Optical Encryption and Information Authentication of 3D Objects Considering Wireless Channel Characteristics

In-Ho Lee and Myungjin Cho*

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

(Received October 7, 2013 : revised October 15, 2013 : accepted October 16, 2013)

In this paper, we present an optical encryption and information authentication of 3D objects considering wireless channel characteristics. Using the optical encryption such as double random phase encryption (DRPE) and 3D integral imaging, a 3D scene with encryption can be transmitted. However, the wireless channel causes the noise and fading effects of the 3D transmitted encryption data. When the 3D encrypted data is transmitted via wireless channel, the information may be lost or distorted because there are a lot of factors such as channel noise, propagation fading, and so on. Thus, using digital modulation and maximum likelihood (ML) detection, the noise and fading effects are mitigated, and the encrypted data is estimated well at the receiver. In addition, using computational volumetric reconstruction of integral imaging and advanced correlation filters, the noise effects may be remedied and 3D information may be authenticated. To prove our method, we carry out an optical experiment for sensing 3D information and simulation for optical encryption with DRPE and authentication with a nonlinear correlation filter. To the best of our knowledge, this is the first report on optical encryption and information authentication of 3D objects considering the wireless channel characteristics.

Keywords : 3D optical encryption, Computational reconstruction, Wireless channel characteristics

OCIS codes : (100.6890) Three-dimensional image processing; (100.4992) Pattern, nonlinear correlators; (110.6880) Three-dimensional image acquisition

I. INTRODUCTION

In information security technologies, encryption has been widely researched [1-17]. In particular, optical encryption techniques [5-16] are helpful to protect the transmitted information. In addition, the speed of the optical encryption is faster than non-optical encryption methods. Double random phase encryption (DRPE) which is the one of the most widely used has been proposed [5]. However, it has a weak point when the decryption keys are used many times without being updated. To solve this problem, DRPE with photon counting imaging techniques has been reported [13]. It considers a photon-limited version of the encrypted distribution such as a Poisson distribution [18-20, 27] in a perfect channel environment. In addition, for 3D objects, three-dimensional (3D) photon counting double-random-phase encryption has been studied recently [26]. In this technique,

encrypted data transmission is not considered. It means that a perfect transmission channel is assumed. However, under practical conditions, the transmission channel is not perfect. There are many parameters which cause the noise of the transmitted information.

In particular, the wireless channel causes severe noise and fading effects of the transmitted information. Thus, when the encrypted data is transmitted via a wireless channel, there are a lot of factors such as channel noise, propagation fading, and so on [21-23]. To obtain the correct encrypted data at the receiver, it is necessary to digitally modulate the encrypted information at the transmitter and correctly detect the modulated signals at the receiver [21-23]. In addition, the nonlinear correlation filters may be used to recognize the primary information [24]. For 3D data encryption, computational volumetric reconstruction of integral imaging [25] may be used. Since this technique uses the superposition of all elemental images at a certain depth, the noise effect

*Corresponding author: mjcho@hknu.ac.kr

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

caused by the wireless channel may be remedied. Therefore, in this paper, we analyze the effects of a wireless channel for optical encryption data using digital modulation and maximum likelihood (ML) detection. Also, we reconstruct and authenticate 3D information at the receiver using computational volumetric reconstruction of integral imaging and nonlinear correlation filters. To the best of our knowledge, this is the first report on considering the wireless channel characteristics of the 3D optical encryption technique.

The paper is organized as follows. First we briefly present the 3D DRPE in Section II. Then, a wireless channel model is presented, and signal modulation and detection techniques are described in Section III. To show the effects of the wireless channel for optical encryption and the authentication of 3D information, experimental results are implemented in Section IV. Finally, we conclude the paper with a summary and future plans in Section V.

II. 3D OPTICAL ENCRYPTION: DOUBLE RANDOM PHASE ENCRYPTION USING INTEGRAL IMAGING

Optical encryption has many advantages such as parallel processing of optical systems, fast processing time, and data handling in various domains. One of the optical encryption methods, double random phase encryption (DRPE), uses two random phase information. Let us consider the encryption of a one-dimensional signal for simplicity. Figure 1 (a) shows the optical schematic setup of DRPE for encryption. Let $s(x)$ be the primary data. Then, for encryption, we use two uniformly distributed random noises over $[0, 1]$ which are $n_s(x)$ in the spatial domain and $n_f(\mu)$ in the spatial frequency domain. First, the random phase noise, $\exp[i2\pi n_s(x)]$ multiplies the primary data, $s(x)$. Then, this data passes through lens 1 which means the Fourier transform of $s(x)\exp[i2\pi n_s(x)]$. To obtain the convolution result between $s(x)\exp[i2\pi n_s(x)]$ and $h(x)$ where the Fourier transform of $h(x)$ is $\mathfrak{F}\{h(x)\}=\exp[i2\pi n_f(\mu)]$, Fourier transforms of $s(x)\exp[i2\pi n_s(x)]$ and $h(x)$ are multiplied by each other. Finally, the inverse Fourier transform of this data can be recorded through lens 2. That is, the encrypted data by DRPE, $s_e(x)$ is a complex value as the following: [13]

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

where $\mathfrak{F}$ and $\mathfrak{F}^{-1}$ mean Fourier transform and inverse Fourier transform, respectively. By the characteristics of the complex-valued function, encrypted data has amplitude and phase, i.e., $s_e(x) = |s_e(x)|\exp[i\phi(x)]$.

Figure 1 (b) illustrates the optical schematic setup of DRPE for decryption. To decrypt the primary data, encrypted data as shown in Eq. (1) is multiplied by complex-conjugate of Fourier transform of $h(x)$ as the following: [13]

$$s_d(x) = \left| \mathfrak{F}^{-1} \left\{ \mathfrak{F} [s_e(x)] \exp[-i2\pi n_f(\mu)] \right\} \right| \quad (2)$$

In integral imaging, multiple elemental images can be captured by a pickup process [25, 28] and their decrypted elemental images can be obtained by Eq. (2). Then, 3D computational reconstruction can be implemented by the following [25]:

$$I(x, z_r) = \frac{1}{O(x, z_r)} \sum_{i=0}^{K-1} s_d^i(x + i\Delta x) \quad (3)$$

where $\Delta x = N_x f p / (c_x z_r)$ is the shifting pixels for computational reconstruction of integral imaging, N_x is the total number of pixels for each elemental image, f is the focal length of pickup lens, p is the pitch between pickup lenses, c_x is the image sensor size in the x direction, z_r is the reconstruction depth, K is the number of elemental images in the x direction, and $O(x, z_r)$ is the overlapping factors among all elemental images at the reconstruction depth z_r .

III. TRANSMISSION OF OPTICAL ENCRYPTED DATA THROUGH WIRELESS CHANNEL

We consider an elemental image with size $M \times N$ as the encrypted signal for transmission through a wireless communication channel, and it is assumed that the receiver has

FIG. 1. Optical schematic setup of double-random-phase encryption technique for (a) encryption and (b) decryption.

perfect phase information of encrypted data, i.e., $\phi(x)$. Thus, in this paper, we focus on the transmission of only the amplitude of encrypted data. The amplitudes of encryption output from Eq. (1) can be expressed as an $M \times N$ matrix with normalized real values between 0 and 1, which is written as

$$|s_e(x)| = \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,N} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ v_{M,1} & v_{M,2} & \cdots & v_{M,N} \end{bmatrix} \quad (4)$$

where v_{ij} represents the normalized amplitude for the pixel at (i, j) on the $M \times N$ encrypted image. By sampling the normalized values in Eq. (4) with the sampling interval per dimension, L , the $M \times N$ encrypted matrix is shrunk to the $\lceil M/L \rceil \times \lceil N/L \rceil$ matrix, and then the shrunk matrix is transformed into a vector as follows:

$$\begin{bmatrix} v_{1,1} & v_{1,L+1} & \cdots & v_{1,LN_s+1} & v_{L+1,1} & v_{L+1,L+1} & \cdots & v_{L+1,LN_s+1} \\ \cdots & v_{LM_s+1,1} & v_{LM_s+1,L+1} & \cdots & v_{LM_s+1,LN_s+1} \end{bmatrix}^T \quad (5)$$

where $M_s = \lceil M/L \rceil - 1$, $N_s = \lceil N/L \rceil - 1$, T is the transpose of a matrix, and L can be adjusted according to available channel capacity.

For digital modulation, each normalized value in Eq. (5) is quantized with 16 uniform levels (i.e., 0, 1, 2, ..., and 15), and then the quantized values are respectively mapped into the corresponding 4-bits sequences. For instance, if $v_{ij}=0, 0.6$, and 1, then the quantized values are 0, 9, and 15, respectively, and the corresponding 4-bits sequences are 0000, 1001, 1111, respectively. In order to transmit the 4-bits sequences through a wireless channel, the 4-bits information is sequentially modulated with 16-ary square quadratic amplitude modulation (QAM), where a Gray code is used to assign 4-tuples with only one-bit difference to two adjacent signals in the QAM constellation [21].

In this paper, a wireless channel is assumed to be time-varying frequency-flat Rayleigh fading that is one of the most typical wireless channels [21-23]. Then, with the symbol duration, T , the received signal is expressed as

$$r(kT) = c(kT)s_{QAM}(kT) + \varepsilon(kT), k = 0, 1, \dots, \lceil M/L \rceil \lceil N/L \rceil - 1 \quad (6)$$

where $c(kT)$ denotes the complex coefficient of a time-varying frequency-flat Rayleigh fading channel with unit average power, $s_{QAM}(kT)$ represents the QAM-modulated signal with an average power, P , which is a transmit power at the transmitter, and $\varepsilon(kT)$ denotes the complex additive white Gaussian noise with zero mean and unit variance. Thus, the average signal-to-noise ratio (SNR) equals P . For generating the time-varying Rayleigh fading channel,

we use a Jakes model [22] with the parameters of a carrier frequency and a receiver speed.

In order to detect the transmitted signal at the receiver, the maximum likelihood (ML) detection [23] is adopted as follows:

$$\tilde{s}_{QAM}(kT) = \arg \min_{Q \in \{s_{QAM,1}, s_{QAM,2}, \dots, s_{QAM,16}\}} \{|r(kT) - \tilde{c}(kT)Q|\} \quad (7)$$

where $\tilde{s}_{QAM}(kT)$ is the estimated QAM signal, $s_{QAM,q}$ is the q th signal among 16 possible QAM signals, and $\tilde{c}(kT)$ is the estimated channel coefficient. In this paper, we consider perfect channel estimation, i.e., $\tilde{c}(kT) = c(kT)$, and no channel estimation, i.e., $\tilde{c}(kT) = 1$. The estimated signals obtained from ML detection are sequentially mapped into the corresponding 4-bits sequences, using the same QAM constellation as used at the transmitter. Then, the estimated 4-bits sequences are changed into the corresponding quantization values, respectively, and the $\lceil M/L \rceil \times \lceil N/L \rceil$ matrix is constructed using the normalized values of the obtained quantization ones. Finally, the $\lceil M/L \rceil \times \lceil N/L \rceil$ matrix is expanded into the $M \times N$ matrix with inserting zeros, which is expressed as

$$|\tilde{s}_e(x)| = \begin{bmatrix} \tilde{v}_{1,1} & 0 & \cdots & 0 & \tilde{v}_{1,L+1} & \cdots & \tilde{v}_{1,LN_s+1} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \tilde{v}_{L+1,1} & 0 & \cdots & 0 & \tilde{v}_{L+1,L+1} & \cdots & \tilde{v}_{L+1,LN_s+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \tilde{v}_{LM_s+1,1} & 0 & \cdots & 0 & \tilde{v}_{LM_s+1,L+1} & \cdots & \tilde{v}_{LM_s+1,LN_s+1} \end{bmatrix} \quad (8)$$

where $\tilde{v}_{i,j}$ is the estimated value for the (i,j) th normalized value of the $M \times N$ encrypted matrix in Eq. (4).

For integral imaging, the amplitudes of encrypted multiple images with size $M \times N$ are sequentially transmitted over a wireless channel. Thus, the receiver can successively obtain $|\tilde{s}_e(x)|$ in Eq. (8) for each encrypted image.

IV. OPTICAL EXPERIMENT AND SIMULATION RESULTS

Figure 2 shows the optical setup for recording 3D objects. To record multiple 2D images optically, we used synthetic aperture integral imaging (SAII). We capture 8×8 elemental images which have $2496(H) \times 1664(V)$ pixels. The focal length of the pickup camera is 50 mm. The pitch between cameras is 2 mm.

Figures 3 and 4 show the experimental results for 2D/3D optical encryption with wireless channel. In the 3D encrypted data transmission simulation, we used the wireless channel parameters as SNR is -20 dB and 20 dB,

FIG. 2. Optical setup for recording 3D objects using synthetic aperture integral imaging.

FIG. 3. Experimental results of optical encryption for 2D images using double random phase encryption. (a) primary image, (b) encrypted 2D image, (c) decrypted 2D image with 20 dB SNR using channel estimation, (d) decrypted 2D image with 20 dB SNR using no channel estimation, (e) decrypted 2D image with -20 dB SNR using channel estimation, and (f) decrypted 2D image with -20 dB SNR using no channel estimation.

the carrier frequency is 2GHz, the receiver speed is 3km/h, the symbol duration, T , is 0.1ms, and the sampling interval per dimension, L , is 3. As shown in Fig. 3(a), two different objects (true class: car, false class: tank) with different depths (car: 290 mm and tank: 340 mm) are used as primary images. The encrypted 2D elemental image by using Eq. (1) is shown in Fig. 3(b). It seems the noise-like image. Using Eq. (2) and Eqs. (4)-(8), the decrypted 2D elemental

FIG. 4. Experimental results of optical encryption for 3D images using double random phase encryption. (a) true class (car) result; original 3D image reconstruction and enlarged image (left), reconstructed 3D image with 20 dB and -20 dB SNRs using channel estimation (front), and reconstructed 3D image with 20 dB and -20 dB SNRs using no channel estimation (right). (b) false class (tank) result; original 3D image reconstruction and enlarged image (left), reconstructed 3D image with 20 dB and -20 dB SNRs using channel estimation (front), and reconstructed 3D image with 20 dB and -20 dB SNRs using no channel estimation (right).

images with various wireless channel environments and no channel estimation as shown in Fig. 3(d) and (f) can be generated. In addition, the decrypted 2D elemental images with channel estimation as shown in Fig. 3(c) and (e) can be estimated. They are still not recognizable. However, using Eq. (3) which is 3D computational reconstruction of integral imaging, the reconstructed 3D images can be obtained as shown in Fig. 4. In Fig. 4(b), tank images are darker because it has lower light intensity. As shown in Fig. 4, the reconstructed 3D images with channel estimation have higher visual quality than the one without channel estimation. However, in -20 dB SNR case, both of them have almost the same visual quality.

To compare the performance of our method, the k th-law nonlinear correlation filter [24] and peak correlation energy (PCE) are introduced. The nonlinear correlation filter is designed by the following [24]:

$$c(x) = \Im^{-1} \left[\left[\Im \{ I(x, z_r) \} \Im \{ I_{ref}(x, z_{ref}) \} \right]^k \exp \{ i(\phi(\mu) - \psi(\mu)) \} \right] \quad (9)$$

where $I_{ref}(x, z_{ref})$ is the reference 3D image at reference

reconstruction depth, z_{ref} , $\phi(m)$ is the phase information of the reconstructed 3D image, $I(x, z_r)$, $\psi(m)$ is the phase information of the reference 3D image, and k is the nonlinear coefficient.

Then, to select the optimum k value of this correlation filter, we used PCE as defined by:

$$PCE = \frac{\max \left[|c(x)|^2 \right]}{\sum_{i=1}^N |c(x_i)|^2} \quad (10)$$

Figure 5 illustrates the correlation results of 3D reconstructed images for each wireless channel environment. The reference reconstruction depth is $z_{ref}=290$ mm (car). Thus, in Fig. 5, the highest PCE value can be observed at $z=290$ mm for each wireless channel environment. In Fig. 5, maximum PCE values are 0.9087×10^{-3} (-20 dB SNR, channel estimation), 0.8094×10^{-3} (-20 dB SNR, no channel estimation), 2.7475×10^{-3} (20 dB SNR, channel estimation), and 1.4363×10^{-3} (20 dB SNR, no channel estimation) at reconstruction depth $z_r=290$ mm. For wireless channel environment with 20 dB SNR and channel estimation, PCE value is the highest. However, for wireless channel environment with -20 dB SNR, PCE values of both channel estimation and no channel estimation are almost the same. It means that

FIG. 5. Peak Correlation Energy (PCE) value of the reconstructed 3D images for various wireless channel environments via various reconstruction depths.

FIG. 6. Peak Correlation Energy (PCE) value of the decrypted 2D images for various wireless channel environments via various reconstruction depths.

the channel estimation is not efficient for the case of the severe noise environment or the low transmit power.

On the other hand, Fig. 6 shows the correlation results of 2D decrypted images for each wireless channel environment. The reference image is the primary image as shown in Fig. 3(a). In Fig. 6, PCE values are 0.1613×10^{-3} (-20 dB SNR, channel estimation), 0.1720×10^{-3} (-20 dB SNR, no channel estimation), 0.4243×10^{-3} (20 dB SNR, channel estimation), and 0.1959×10^{-3} (20 dB SNR, no channel estimation) at all reconstruction depths, because 2D images do not have any depth information.

Figures 7 and 8 show the nonlinear correlation results ($k=0.3$) of the reconstructed 3D images for true and false classes with and without channel estimation. As shown in Fig. 7(c), the highest correlation peak can be observed for the reconstructed 3D image with 20 dB SNR and channel estimation of true class. In addition, correlation peaks for

FIG. 7. Nonlinear correlation results ($k=0.3$) of the reconstructed 3D images for true class with and without channel estimation.

FIG. 8. Nonlinear correlation results ($k=0.3$) of the reconstructed 3D images for false class with and without channel estimation.

the reconstructed 3D images with -20 dB SNR using channel estimation and no channel estimation are similar to each other. Thus, channel estimation is inefficient for the -20 dB SNR case. For the false case, the flat correlation results can be achieved as shown in Fig. 8. Therefore, it proves that our proposed method can authenticate the 3D information of optically encrypted objects.

V. CONCLUSION

In this paper, we have presented the optical encryption and information authentication of 3D objects with wireless channel characteristics. The wireless channel environment has several factors such as channel noise, channel fading, and so on. Using digital modulation and ML detection, we have estimated the encrypted information transmitted over a wireless channel and then decrypted the primary image at the receiver. In addition, introducing the computational volumetric reconstruction of 3D integral imaging, 3D information of the primary image can be obtained. This reconstruction method may remedy the residual noise after ML detection. We have proven that our method can effectively mitigate wireless channel effects by using 3D optical encryption technique and carrying out the simulation of wireless transmission. Also, our method shows that the performance of information authentication for optical encryption is improved using nonlinear correlation filters. In future plans, we will consider more wireless channel parameters and study various modulation and estimation methods. In addition, we will apply our method to various three-dimensional imaging or photon counting encryption techniques.

REFERENCES

1. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. on Info. Th.* **39**, 1639-1646 (1993).
2. C. Rackoff and D. Simon, "Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack," *Proc. Crypto' 91*, 433-444 (1991).
3. 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).
4. H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Proc. Crypto' 87* (Santa Barbara, USA, 1987), pp. 341-349.
5. P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767-769 (1995).
6. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," *Appl. Opt.* **38**, 7288-7293 (1999).
7. T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Appl. Opt.* **39**, 4783-4787 (2000).
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. 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).
10. 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).
11. 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).
12. 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).
13. E. Perez-Cabre, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.* **36**, 22-24 (2011).
14. T. Sarkadi and P. Koppa, "Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys," *Appl. Opt.* **51**, 745-750 (2012).
15. T. Ujvári, P. Koppa, M. Lovasz, P. Varhegyi, S. Sajti, E. Lorincz, and P. Richter, "A secure data storage system based on phase-encoded thin polarization holograms," *J. Opt. Pure Appl. Opt.* **6**, 401-411 (2004).
16. P. Koppa, "Phase-to-amplitude data page conversion for holographic storage and optical encryption," *Appl. Opt.* **46**, 3561-3571 (2007).
17. Z. Liu, M. Yang, W. Liu, S. Li, M. Gong, W. Liu, and S. Liu, "Image encryption algorithm based on the random local phase encoding in gyrator transform domains," *Opt. Commun.* **285**, 3921-3925 (2012).
18. J. W. Goodman, *Statistical Optics* (Wiley & Sons, Inc., New York, USA, 1985).
19. G. M. Morris, "Scene matching using photon-limited images," *J. Opt. Soc. Am. A* **1**, 482-488 (1984).
20. E. A. Watson and G. M. Morris, "Imaging thermal objects with photon-counting detector," *Appl. Opt.* **31**, 4751-4757 (1990).
21. F. Xiong, *Digital Modulation Technique* (Artech House, Norwood, USA, 2000).
22. M. Patzold, *Mobile Fading Channels* (John Wiley & Sons, New York, USA, 2002).
23. J. G. Proakis and M. Salehi, *Digital Communications* (McGraw-Hill, New York, USA, 2008).
24. B. Javidi, "Nonlinear matched filter based optical correlation," *Appl. Opt.* **28**, 4518-4520 (1989).
25. S.-H. Hong, J.-S. Jang, and B. Javidi, "Three-dimensional volumetric object reconstruction using computational integral imaging," *Opt. Express* **12**, 483-491 (2004).
26. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.* **38**, 3198-3201 (2013).
27. S. Yeom, Y.-H. Woo, and W.-W. Baek, "Distance extraction by means of photon-counting passive sensing," *J. Opt. Soc. Korea* **15**, 357-361 (2011).
28. J. Kim, J.-H. Jung, J. Hong, J. Yeom, and B. Lee, "Elemental image generation method with the correction of mismatch error by sub-pixel," *J. Opt. Soc. Korea* **16**, 29-35 (2012).