Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 13(4): 280-285, Dec. 2015 **Regular paper**

Key Phase Mask Updating Scheme with Spatial Light Modulator for Secure Double Random Phase Encryption

Seok-Chul Kwon[1] and In-Ho Lee[2*], *Member, KIICE*

[1]Next Generation and Standards Division, Communication and Devices Group, Intel Corporation, Santa Clara, CA 95054, USA
[2]Department of Electrical, Electronic and Control Engineering, Hankyong National University, Anseong 17579, Korea

Abstract

Double random phase encryption (DRPE) is one of the well-known optical encryption techniques, and many techniques with DRPE have been developed for information security. However, most of these techniques may not solve the fundamental security problem caused by using fixed phase masks for DRPE. Therefore, in this paper, we propose a key phase mask updating scheme for DRPE to improve its security, where a spatial light modulator (SLM) is used to implement key phase mask updating. In the proposed scheme, updated key data are obtained by using previous image data and the first phase mask used in encryption. The SLM with the updated key is used as the second phase mask for encryption. We provide a detailed description of the method of encryption and decryption for a DRPE system using the proposed key updating scheme, and simulation results are also shown to verify that the proposed key updating scheme can enhance the security of the original DRPE.

Index Terms: Double random phase encryption, Image transmissions, Key phase mask, Optical encryption, Spatial light modulator

I. INTRODUCTION

A number of optical encryption techniques have been developed for information security [1-20]. One of the most well-known optical encryption techniques is double random phase encryption (DRPE), which adopts random phase encoding in the input and the Fourier planes [1]. In DRPE, two physical phase masks are used for random phase encoding and are keys for correct decryption. Since the physical phase masks are not modifiable, DRPE can be insecure [2]. Thus, various techniques for enhancement of security with DRPE have been developed, including the following: DRPE in the Fresnel domain [3], photon-counting DRPE [4, 5], DRPE using fractional Fourier transformation [6-8], DRPE using orthogonal encoding [9], and DRPE using accumulation encoding [10].

In order to improve the security of DRPE, photon-counting DRPE generates a sparse encrypted image with a limited number of photons, while DRPE using the Fresnel domain or fractional Fourier transformation employs more complex keys than the original DRPE, and DRPE using orthogonal encoding or accumulation encoding performs additional encoding for encrypted images from the original DRPE. However, the fundamental security problem of using fixed phase masks may be effectively solved by updating the phase masks, rather than using additional schemes for the DRPE. Therefore, in this paper, we propose a key phase mask updating scheme for DRPE, in which a spatial light modulator (SLM) is used to implement key phase mask updating. In the proposed scheme, only the second phase mask is updated

Received 21 September 2015, **Revised** 08 October 2015, **Accepted** 20 October 2015
***Corresponding Author** In-Ho Lee (E-mail:ihlee@hknu.ac.kr, Tel: +82-31-670-5197)
Department of Electrical, Electronic and Control Engineering, Hankyong National University, 327 Jungang-ro, Anseong 17579, Korea.

Open Access **http://dx.doi.org/10.6109/jicce.2015.13.4.280** print ISSN: 2234-8255 online ISSN: 2234-8883

with the SLM, and the input data of the SLM (i.e., the updated key data) are the amplitudes of the data that are obtained by Fourier transform after multiplying previous image data by the first phase mask. Thus, the proposed scheme requires only information from a previous image and the first phase mask to update the key phase mask, and hence it can be considered a simple key updating scheme. In this paper, we provide a detailed method for encryption and decryption of a DRPE system with the proposed key updating scheme, and also report simulation results to verify the security of DRPE with the proposed scheme.

The paper is organized as follows: in Section II, the original DRPE concept is introduced. In Section III, the key phase mask updating scheme for a DRPE system is described. In Section IV, simulation results for the proposed key updating scheme are provided to verify its security. In Section V, we conclude the paper.

II. DOUBLE RANDOM PHASEENCRYPTION CONCEPT

Encryption and decryption for the original DRPE proposed in [1] are described in Fig. 1(a) and (b), respectively. Without loss of generality, we assume one-dimensional data only. For encryption of DRPE, the primary data $p(x)$ are multiplied by the first random phase mask $\exp\{i2\pi n_s(x)\}$ in the spatial domain, where $n_s(x)$ denotes the random phase that is uniformly distributed over [0, 1]. Then, $\Im\{p(x)\exp\{i2\pi n_s(x)\}\}$ is obtained by passing through the first lens with the focal length f, where $\Im\{\cdot\}$ represents the Fourier transform. It is multiplied by the second random phase mask $\exp\{i2\pi r_f(w)\}$ in the spatial frequency domain, where $r_f(w)$ denotes the uniformly distributed random phase between 0 and 1. Finally, by passing through the second lens with a focal length f, the encrypted data $e(x)$ are obtained as in [4]:

$$e(x)=\Im^{-1}\left[\Im\left\{p(x)\exp\left\{i2\pi n_s(x)\right\}\right\}\times\exp\left\{i2\pi r_f(w)\right\}\right], \quad (1)$$

where $\Im^{-1}\{\cdot\}$ is the inverse Fourier transform.

For decryption of DRPE, the encrypted data $e(x)$ pass through the first lens with a focal length f, and thus $\Im\{e(x)\}$ is obtained. It is then multiplied by the complex-conjugate random phase mask $\exp\{-i2\pi r_f(w)\}$ to decode the encoded data by the second random phase mask. Finally, by passing through the second lens with a focal length f, the decrypted data $d(x)$ are obtained as in [4]:

$$d(x)=\left|\Im^{-1}\left[\Im\{e(x)\}\exp\left\{-i2\pi r_f(w)\right\}\right]\right|. \quad (2)$$

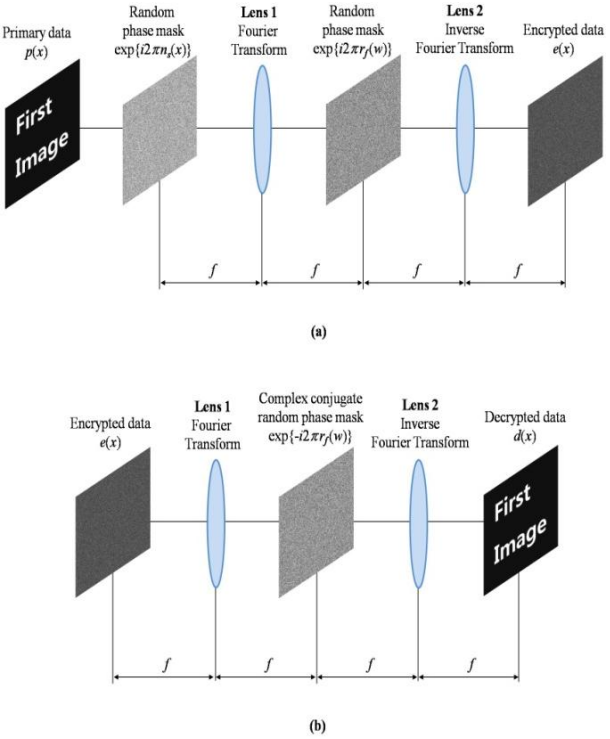

Fig. 1. Schematic setup of (a) encryption and (b) decryption for DRPE.

III. KEY PHASE MASK UPDATING SCHEME FOR DRPE SYSTEM

Fig. 2(a) depicts the encryption of the key phase mask updating scheme for a DRPE system. We assume that for encryption the initial key $r_{in}(x)$ is used until the k^{th} primary image $p_k(x)$, and an updated key $r_{up}(w)$ is used from the $(k+1)^{\text{th}}$ primary image $p_{k+1}(x)$. As shown in Fig. 2(a), only the second phase mask is considered for updating because it is used for both encryption and decryption, whereas the first phase mask $\exp\{i2\pi n_s(x)\}$ is used only for encryption. Thus, the first phase mask is regarded as a physical key phase mask (i.e., a fixed phase mask). SLM is employed as the second phase mask in order to implement updatable key data. The initial key data $r_{in}(w)$, which are the input of SLM, are generated with uniform distribution over [0, 1] and electronically synthesized. Hence, the second phase mask for the initial key is yielded as $\exp\{i2\pi r_{in}(w)\}$. Meanwhile, in order to update the key data for encrypting the $(k+1)^{\text{th}}$ primary image, the k^{th} primary data are multiplied by the first phase mask and passed through the lens. Then, the amplitudes of the resultant data are used as the updated key data, i.e., $r_{up}(w)=|\Im\{p_k(x)\exp\{i2\pi n_s(x)\}\}|$. The phases of SLM are determined by using the updated key data. Therefore, by SLM the second phase mask for the updated key is generated as $\exp\{i2\pi r_{up}(w)\}$. Accordingly,

the key data for the second phase mask can be frequently updated by using previous primary data and the first phase mask.

Fig. 2(b) shows the decryption of the key phase mask updating scheme for a DRPE system. We assume that complete initial key data are known for decryption. As seen in Fig. 2(b), the complex-conjugate phase mask $\exp\{-i2\pi\ r_{in}(w)\}$ is obtained by SLM using the known initial key data, and then using the phase mask, the k^{th} encrypted data $e_k(x)$ are perfectly decrypted. To update the key data in decryption, the k^{th} decrypted data $\tilde{d}_k(x)$ are multiplied by the first phase mask, and they pass through the lens. Thus, from the resultant data, the updated key data are obtained as $\tilde{r}_{up}(w) = |\Im\{\tilde{d}_k(x)\exp\{i2\pi n_s(x)\}\}|$. Analogous to Fig. 2(a), the updated key data are used as the phase information of SLM, and then SLM with the updated phases produces the complex conjugate of the second phase mask $\exp\{-i2\pi\tilde{r}_{up}(w)\}$ to decrypt the $(k+1)^{\text{th}}$ encrypted data $e_{k+1}(x)$.

As shown in Fig. 2, the proposed scheme requires only information on the previous image and the first phase mask to update the key phase mask in both encryption and decryption. Therefore, it can be considered a simple key updating scheme. In addition, the proposed scheme fully utilizes two phase masks in both encryption and decryption unlike the original DRPE, in which the first phase mask is not used in decryption. In this paper, in order to focus on security performance evaluation of the proposed scheme, we only consider that the previous image is perfectly decrypted by assuming perfect initial key data in decryption. We also assume that there is no modulation error in SLM, and the size of the phase mask and SLM is the same because a DRPE system with a unity magnification ratio is considered.

IV. SIMULATION RESULTS

For simulation of a DRPE system with the key phase mask updating scheme, we consider two primary images with 500(H)×500(V) pixels, as shown in Fig. 3. The first primary image in Fig. 3(a) is encrypted through DRPE using the initial key in Fig. 4(a), and then the second primary image in Fig. 3(b) is encrypted through DRPE using the updated key in Fig. 4(b). The initial key data in Fig. 4(a) are randomly generated with uniform distribution over [0, 1] and correspond to $r_{in}(x)$ in Fig. 2(a), whereas the updated key data in Fig. 4(b) are obtained as the amplitudes of data generated by Fourier transform after multiplying the first primary data by the first phase mask that is randomly made, which mean $r_{up}(w)$ in Fig. 2(a). Fig 4(c) and (d) show encrypted images by DRPE using the initial key and the updated key, respectively.

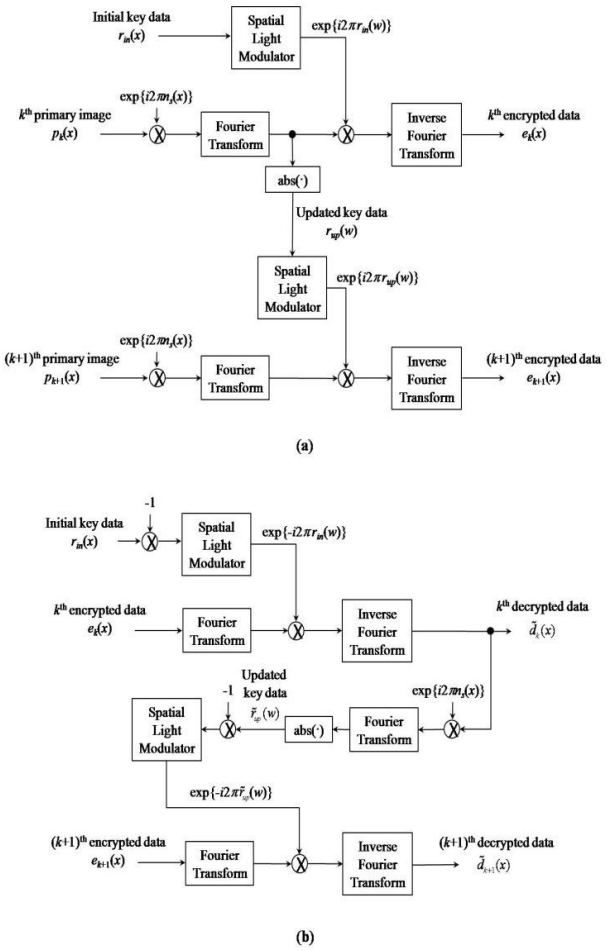

Fig. 2. Key phase mask updating scheme for a DRPE system: (a) encryption and (b) decryption.

Fig. 5(a) and (b) show correctly decrypted images by DRPE with the key phase mask updating scheme. By assuming that the initial key is perfectly known for decryption, the first encrypted image in Fig. 4(c) is completely decrypted, as seen in Fig. 5(a). The updated key data are then obtained by using the first decrypted image and the known first phase mask as in Fig. 2(b), which are the same as Fig. 4(b). With the updated key, the second encrypted image is correctly decrypted, and the second primary image is clearly obtained, as shown in Fig. 5(b).

Fig. 6(a) and (b) show simulation results of decryption for a DRPE system with the key phase mask updating scheme when only the initial key is used for decryption. The first decrypted image in Fig. 6(a) is correct because the known initial key is used for decryption of DRPE. However, the second decrypted image in Fig. 6(b) is incorrect and entirely unrecognizable since the key is not updated and the initial key is used to decrypt the second encrypted image, i.e., $\tilde{r}_{up}(w) = r_{in}(x)$ in Fig. 2(b).

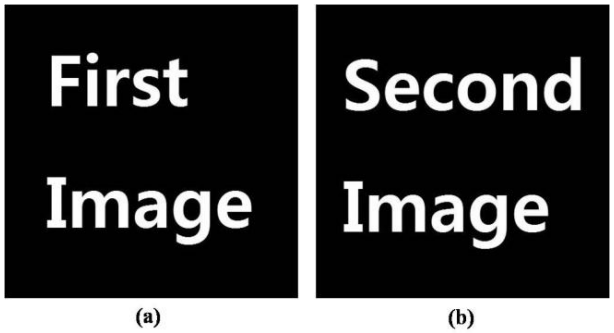

Fig. 3. 1st and 2nd primary images.

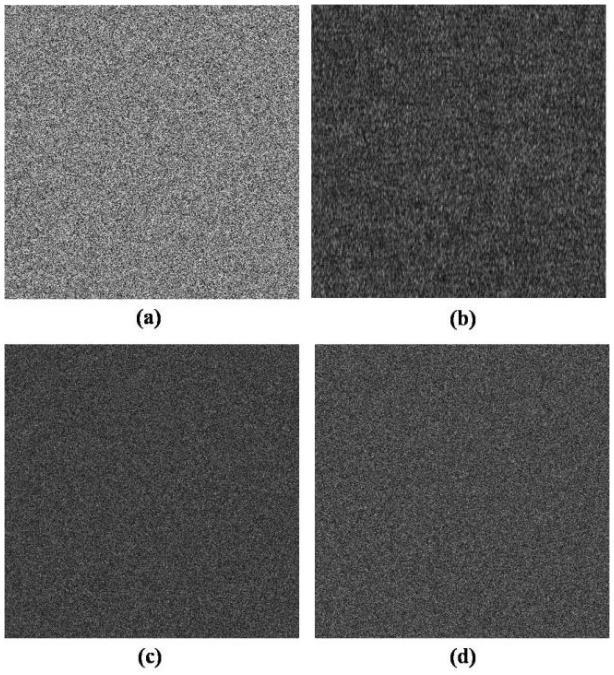

Fig. 4. Simulation results of a DRPE system with the key phase mask updating scheme: (a) initial key data, (b) updated key data, (c) 1st encrypted image, and (d) 2nd encrypted image.

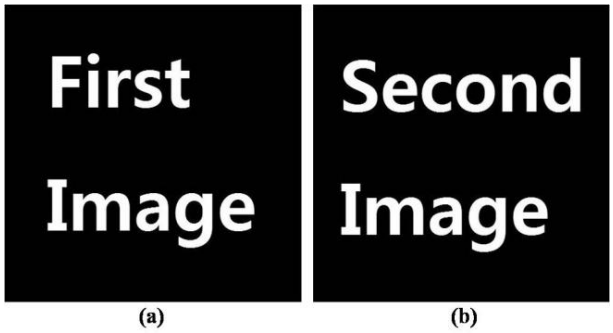

Fig. 5. Simulation results of correct decryption of a DRPE system with the key phase mask updating scheme: (a) 1st decrypted image and (b) 2nd decrypted image.

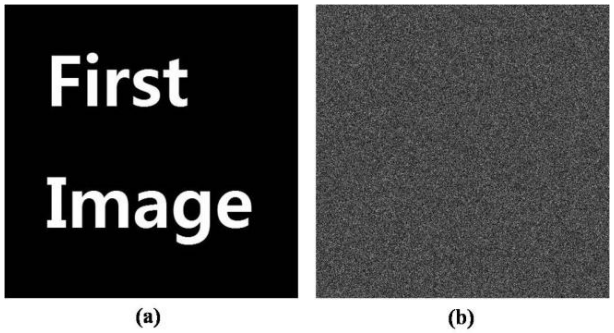

Fig. 6. Simulation results of decryption for a DRPE system with the key phase mask updating scheme when only initial key is used for decryption. (a) 1st decrypted image and (b) 2nd decrypted image.

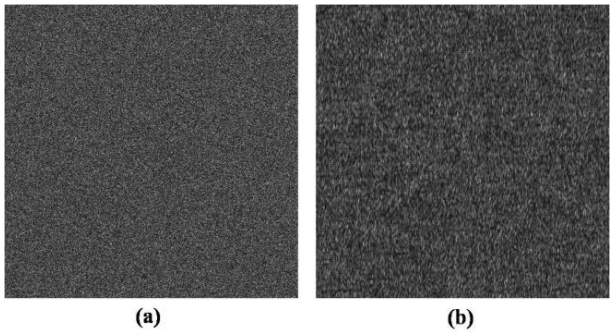

Fig. 7. Simulation results of decryption for a DRPE system with the key phase mask updating scheme when the key is updated with a wrong first phase mask in decryption: (a) 2nd decrypted image and (b) incorrectly updated key data.

Fig. 7(a) shows the second decrypted image by DRPE with the key phase mask updating scheme when the first decrypted image is correct but the key is updated with an incorrect first phase mask in decryption. The wrong phase mask is randomly generated, and it does not match the first phase mask used in encryption. Fig. 7(b) shows the updated key data that are obtained by using the wrong phase mask. As seen in Fig. 7(a), although the first encrypted image is perfectly decrypted, the decryption of the second encrypted image fails if the first phase mask is wrong. From the simulation results in Figs. 6(b) and 7(a), we verify that the proposed key phase mask updating scheme can improve the security of the original DRPE.

V. CONCLUSIONS

We propose a key phase mask updating scheme to enhance the security of a DRPE system, where SLM is used to update a key phase mask. In fact, we present the method of encryption and decryption in detail for a DRPE system using the proposed key updating scheme. From the simulation results, we also verify that the updated key data

by the proposed scheme include randomness such as noise, and DRPE using the updated key is able to achieve the security enhancement. Moreover, as the proposed scheme only requires the information of a previous image and the first phase mask to update the key phase mask, it can be considered a simple and effective key updating scheme for DRPE systems.

REFERENCES

[1] P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767-769, 1995.

[2] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Optics Express*, vol. 15, no. 16, pp. 10253-10265, 2007.

[3] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, vol. 24, no. 11, pp. 762-764, 1999.

[4] E. Perez-Cabre, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Optics Letters*, vol. 36, no. 1, pp. 22-24, 2011.

[5] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Optics Letters*, vol. 38, no. 17, pp. 3198-3201, 2013.

[6] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887-889, 2000.

[7] M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," *Optics Communications*, vol. 279, no. 1, pp. 35-42, 2007.

[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," *Optics Communications*, vol. 283, no. 12, pp. 2496-2505, 2010.

[9] I. H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," *Journal of the Optical Society of Korea*, vol. 18, no. 3, pp. 201-206, 2014.

[10] I.H. Lee, "Accumulation encoding technique based on double random phase encryption for transmission of multiple images," *Journal of the Optical Society of Korea*, vol. 18, no. 4, pp. 401-405, 2014.

[11] T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Applied Optics*, vol. 39, no. 26, pp. 4783-4787, 2000.

[12] D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," *Applied Optics*, vol. 46, no. 26, pp. 6641-6647, 2007.

[13] 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," *Optics & Laser Technology*, vol. 40, no. 4, pp. 619-624, 2008.

[14] T. Sarkadi and P. Koppa, "Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys," *Applied Optics*, vol. 51, no. 6, pp. 745-750, 2012.

[15] 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," *Optics Express*, vol. 18, no. 13, pp. 13772-13781, 2010.

[16] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," *Optics Communications*, vol. 259, no. 2, pp. 532-536, 2006.

[17] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," *Applied Optics*, vol. 40, no. 14, pp. 2310-2315, 2001.

[18] W. Chen and X. Chen, "Space-based optical image encryption," *Optics Express*, vol. 18, no. 26, pp. 27095-27104, 2010.

[19] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," *Proceedings of the IEEE*, vol. 97, no. 6, pp. 1128-1148, 2009.

[20] S. H. Jeon and S. K. Gil, "Dual optical encryption for binary data and secret key using phase-shifting digital holography," *Journal of the Optical Society of Korea*, vol. 16, no. 3, pp. 263-269, 2012.

Seok-Chul Kwon

earned his Ph.D. degree from Georgia Institute of Technology in Atlanta, Georgia, US in 2013. Before that, Dr. Kwon earned a M.Sc. degree from the University of Southern California in 2007; and a B.Sc. degree from Yonsei University, Seoul, South Korea in 2001.Dr. Kwon conducted postdoctoral research at the Wireless Devices and Systems Group, University of Southern California in 2014 to 2015, and is currently with Intel Corporation, in particular, the Next Generation and Standards Division in the Communication and Devices Group. He has been involved in several projects for organizations such as DARPA and the US Army Research Lab; and contributed to six mobile-station products for Motorola and Sprint, which were successfully brought to market. His current research interests are in 5G wireless system design; polarization diversity and multiplexing; body area networks such as wearable computing and in-vivo communications; wireless channel modeling and its applications; and network coding-aware channel assignment.

In-Ho Lee
earned B.S., M.S. and Ph.D. degrees in electrical engineering from Hanyang University, Ansan, Korea, in 2003, 2005 and 2008, respectively. He worked on LTE-Advanced standardization at Samsung Electronics from 2008 to 2010. He was a Post-Doctoral Fellow in the Department of Electrical Engineering, Hanyang University, Ansan, Korea, from April 2010 to March 2011. Since March 2011, he has been with the Department of Electrical, Electronic and Control Engineering, Hankyong National University, Anseong, Korea. His present research interests include optical encryption, image transmissions, wireless cooperative communications, and wireless multiple-input multiple-output communications.