3D Optical Encryption System using Merging Reconstruction Method

著者	Lee Jaehoon, Cho Myungjin, Inoue Kotaro, Lee Min-Chul
journal or publication title	EEET '20: Proceedings of the 2020 3rd International Conference on Electronics and Electrical Engineering Technology
page range	55-61
year	2020-09
URL	http://hdl.handle.net/10228/00008016

doi: https://doi.org/10.1145/3429536.3429540

3D optical encryption system using merging reconstruction method

Jaehoon Lee
Kyushu institute of technology, CSE
680-4, Kawazu, Iizuka-shi
Fukuoka, Japan
+81-70-2665-6630
jhlee@leo10.cse.kyutech.ac.jp

Myungjin Cho
Hankyong National university, IITC
327, Chungang-ro, Anseong-si
Gyeonggi-do, Republic of Korea
+82-31-670-5298
mjcho@hknu.ac.kr

Kotaro Inoue
Hankyong National university, IITC
327, Chungang-ro, Anseong-si
Gyeonggi-do, Republic of Korea
+82-10-3051-4022
inoue@hknu.ac.kr

Min-Chul Lee
Kyushu Institute of Technology, CSE
680-4 Kawazu, Iizuka-shi
Fukuoka, Japan
+81-948-29-7699
lee@cse.kyutech.ac.jp

ABSTRACT

In this paper, we propose a photon-counting double random phase encryption with merging reconstruction. Double random phase encryption (DRPE) is a simple and secure optical encryption technique using phase random masks. To enhance the security level, a three-dimensional photon counting technique has been applied to DRPE. However, we cannot recognize the original image information in a photon-limited scene. To solve this problem, we propose a merging reconstruction method, which can detect the photons using several reconstruction layers. Through this method, we can obtain a decrypted image of enhanced visual quality. This paper presents a simulation test for the proposed method.

CCS Concepts

• Computer systems organization → Architectures → Other architectures → Optical computing • Theory of computation → Computational complexity and cryptography → Cryptographic primitives • Mathematics of computing → Probability and statistics → Probabilistic interference problems → Maximum likelihood estimation

Keywords

"Three-dimensional imaging", "Integral imaging", "Photon-counting", "3D visualization", "Optical encryption".

1. INTRODUCTION

Double random phase encryption (DRPE) is one of the most well-known optical encryption techniques [1]. It can encrypt data using two phase masks and decrypt the data with a phase mask key. DRPE can encrypt data at the speed of light and it does not require the updating of an authentication key for encryption. Based on these advantages, many DRPE studies have been reported.

To effectively enhance its security level, photon counting imaging was applied to DRPE. Photon counting imaging can visualize an object in photon-starved conditions [2-3]. It can detect the photons from a scene using the Poisson random process and statistically estimate the scene. DRPE with photon counting imaging can encrypt data with an improved security level and is referred to as photon-counting double random phase encryption (PDRPE) [4]. However, PDRPE cannot generate a high-quality decrypted image. Thus, we cannot easily recognize data in a photon-limited scene. Moreover, this technique can only encrypt two-dimensional (2D) data. To address these challenges, the integral imaging technique has been applied to PDRPE.

The integral imaging technique can generate a 3D reconstructed image and it can be divided into two processes: pick-up and reconstruction [5]. In the pick-up process, object images of different perspectives are recorded through the lens array; these images are called elemental images. In the reconstruction process, 3D images are generated by back-projecting the elemental images through the virtual pinhole array. This reconstruction method is called volumetric computational reconstruction (VCR) [6-7]. In VCR, the reconstructed 3D images can be generated with different depths. Therefore, PDRPE with integral imaging can encrypt not only 2D images, but also 3D data. Additionally, it can visualize decrypted images with photon-starved conditions [8-13]. However, it is difficult to visualize a decrypted image in *severely* photon-starved conditions. For these conditions, we propose a merging reconstruction method. For this technique, several reconstruction layers are constructed to enhance the visual quality of the decrypted image. Finally, we can obtain a high quality decrypted image and recognize the image under a severely photon-starved condition.

This paper is organized as follows: in section 2, we describe the conventional 3D optical encryption and then present our proposed method; in section 3, we discuss the implementation of the computer simulation and present the results which compare the performance of our proposed method with the conventional method; finally, we present the concluding remarks in section 4.

Integral imaging technique can generate the three-dimensional (3D) reconstructed image and it can be divided into two processes; pick up and reconstruction process [5]. In the pick-up process, different perspective object images through the lens array are recorded where these images are called as elemental images. In the reconstruction process, 3D images are generated by back-projecting the elemental images through the virtual pinhole array. This reconstruction method is called as volumetric computational reconstruction (VCR) [6-7]. In VCR, the reconstructed 3D images with different depths can be generated. Therefore, PDRPE with integral imaging can encrypt not only 2D images but also 3D data. Also, it can visualize the decrypted images with photon-starved conditions [8-13]. However, it is difficult to visualize the decrypted image in severely photon-starved conditions. To visualize the decrypted image even in these conditions, we propose a merging reconstruction method. In this technique, several reconstruction layers are constructed to enhance the visual quality of the decrypted image. Finally, we can obtain the high quality decrypted image and can recognize the image under severely photon-starved situation.

This paper organized as follows. In section 2, we present the conventional 3D optical encryption and explain our proposed method. In section 3, we implement the computer simulation and show the results to compare the performance of our proposed method with the conventional method. Finally, we present the conclusion in section 4.

2. 3D optical encryption

2.1 Double Random Phase Encryption (DRPE)

The DRPE technique is the simplest and fastest optical encryption method. It uses two random phase masks to encrypt an image. Let f(x) be the original image in 1D notation. n(x) represents the spatial domain random noise and n(μ) represents the frequency domain of the encoded random noise, which is uniformly distributed over [0, 1]. To encrypt the original image, the original image is multiplied by the random phase mask exp[i2πn(x)]. It is then convolved with the function h(x), the Fourier transform of which is exp[i2πn(μ)]. As a result, the encrypted image E(x) is defined as below.

$$\mathrm{E(x)} = F^{-1}\{F[f(x)\exp\{i2\pi n(x)\}]\exp[\,i2\pi n(\mu)]\} \quad (1)$$

F represents the Fourier transform and F^{-1} is the inverse Fourier transform. The encrypted image E(x) is a complex term and it can be expressed by its amplitude and phase terms, as below.

$$\mathrm{E(x)} = |E(x)|\exp[i\emptyset(x)] \quad (2)$$

E(x) can be decrypted by multiplying the conjugate of the second random phase mask, as written below.

$$\mathrm{D(x)} = |F^{-1}[F\{E(x)\}\exp\{-i2\pi n(\mu)\}]| \quad (3)$$

Finally, the decrypted image D(x), which is the same as the original image f(x), can be obtained. Figure 1 illustrates the entire process of DRPE.

DOI: http://dx.doi.org/10.1145/12345.67890

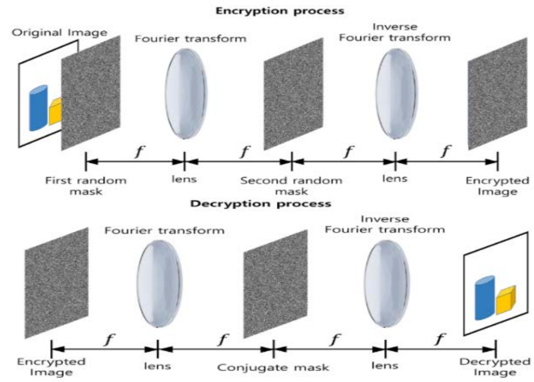

Figure 1. Process of double random phase encryption.

To keep the original image safe and develop a more secure encryption process, photon counting imaging is applied. Because it can extract a few photons from the encrypted image, the security level of DRPE can be enhanced; i.e., even if the key random phase mask is known, it is not possible to visualize the decrypted image, owing to the lack of information of the encrypted image. Therefore, we can enhance the security of the data so that it is superior to the conventional method. In the next section, we present the photon-counting double random phase encryption method.

2.2 Photon counting Double Random Phase Encryption (PDRPE)

When the light source illuminates the object, the reflected photons emanate from the object. An image sensor records these photons to visualize the object shape. However, these photons are rarely detected in unit time and space under photon-starved conditions. Therefore, photon counting imaging can be used under these conditions because it is able to detect these photons. In addition, photon counting imaging can be modeled by a Poisson distribution. Figure 2 describes the photon counting process.

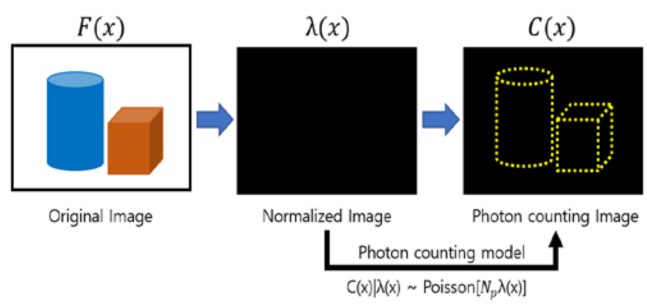

Figure 2. Photon counting process.

When the light source illuminates the object, the reflected photons emanate from the object. An image sensor records these photons to visualize the object shape. However, these photons are rarely detected in unit time and space under photon-starved conditions. Therefore, photon counting imaging can be used under these conditions because it is able to detect these photons. In addition, photon counting imaging can be modeled by a Poisson distribution. Figure 2 describes the photon counting process.

This technique may be used to improve on the security of the original image, compared with the conventional DRPE method. To generate the photon-limited encrypted image from the conventional encrypted image, we normalize this image.

$$\lambda(\mathrm{x}) = \frac{E(x)}{\sum_{x=1}^{N_x} E(x)}, \quad (4)$$

where N_x represents the number of pixels in the image. The photon-limited encrypted image can subsequently be generated from the normalized image $\lambda(x)$ using the Poisson distribution, as follows.

$$C(x)|\lambda(x) \sim Poisson[N_p \lambda(x)], \quad (5)$$

where N_p is the expected number of photons in the image. Here, we detect the number of photons N_p from the normalized image $\lambda(x)$. We can generate the photon-limited encrypted image $C(x)$. We can then decrypt the image with the same method, as described in section 2.1. Equation 6 represents the decryption process of PDRPE.

$$D_{ph}(x) = |F^{-1}[F\{C(x)\}\exp\{-i2\pi n(\mu)\}]| \quad (6)$$

However, under severely photon-starved conditions, it cannot reveal the original information data because there is too little information for the encrypted image. Thus, the decrypted image appears as an image with white noise. To enhance the visual quality of the decrypted image and recognize its information, integral imaging can be applied. In the next section, we present the PDRPE technique with integral imaging.

2.3 Integral Imaging

Integral imaging can generate a full parallax 3D image without a coherent light source. It uses elemental images of different perspectives to reconstruct the 3D image. Figure 3 represents the concept of integral imaging.

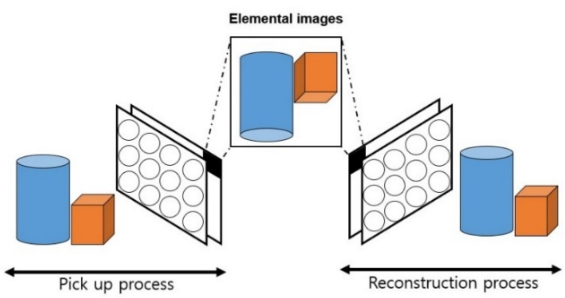

Figure 3. Concept of integral imaging.

It can record the elemental images through a lenslet array and reconstruct the 3D images, with different depths, through the homogeneous lenslet array used in pick-up. However, the lenslet array may decrease the elemental image resolution; thus, a camera array may be used to enhance the resolution of each elemental image. In addition, to reconstruct the 3D image using the computational method, we apply the VCR method. Each elemental image passes through the virtual pinhole array and is propagated onto the reconstruction plane, where the elemental images are overlapped; finally, we can obtain the 3D reconstructed images at each depth.

The VCR technique, used with PDRPE, can decrypt the 3D data and visualize the photon-limited decrypted image. For this technique, the photon-limited encrypted images are used as the elemental images. Figure 4 illustrates the PDRPE with the VCR method.

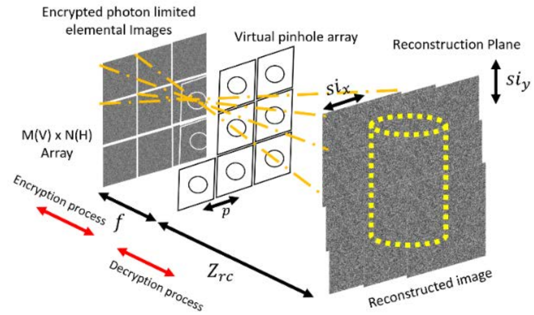

Figure 4. PDRPE with volumetric computational reconstruction.

f is the distance between the elemental images and the virtual pinhole array. p is the distance between pinholes. Z_{rc} is the depth between the pinhole array and the reconstruction plane. si_x and si_y are the shifting pixel values of each elemental image on the reconstruction plane. The shifting pixel values and reconstruction process are defined in the following equations.

$$si_x = \frac{N_{Ex} \times p \times f}{C_{sx} \times Z_{rc}} \qquad si_y = \frac{N_{Ey} \times p \times f}{C_{sy} \times Z_{rc}} \quad (7)$$

$$RC(x, y, Z_{rc}) = \frac{1}{N_p O(x, y, Z_{rc})} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} D_{ph}(x + si_x m, y + si_y n) \quad (8)$$

N_{Ex} and N_{Ey} are the number of pixels for the elemental image in the x and y directions, respectively. C_{sx} and C_{sy} are the image sensor size. $O(x, y, Z_{rc})$ is the overlap matrix on the reconstruction plane and M and N are the number of elemental images in the x and y directions, respectively. We can then reconstruct the decrypted photon limited 3D image $R(x, y, Z_{rc})$.

However, this method is not able to generate high visual quality for 3D objects and it cannot visualize the object in severely photon-starved conditions. To visualize images of high visual quality, many elemental images with a large number of photons are required. However, if the number of photons increases, the security level of the DRPE is degraded and it makes the photon counting process meaningless.

To solve this problem, we require a new reconstruction method that can visualize the original information with a few photons. In the next section, we propose the new reconstruction method, which is able to visualize the original information data under severely photon-starved conditions, called the 3D merging reconstruction method

2.4 3D optical encryption system with merging reconstruction method

To visualize the decrypted image, the size of the original photon data effectively increases. To increase the number of photons in the reconstruction process, the reconstruction plane is divided into several reconstruction layers. On each reconstruction layer, we reconstruct a new elemental image using 2(H) × 2(V) original elemental images, which can effectively collect the continuous photon information. We can thus obtain the single reconstructed image with many photons.

To visualize the 3D image, the overlapping matrix is modified because the conventional overlapping matrix may attenuate the intensity of the photons. The conventional method calculates the overlapping number in unit image. However, when the image has no pixel intensity values, it can decrease the photon intensity and it may lose the information of the original photons. However, we calculate the overlapping number in unit pixel. Therefore, we can increase the pixel density and effectively visualize the photon image under severely photon-starved conditions. Figure 5 describes the reconstruction process of the proposed method and Fig. 6 presents the difference between the conventional and proposed overlapping matrices.

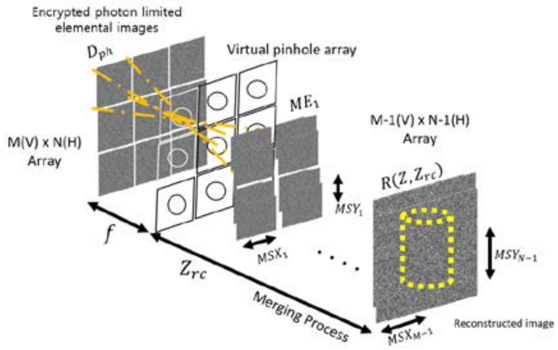

Figure 5. PDRPE with merging reconstruction method.

ME_m represents the elemental images in each reconstruction layer. PEX_m and PEY_m are the number of pixels of ME_m in the x and y directions, respectively. MSX_m and MSY_m are the shifting pixel values in each layer. We can define the shifting pixel values, MSX_m and MSY_n, and the reconstructed image ME_m as below.

$$ME_m = \frac{1}{N_p O_v(x)} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} D_{ph}\left(x + MSX_m m, y + MSY_m n\right) \quad (9)$$

$$MSX_m = \frac{f \times p \times PEX_m}{C_{sx} \times Z_{rc}}, \; MSY_m = \frac{f \times p \times PEY_m}{C_{sy} \times Z_{rc}} \quad (10)$$

To generate a single reconstructed image, ME_m elemental images are reconstructed in each layer. Thus, we can generate a high visual quality 3D image using the merging reconstruction method.

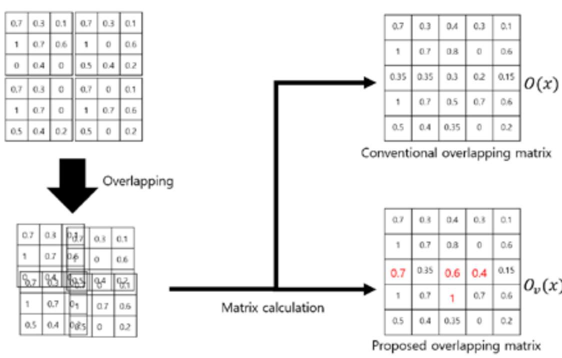

Figure 6. The concept of proposed overlapping matrix.

As seen in Fig. 6, the conventional overlapping matrix may lose the photon data when the matrix has a zero-pixel intensity value. To compensate for this, we calculate the overlapping number in unit pixel. We can thus maintain the photon intensity of each elemental image, which is an improvement on the conventional method. In the next section, we present a computer simulation to verify our proposed method.

3. Simulation setup and results

To demonstrate the performance of our proposed method, we implement a computer simulation. To generate the 3D decrypted image, we have to pick-up the elemental images. Therefore, we use the 5(H) × 5(V) camera array. The focal length of the camera is 50 mm. To obtain different perspectives in each elemental image, the pitch between cameras is 2 mm. Each elemental image has a pixel resolution of 800(H) × 800(V). We use these elemental images to decrypt the original data for the PDRPE method. To apply this simulation to a realistic situation, we test two types of the elemental images and we set each information data point in front of the camera array. The distance between the camera and the information data is 120 mm. Figures 7 and 8 present the simulation setup and the elemental images, respectively.

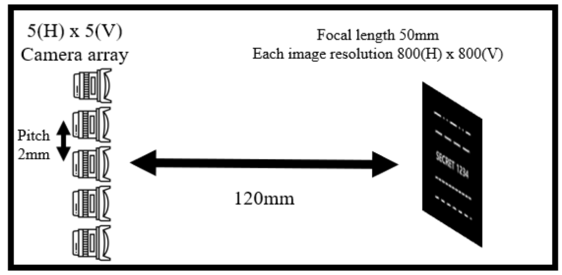

Figure 7. Computer simulation setup.

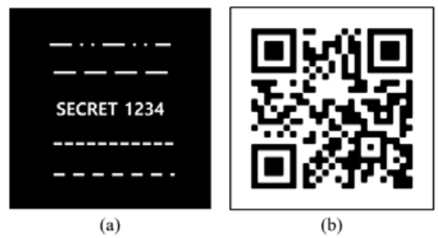

Figure 8. The elemental images. (a) Information data, (b) QR (Quick Response) code.

First, we implement the simulation for the information data, as shown in Fig. 8(a). We generate the decrypted images with photon limited elemental images, which has photons from 4000 to 7000. We compare the result of the conventional method with that of the proposed method, as below.

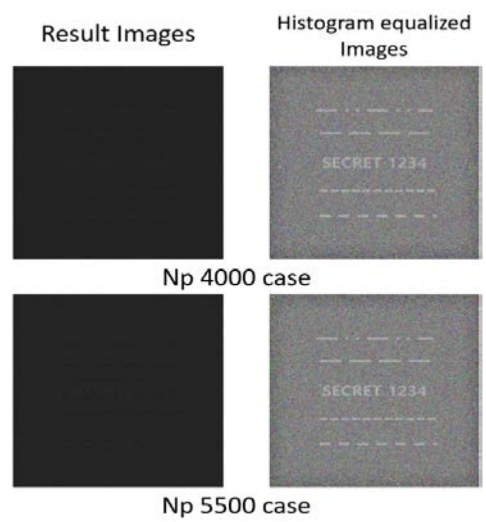

Figure 9. Conventional DRPE result images.

We present two images in Fig. 9. We cannot observe the resulting images; thus, we visualize the images using histogram equalization. We cannot clearly observe the word in the resulting image for the conventional method. We therefore gradually increase the expected photons up to 5500; however, we cannot clearly visualize the information.

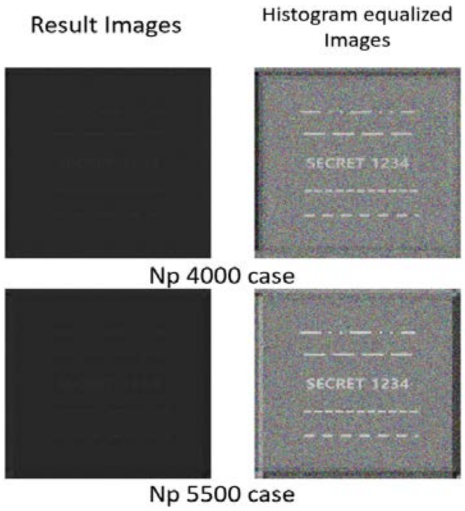

Figure 10. DRPE with merging reconstruction method result images.

However, using our proposed method, we can observe the word with more clarity, in comparison to the conventional method, as shown in Fig. 10. It is difficult to determine the difference between the two results; therefore, we evaluate the image quality using various performance metrics.

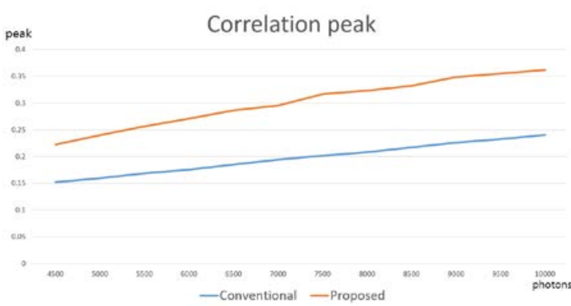

Figure 11. Correlation peak analysis data.

We test the correlation peak using the result image, which has 4000–7000 photons. Furthermore, we obtain the peak to noise signal ratio (PSNR), mean square error (MSE), and structural similarity (SSIM), as below.

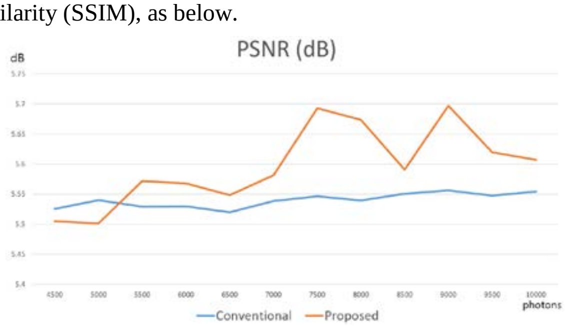

Figure 12. Peak to signal noise ratio analysis data.

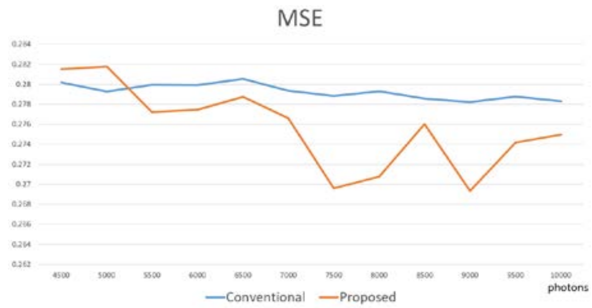

Figure 13. Mean square error analysis data.

Figure 14. Structural similarity analysis data.

According to Figs. 11–14, our proposed method demonstrates better performance than the conventional method. Specifically, our proposed method exhibits a higher correlation peak value in this simulation.

In addition, we apply our method to a quick response (QR) code. The reconstruction depth is the same as the previous simulation. We detect 10000–100000 because it is difficult to visualize the whole QR code with a few estimated photons; therefore, we detect more photons than the previous simulation. Figure 15 shows the conventional DRPE result images.

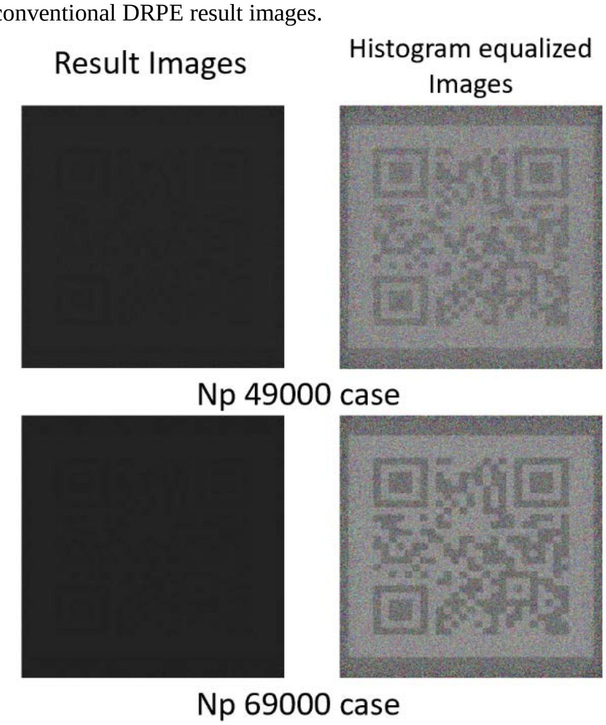

Figure 15. Conventional method QR code result images.

We generate the resulting image with 49000 photons. However, we cannot recognize the QR code image using the conventional reconstruction method. To attempt to visualize the QR code, we detect more photons, approximately 69000; however, the QR code image still cannot be visualized.

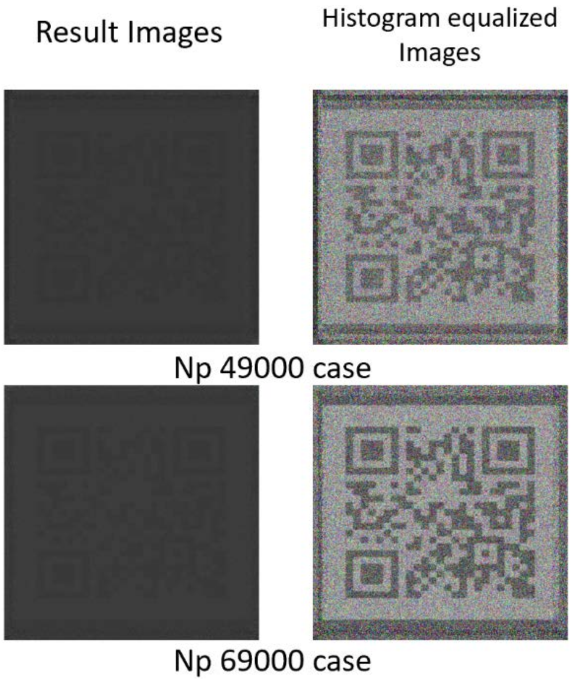

Figure 16. Proposed method QR code result images.

Figure 16 shows the resulting images for the proposed method. We can faintly observe the QR code shape using 49000 photons. When we increase the number of photons, we can accurately obtain the QR code shape. To verify the visual quality of the resulting images, we implement the correlation peak analysis, as shown in Fig. 17.

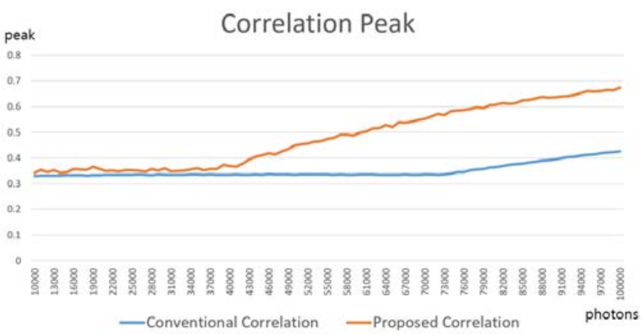

Figure 17. QR code result correlation peak plot.

As observed in Fig. 17, our proposed method shows high correlation values. Until the use of 35000 photons, it is difficult for both methods to recognize the QR code in the image. The conventional method cannot recognize the QR code until 73000 photons; however, our proposed method is able to recognize the QR code even when 34000 photons are used. Additionally, we plot the 2D correlation peak for 79000 photons, as shown in Fig. 18.

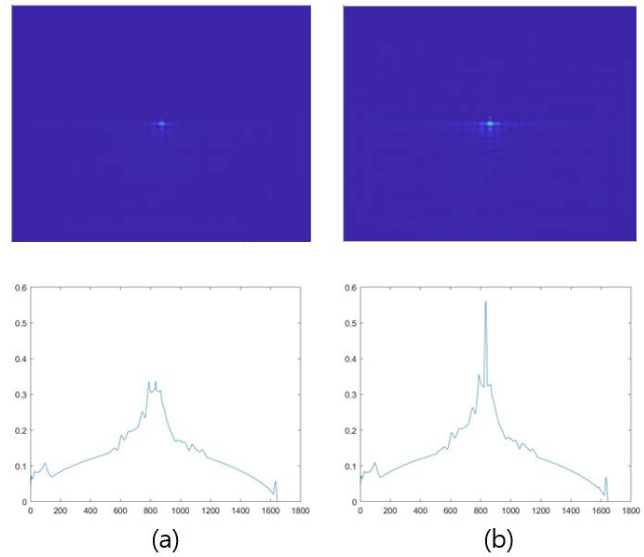

Figure 18. 2D correlation peak. (a) conventional method result, (b) proposed method result.

The 2D correlation peak plot for our proposed method shows a higher value than that of the conventional method. This indicates that our proposed method is better able to visualize the original image data, compared with the conventional method. To verify that our method can enhance the image quality, we evaluate the image quality using the same performance metrics used for the conventional method and calculate the average value of each metric. Table 1 shows the result of the performance metrics.

Table 1. Image test result of QR code image.

	Correlation	PSNR(dB)	MSE	SSIM
Conventional	0.3497	5.046	0.3135	0.0880
Proposed	0.5007	5.067	0.3111	0.1011

Table 1 shows that our method can improve on the image quality obtained by the conventional method. To summarize, we presented two simulations to verify the performance of our method, which is able to clearly visualize the original data, even if sparse estimated photons are used.

4. Conclusion

In this paper, we presented the PDRPE technique with the merging reconstruction method. The conventional method showed a good performance in encrypting data; however, it was unable to restore the original input image under photon-starved conditions. Our proposed method can visualize the original image better, compared with the conventional method; it also demonstrates enhanced image quality under the same conditions. Using the proposed method, we can effectively and securely keep information data. E-commerce systems are popular and most people transfer their personal information through their smartphones. We intend to use our technique to preserve data and we can also use it as an authentication method. In future work, we will apply this technique to encrypt fingerprints and human iris information. However, our proposed method has a limitation, i.e., the noise of the resulting image. The method cannot visualize information under severely photon-starved conditions. Therefore, we plan to do investigation for overcoming this limitation in a future study.

5. ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2017R1D1A1B03030343, NRF-2017K1A3A1A19070753).

6. REFERENCES

[1] P. Refregier, B. Javidi, 1995. “Optical image encryption based on input plane and Fourier plane random encoding,” Optics letters, vol.20, issue7, pp.767-769. DOI= https://doi.org/10.1364/OL.20.000767

[2] J.W.Goodman, 1985. Statistical optics (John Wiley and Sons, inc.), Chapter9

[3] Watson and G. M. Morris, 1990 “Comparison of infrared up conversion methods for photon-limited imaging,” Journal of Apply Physics, vol.67, pp.6075-6084. DOI= https://doi.org/10.1063/1.345167

[4] Elisabet Perez-Cabre, M. Cho, B. Javidi, 2011.“Information authentication using photon-counting double-random-phase encrypted images,” Optics letters, vol.36, issue1, pp.22-24.DOI= https://doi.org/10.1364/OL.36.000022

[5] Lippmann, Gabriel, 1908. "Epreuves reversibles. photographies integrals." Comptes-Rendus Academie des Sciences 146, pp.446-451

[6] Seung-Hyun Hong, Ju-Seog Jang, and Bahram Javidi, 2004."Three-dimensional volumetric object reconstruction using computational integral imaging." Optics Express vol.12, no.3, pp.483-491. DOI= https://doi.org/10.1364/OPEX.12.000483

[7] JS Jang, B. Javidi, 2002. "Three-dimensional synthetic aperture integral imaging," Optics letters, vol.27, issue13, pp.1144-1146 DOI= https://doi.org/10.1364/OL.27.001144

[8] B. Tavakoli, B. Javidi, 2008. “Three-dimensional visualization by photon counting computational Integral Imaging,” Optics Express, vol.16, issue7, pp.4426-4436. DOI= https://doi.org/10.1364/OE.16.004426

[9] J. Jung, M. Cho, 2010. “Three-dimensional photon counting integral imaging using bayesian estimation,” Optics Letters, vol.35, issue11, pp.1825-1827. DOI= https://doi.org/10.1364/OL.35.001825

[10] M. Cho, B. Javidi, 2012. “Three-dimensional photon counting integral imaging using moving array lens technique,”, Optics Letters, vol.37, issue9, pp.1487-1489. DOI= https://doi.org/10.1364/OL.37.001487

[11] M. Cho, 2015. “Three-dimensional color photon counting microscopy using Bayesian estimation with adaptive priori information,” Chinese optics letter, vol.13, issue7, pp.070301-070304

[12] M. Cho, B. Javidi, 2013. “Three-dimensional photon counting double-random-phase encryption,” Optics letters, vol.38, issue17, pp.3198-3201. DOI= https://doi.org/10.1364/OL.38.003198

[13] J.Y. Jang, Kotaro Inoue, Min-Chul Lee, M. Cho, 2016. “Information Authentication of Three-Dimensional Photon Counting Double Random Phase Encryption Using Nonlinear Maximum Average Correlation Height Filter,” Journal of the Optical Society of Korea, vol.20, no.2, pp.228-233

Authors' background

Your Name	Title*	Research Field	Personal website
Jaehoon Lee	Phd candidate	3D display, computational optics	https://ois3d.cse.kyutech.ac.jp/
Myungjin Cho	Associate professor	Integral imaging, computational optics, machine learning	3cholab.wordpress.com
Kotaro Inoue	Phd candidate	3D imaging, Optical security	kotaro-inoue.gitlab.io
Min-Chul Lee	Associate professor	Biomedical imaging, 3D imaging, computational optics, holography, 3D display	https://ois3d.cse.kyutech.ac.jp/

*This form helps us to understand your paper better, the form itself will not be published.

*Title can be chosen from: master student, Phd candidate, assistant professor, lecturer, senior lecturer, associate professor, full professor, research, senior research