Enhanced security computational double random phase encryption by using additional random function

doi: https://doi.org/10.1109/ICTC52510.2021.9621077

Enhanced security computational double random phase encryption by using additional random function

Kazuaki Honda
dept. of Computer Science and Networks, Kyushu Institute of Technology,
Iizuka City, Fukuoka, Japan
honda@ois3d.cse.kyutech.ac.jp

Jaehoon Lee
dept. of Computer Science and Networks, Kyushu Institute of Technology,
Iizuka City, Fukuoka, Japan
jhlee@ois3d.cse.kyutech.ac.jp

Hyun-Woo Kim
dept. of Computer Science and Networks, Kyushu Institute of Technology,
Iizuka City, Fukuoka, Japan
kim@ois3d.cse.kyutech.ac.jp

Myungjin Cho
dept. of ICT, Robotics, Mechanical Engineering, IITC, Hankyong National University,
Anseong-si, Kyonggi-do, South Korea
mjcho@hknu.ac.kr

Min-Chul Lee
dept. of Computer Science and Networks, Kyushu Institute of Technology,
Iizuka City, Fukuoka, Japan
lee@csn.kyutech.ac.jp

***Abstract*—Image encryption technique has been actively researched and improved. Double Random Phase Encryption (DRPE), known as the typical way of optical encryption, can easily encrypt images. In the decryption process of DRPE, the complex conjugate of random phase mask used as the encryption key in the Fourier domain is used as the decryption key. As a result, computational DRPE has a vulnerability in image transmission when the random phase mask is stolen. Our proposed method utilizes the random function defined by the sender, and it generates additional random variable to multiply the random phase mask. Finally, our proposed method can enhance the security of the encryption process. However, the random phase mask and random variable information generated by random function are needed to decrypt the image. To send both information, high cost is required in the transmission process. To overcome this problem, our proposed method sends the conjugate random phase mask and random function to the receiver for the decryption process. Finally, our proposed method can enhance security with a low transmission cost.**

***Index Terms*—Double Random Phase Encryption, Encryption, Information security**

I. Introduction

Recently, the encryption technique has been more critical for information security. Especially, in image encryption, the encrypted image must not contain any feature or shapes of the original image. To preserve the image securely, lots of image encryption techniques have been presented, such as the method based on DNA encoding and chaos map [1], the algorithm based on parallel compressive sensing and DNA sequence [2], and Double Random Phase Encryption (DRPE) [3]. DRPE is one of the simplest optical encryption methods. This is because both encryption and decryption processes use only two random phase masks. In this technique, the image is encoded using two random phase masks according to 4-f optical system. To decrypt the image, it uses complex conjugate of the second random phase mask as the decryption key. However, in computational DRPE for data transmission, there is a vulnerable problem with the decryption key. To enhance the security of DRPE, many types researches have been presented, such as a lensless optical security system in the Fresnel domain [4], photon counting DRPE [5], and optical nonlinear cryptosystem [6]. However, if the attacker knows the complex conjugate of random phase mask information, the attacker can reveal the image.

To solve this problem, our proposed method enhanced security by adding the random function. This function can be defined by the sender who wants to encrypt the image. Therefore, it is difficult for an attacker to estimate the function. However, to decrypt the image, both complex conjugate of the second random phase mask and random variable information are required. To send both information, higher transmission cost is required than the conventional method. Thus, our proposed method sends the complex conjugate of random phase mask and random function to the receiver. The random function data size is smaller than the random variable data. Therefore, the transmission data size is almost the same as the conventional method. A random function received from a sender is used to generate random variables, which the sender used to encrypt the image. Finally, the receiver can decrypt the original image using the of random conjugate of random phase mask and the random variable.

Our paper is organized as follows. In Section 2, we explain the principle of encryption and decryption processes for DRPE, and we present our proposed method. In Section 3, we present

the experimental setup and the result. Finally, we present the conclusion in Section 4.

II. Image Encryption Method

A. Double Random Phase Encryption

Double Random Phase Encryption (DRPE) is the optical encryption method that encrypts the image with two random phase masks. Fig. 1 shows the process of DPRE of image transmission.

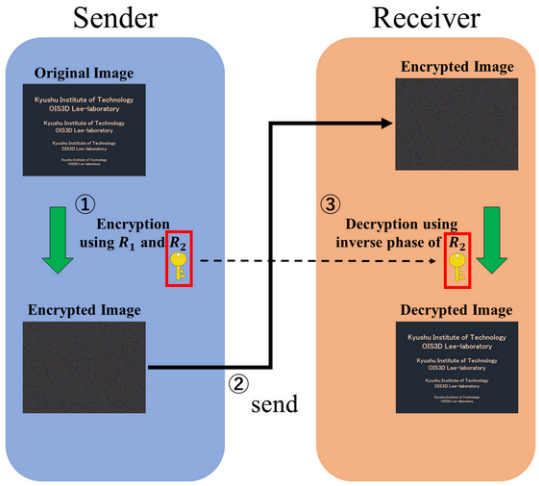


Fig. 1. Image transmission diagram using DRPE.

The sender encrypts the image through the DRPE process. Then the encrypted image is transmitted to the receiver. The receiver decrypts the encrypted image by using the complex conjugate of the second random phase mask.
To encrypt the image, double random phase masks are needed. Fig. 2 presents the processing flowchart of the encryption process.

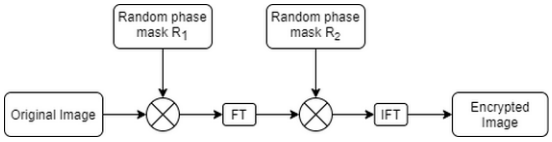


Fig. 2. Flowchart of encryption process of DRPE.

The original image is multiplied by the first random phase mask given as eq. 1.

$$R_1(x,y) = e^{(i2\pi \times r_1)} \tag{1}$$

where r_1 denotes the random variable from Uniform distribution with support [0, 1]. R_1 is located in the input plane of the 4-f system. However, this random phase mask R_1 contributes to making a featureless encrypted image. To encrypt the image, in Fourier domain, original image with the first random phase mask is multiplied by the second random phase mask $R_2(x,y)$ defined as eq. 2.

$$R_2(x,y) = e^{(i2\pi \times r_2)} \tag{2}$$

where r_2 is the random variable from Uniform distribution with support [0, 1]. This second random phase mask in the Fourier domain highly contributes to the encryption strength of DRPE. Finally, the encrypted image $E(x,y)$ can be defined by using eq. 3.

$$E(x,y) = IFT\left\{FT\left\{I(x,y) \times R_1(x,y)\right\} \times R_2(x,y)\right\} \tag{3}$$

where FT means Fourier Transform and IFT refer to as Inverse Fourier Transform.
To decrypt the image, the complex conjugate of random phase mask R_2 is needed. The decryption process of DRPE is illustrated in fig. 3.

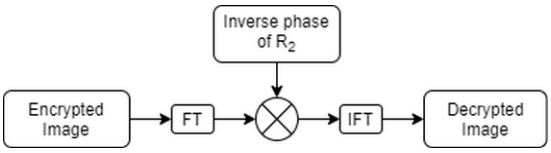


Fig. 3. Flowchart of decryption process of DRPE.

As shown in fig. 3, the encrypted image is decrypted by using Fourier transform, inverse Fourier transform and the complex conjugate of the second random phase mask. Finally, the decrypted image $D(x,y)$ can be defined as below eq. 4.

$$\begin{aligned} D(x,y) &= IFT\left\{FT\left\{E(x,y)\right\} \times R_2^{-1}\right\} \\ &= IFT\left\{FT\left\{E(x,y)\right\} \times e^{(-2\pi i \times r_2)}\right\} \end{aligned} \tag{4}$$

However, if the attacker knows the decryption key R_2, the original image can be revealed easily. To solve this problem, our proposed method uses the additional random variable in the Fourier domain.

B. Enhanced security computational DPRE by using additional random function

The encryption flowchart of our proposed method is presented in fig. 4.

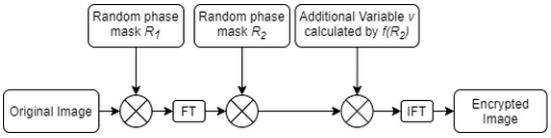


Fig. 4. Encryption flowchart of our proposed method.

To enhance the security of DPRE, our proposed method changes the phase information by using the random variable. The random variable can be defined by the random function f which is defined by the sender. Through the function f, additional random variable v can be defined as below eq. 5.

$$v = e^{(2\pi i \times f(R_2))} \tag{5}$$

The phase information is randomly distributed through the random variable v. Fig. 5 explains the phase information encryption process by using additional variable v.

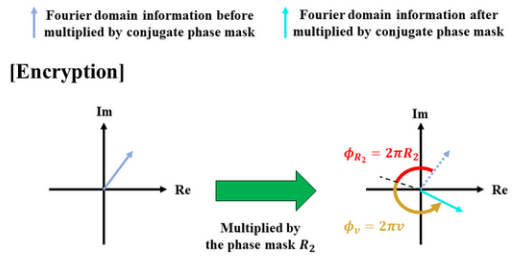


Fig. 5. Diagram of phase information encryption process.

Through the random variable, the encrypted image $E'(x, y)$ be defined as below eq. 6.

$$E'(x,y) = IFT\left\{FT\left\{I(x,y) \times R_1(x,y)\right\} \times R_2(x,y) \times v\right\} \tag{6}$$

Comparing with the conventional method, our proposed method multiplies v by the second random phase mask in the Fourier domain. Therefore, our proposed method can encrypt the image more securely than the conventional method. To decrypt the original image accurately, the complex conjugate of the additional random variable v is required as shown in fig. 6.

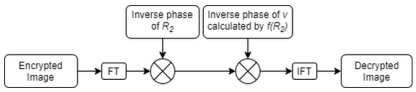


Fig. 6. Decryption flowchart of our proposed method.

If the receiver only has the random phase mask R_2 , the receiver cannot decrypt the encrypted image. This is because the phase information is still randomly distributed by random variable v. Therefore, to generate the original image phase information, the receiver must have both the random phase mask R_2 and additional variable v. Fig. 7 illustrates the phase information decryption process. Finally, decrypted image can be obtained as eq. 7.

$$\begin{aligned} D'(x,y) &= IFT\left\{FT\left\{E(x,y)\right\} \times R_2^{-1} \times v^{-1}\right\} \\ &= IFT\left\{FT\left\{E(x,y)\right\} \times e^{(-2\pi i \times (r_2 + f(R_2)))}\right\} \end{aligned} \tag{7}$$

The conventional method only sends the random phase mask R_2 to the receiver for decryption. In contrast, our proposed method sends the phase information of R_2 and v. Therefore, transmission cost will be double compared with the conventional method because the data size of the additional variable is the same as the random phase mask R_2 . Therefore, our proposed method sends the function instead of sending v to decrease the transmission cost. Then, the receiver generates the random mask v. Through the calculation, the receiver can obtain two decryption keys as fig. 8.

Through the random function, transmission data size can be decreased effectively. Finally, our proposed method can enhance the security of the computational DRPE with less transmission data size difference. Moreover, if the attacker tries to decrypt the image, it is difficult to obtain both phase information.

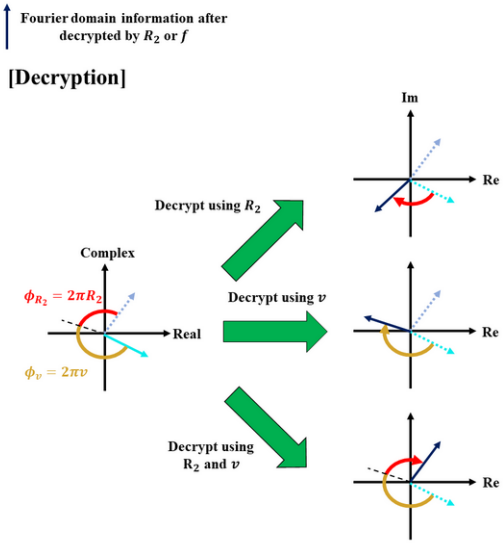


Fig. 7. Diagram of phase information decryption process.

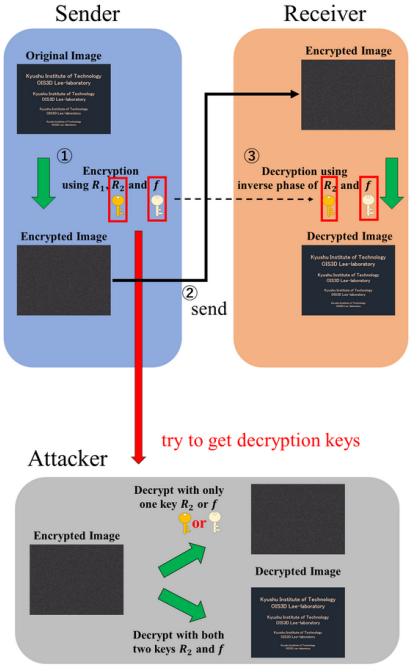


Fig. 8. Image transmission diagram of our proposed method.

To prove the performance of our proposed method, we carried out a simulation in Section 3.

III. Simulation Setup and Results

In our simulation, we use the image as original image in fig. 9. This is the RGB image which size is 960×720 pixels.

We use the words "Kyushu Institute of Technology OIS3D Lee-laboratory" four times with different font sizes as the original image. Thus, the evaluation index of the encryption is whether we can recognize those words or not. We encrypt

Fig. 9. Original image for encryption.

this original image by using the conventional method and our proposed method, respectively. In our proposed method for this simulation, random function is given as the following eq. 8.

$$f(R_2) = 2R_2^3 + R_2^2 + \frac{5}{4}R_2 \tag{8}$$

To compare the decryption image of each method, fig. 10 shows the encrypted images of the conventional method and proposed method, respectively.

(a) conventional method.

(b) proposed method.

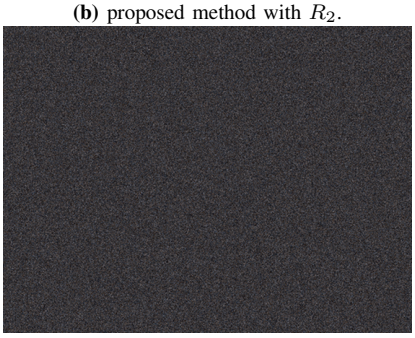
Fig. 10. Encrypted images.

Both encrypted images are the noise images. We cannot recognize any characters or shapes in both encrypted images. However, since our proposed method uses the additional random variable through the encryption process, even if attacker knows the second random phase mask information (i.e., decryption key), our proposed method can preserve the image securely. To show the decryption performance of both methods, we show decrypted images using in fig. 11.

In conventional method, we use only R_2 as the decryption key, the attacker can obtain the original image if R_2 is revealed. On

(a) conventional method with R_2.

(b) proposed method with R_2.



(c) proposed method with $f(R_2)$.

Fig. 11. Decrypted images

the other hand, in our proposed method, the attacker cannot obtain an original image by using the random phase mask R_2. In addition, the attacker cannot decrypt the encrypted image precisely by using the $f(R_2)$. Therefore, the attacker cannot obtain the original image even if the attacker knows either R_2 or $f(R_2)$. Finally, our proposed method can enhance the security of DRPE in image transmission. To recover the original image clearly, the receiver must have both the random phase mask R_2 and the function $f(R_2)$ freely defined by the sender. We show the decrypted image by our proposed method in fig. 12.

In this decrypted image, we can recognize the full words written in the original image. Thus, the visual quality of this decrypted image is the same as the original image. Furthermore, in our proposed method, the data size of the program file containing the random function $f(R_2)$ defined by sender is lower than the random variable for encryption. The comparison of data size is shown in table I.

When we transmit the two independent phase information, the transmission cost increases. In contrast, our proposed

Fig. 12. Decrypted image using R_2 and $f(R_2)$ as decryption keys.

Table I. Data size comparison.

Original image [byte]	R_1[byte]	R_2[byte]	$f(R_2)$[byte]
16,588,800	11,059,200	11,059,200	88

method transmits the mask and the random function to the receiver. According to Table I, the transmitted data size can decrease effectively. As a result, in our proposed method, the transmission cost increases around $3.2 \times 10^{-4}[\%]$ through the below eq. 9.

$$\begin{aligned} 88 \div (16588800 + 11059200) &\fallingdotseq 3.2 \times 10^{-6} \\ &= 3.2 \times 10^{-4}[\%] \end{aligned} \tag{9}$$

On the other hand, if we utilize the additional random variable instead of the random function, the transmission cost will increase $40[\%]$ compared with the conventional method as below eq. 10.

$$11059200 \div (16588800 + 11059200) = 40[\%] \tag{10}$$

Finally, our proposed method shows the better cost performance than using the additional random variable to encrypt the data securely.

IV. Conclusion

In this paper, we have proposed a method that uses the additional random variable generated by the random function f in the Fourier domain to enhance the security of DRPE. The random variable can be utilized for changing the random phase mask R_2 information. Therefore, the security level can be improved. Moreover, the transmission cost is almost the same as the conventional method because the random function data size is small enough and it is negligible. We believe that our proposed method can be utilized in e-commerce industries for a safe smart contract and a safe internet backup system.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (NRF-2020R1F1A1068637).

References

[1] Yuansheng Liu, Jie Tang, Tao Xie, “Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map”, Optics and Laser Technology, Vol.60, pp. 111-115, 2014.
[2] Deyun Wei, Mingjie Jiang, “A fast image encryption algorithm based on parallel compressive sensing and DNA sequence”, Optik – International Journal for Light and Electron Optics, Vol. 238, 166748, 2021.
[3] Philippe Réfrégier, Bahram Javidi, “Optical image encryption based on input plane and Fourier plane random encoding”, Optics Letters, Vol.20, 767, 1995.
[4] Guohai Situ, Jingjuan Zhang, “Double random-phase encoding in the Fresnel domain”, Optics Letters, Vol. 29, No. 14, pp. 1584-1586, 2004.
[5] Myungjin Cho, Baharm Javidi, “Three-dimensional photon counting double-random-phase encryption”, Optics Letters, Vol. 38, No. 17, pp. 3198-3201, 2013.
[6] Shuaifeng Dou, Xueju Shen, Chao Lin, “Security-enhanced optical nonlinear cryptosystem based on double random phase encoding”, Optics and Laser Technology, Vol. 123, 105897, 2020.
[7] G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain”, Optics Letters, Vol. 25, No. 12, pp. 887-889, 2000.
[8] Yann Frauel, Albertina Castro, Thomas J. Naughton, Bahram Javidi, “Resistance of the double random phase encryption against various attacks”, Optics Express, Vol. 15, No. 16, pp. 10253-10265, 2007.
[9] David S. Monaghan, Unnikrishnan Gopinathan, Thomas J. Naughton, John T. Sheridan, “Key-space analysis of double random phase encryption technique”, Applied Optics, Vol. 46, No. 26, pp. 6641-6647, 2007.
[10] X. C. Cheng, L. Z. Cai, Y. R. Wang, X. F. Meng, H. Zhang, X. F. Xu, X. X. Shen, G. Y. Dong, “Security enhancement of double-random phase encryption by amplitude modulation”, Optics Letters, Vol. 33, No. 14, pp. 1575-1577, 2008.
[11] Pramod Kumar, Arvind Kumar, Joby Joseph, Kehar Singh, “Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions”, Optics Letters, Vol. 34, No. 3, pp. 331-333, 2009.
[12] Kazuya Nakano, Hiroyuki Suzuki, “Analysis of singular phase based on double random phase encoding using phase retrieval algorithm”, Optics and Lasers in Engineering, Vol. 134, 106300, 2020.
[13] Jaehoon Lee, Myungjin Cho, Kotaro Inoue, Min-Chul Lee, “3D Optical Encryption System using Merging Reconstruction Method”, Proceeding of the 2020 3rd International Conference on Electronics and Electrical Engineering Technology, pp. 55-61, 2020.