoding for multiple-image transmission is more powerful than that for the single-image transmission, in terms of security. Furthermore, since the orthogonal encoder and decoder consist of only simple linear operations, the DRPE system using orthogonal encoding for multiple-image transmission can be implemented with low cost and effort.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R 1A1A2057549).

REFERENCES

1. S. Tsuji and T. Itoh, “An ID-based cryptosystem based on the discrete logarithm problem,” IEEE Journal on Selected Areas in Communication **7**, 467-473 (1989).
2. A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” IEEE Tran. on Info. Th. **39**, 1639-1646 (1993).
3. P. Refregier and B. Javidi, “Optical-image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767-769 (1995).
4. 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).
5. O. Matoba and B. Javidi, “Encrypted optical storage with angular multiplexing,” Appl. Opt. **38**, 7288-7293 (1999).
6. T. Nomura and B. Javidi, “Optical encryption system with a binary key code,” Appl. Opt. **39**, 4783-4787 (2000).
7. 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).
8. 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).
9. 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).
10. Z. Liu, S. L. Xu, C. Lin, J. Dai, and S. Liu, “Image encryption scheme by using iterative random phase encoding in gyrator transform domains,” Opt. Lasers Eng. **49**, 542-546 (2011).
11. E. Perez-Cabre, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” Opt. Lett. **36**, 22-24 (2011).
12. Z. Liu, S. Li, M. Yang, W. Liu, and S. Liu, “Image encryption based on the random rotation operation in the fractional Fourier transform domains,” Opt. Lasers Eng. **50**, 1352-1358 (2012).
13. T. Sarkadi and P. Koppa, “Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys,” Appl. Opt. **51**, 745-750 (2012).
14. P. Koppa, “Phase-to-amplitude data page conversion for holographic storage and optical encryption,” Appl. Opt. **46**, 3561-3571 (2007).
15. N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” J. Opt. Soc. Am. A **16**, 1915-1927 (1999).
16. E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” Appl. Opt. **39**, 6595-6601 (2000).
17. 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).
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. 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).
20. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, “Optical encryption based on computational ghost imaging,” Opt. Lett. **35**, 2391-2393 (2010).
21. W. Chen and X. Chen, “Space-based optical image encryption,” Opt. Express **18**, 27095-27104 (2010).
22. 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).
23. 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).
24. M. Cho and B. Javidi, “Three-dimensional photon counting double-random-phase encryption,” Opt. Lett. **38**, 3198-3201 (2013).
25. M. Joshi, Chandrashakher, and K. Singh, “Color image encryption and decryption using fractional Fourier transform,” Opt. Commun. **279**, 35-42 (2007).
26. 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).
27. J. J. Sylvester, “Thoughts on orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton’s rule, ornamental tilework, and the theory of numbers,” Phil. Mag. **34**, 461-475 (1867).