Optical Image Encryption and Decryption Considering Wireless Communication Channels

Myungjin Cho* and In-Ho Lee*

Abstract—In this paper, we discuss optical encryption and decryption considering wireless communication channels. In wireless communication systems, the wireless channel causes noise and fading effects of the transmitted information. Optical encryption technique such as double-random-phase encryption (DRPE) is used for encrypting transmitted data. When the encrypted data is transmitted, the information may be lost or distorted because there are a lot of factors such as channel noise, propagation fading, etc. 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. To the best of our knowledge, this is the first report that considers the wireless channel characteristics of the optical encryption technique.

Keywords—Optical Encryption and Decryption, Wireless Communication Channels

1. INTRODUCTION

In information communication technologies, encryption has been researched widely [1-17]. Optical encryption techniques [5-16] have higher encryption speed than non-optical encryption methods. Optical encryption with digital holography [18] generates two holograms for the encrypted data and the key information; thus enabling secure storage and data transmission. Another optical encryption method, which is polarization encryption of holography [19], can encrypt original holographic data as two-dimensional polarization distribution. Both optical encryption techniques mentioned above need an optical holographic recording system. Thus, they require a complicated system structure. On the other hand, double-random-phase encryption (DRPE), which is one of the most widely used, has a simple system structure [5]. Note, however, that it has a weak point when the decryption keys are used many times without being updated. To address this problem, DRPE with photon-counting imaging techniques has been reported [13]. It considers a photon-limited version of the encrypted distribution such as Poisson distribution [20-22] in a perfect channel environment.

In wireless communication systems, the wireless channel induces noise and fading effects of the transmitted information. Thus, in this paper, we analyze the wireless communication systems for optical encryption data. When the encrypted data is transmitted via a wireless channel, the transmitted data is distorted by a lot of factors such as channel noise, propagation fading, etc. [23-25]. Obtaining the correct encrypted data at the receiver requires digitally modulating the encrypted information at the transmitter and correctly detecting the modulated signals at the receiver [23-25]. In addition, non-linear correlation filters may be used to recognize the primary information [26]. To the best of our knowledge, this is the first report that considers the wireless

Manuscript received on July 19, 2013; accepted on October 22, 2013.

Corresponding Author : In-Ho Lee (ihlee@hknu.ac.kr)

* Dept. of Electrical, Electronic, and Control Engineering, Hankyong National University, Anseong, 456-749, Korea (mjcho@hknu.ac.kr, ihlee@hknu.ac.kr)

channel characteristics of the optical encryption technique.

The rest of this paper is organized as follows: First, we briefly discuss DRPE in Section 2; The characteristics of the wireless communication channel are analyzed, and signal modulation and detection techniques are described in Section 3; To show the effects of wireless channel for optical encryption, experimental results are presented in Section 4; Finally, we conclude the paper with a summary as well as future plans in Section 5.

2. OPTICAL ENCRYPTION: DOUBLE-RANDOM-PHASE ENCRYPTION

Optical encryption has many advantages such as parallel processing of optical systems, short processing time, and data handling in various domains (e.g., spatial and frequency domains). One of the optical encryption methods, double-random-phase encryption (DRPE), uses double-random-phase information. Let us consider the encryption of one-dimensional signal for simplicity. 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 spatial domain and $n_f(\mu)$ in spatial frequency domain. First, random-phase noise $\exp[i2\pi n_s(x)]$ multiplies primary data $s(x)$. Then, function $h(x)$ convolves $s(x)\exp[i2\pi n_s(x)]$ where the Fourier transform of $h(x)$ is $\mathfrak{F}\{h(x)\}=\exp[i2\pi n_f(\mu)]$. In other words, the encrypted data by DRPE, $s_e(x)$, is complex-valued as follows: [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 the Fourier transform and inverse Fourier transform, respectively. By the characteristics of a complex-valued function, the encrypted data has amplitude and phase, $s_e(x) = |s_e(x)|\exp[i\phi_e(x)]$.

To decrypt the primary data, the encrypted data shown in Eq. (1) is multiplied by the complex-conjugate of Fourier transform of $h(x)$ as follows: [13]

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

3. TRANSMISSION OF OPTICAL ENCRYPTED DATA THROUGH WIRELESS COMMUNICATION CHANNEL

We consider an $M \times N$ image as the encrypted signal for transmission through a wireless communication channel. Therefore, the encryption output from Eq. (1) can be expressed as an $M \times N$ matrix with normalized real values between 0 and 1, written as:

$$s_e = \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,N} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ v_{M,1} & v_{M,2} & \cdots & v_{M,N} \end{bmatrix} \quad (3)$$

where $v_{i,j}$ represents the normalized value for pixel at (i, j) on the $M \times N$ encrypted image. By sampling the normalized values in Eq. (3) 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; the shrunk matrix is then transformed into a vector as follows:

$$\begin{bmatrix} v_{1,1} & v_{1,L+1} & \cdots & v_{1,LN_s+1} & v_{L+1,1} & v_{L+1,L+1} & \cdots & v_{L+1,LN_s+1} & \cdots & v_{LM_s+1,1} & v_{LM_s+1,L+1} & \cdots & v_{LM_s+1,LN_s+1} \end{bmatrix}^T \quad (4)$$

where $M_s = \lceil M/L \rceil - 1$ and $N_s = \lceil N/L \rceil - 1$.

For digital modulation, each normalized value in Eq. (4) is quantized with uniform 16 levels (i.e., 0, 1, 2, ..., and 15), and the quantized values are then respectively mapped into the corresponding 4-bit sequences. For instance, if $v_{i,j} = 0, 0.6$, and 1, then the quantized values are 0, 9, and 15, respectively, and the corresponding 4-bit sequences are 0000, 1001, and 1111, respectively. To transmit the 4-bit sequences through a wireless channel, the 4-bit 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 [23].

In this paper, a wireless channel is assumed to be time-varying, frequency-flat Rayleigh fading. Therefore, with symbol duration T , the received signal is expressed as:

$$r(kT) = c(kT)s_{QAM}(kT) + \varepsilon(kT), \quad k = 0, 1, \dots, \lceil M/L \rceil \lceil N/L \rceil - 1 \quad (5)$$

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 average power P , 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 . To generate the time-varying Rayleigh fading channel, we use a Jakes model [24] with parameters, a carrier frequency, and a receiver speed.

To detect the transmitted signal at the receiver, maximum likelihood (ML) detection [25] is adopted as follows:

$$\tilde{s}_{QAM}(kT) = \arg \min_{s_{QAM,q} \in \{s_{QAM,1}, s_{QAM,2}, \dots, s_{QAM,16}\}} \|r(kT) - \tilde{c}(kT)s_{QAM,q}\| \quad (6)$$

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-bit sequences using the same QAM constellation as that used at the transmitter. Therefore, the estimated 4-bit sequences are changed into the corresponding quantization values, 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 by inserting zeroes, expressed as:

$$\tilde{S}_e = \begin{bmatrix} \tilde{v}_{1,1} & 0 & \cdots & 0 & \tilde{v}_{1,L+1} & \cdots & \tilde{v}_{1,LN_s+1} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \tilde{v}_{L+1,1} & 0 & \cdots & 0 & \tilde{v}_{L+1,L+1} & \cdots & \tilde{v}_{L+1,LN_s+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \tilde{v}_{LM_s+1,1} & 0 & \cdots & 0 & \tilde{v}_{LM_s+1,L+1} & \cdots & \tilde{v}_{LM_s+1,LN_s+1} \end{bmatrix} \quad (7)$$

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. (3).

4. EXPERIMENTAL RESULTS

Figure 1 shows the experimental results for optical encryption with the wireless communication channel. In this experiment, we used the following wireless communication system parameters: SNR of -20dB ~ 20dB, carrier frequency of 2GHz, receiver speed of 3km/h, symbol duration T of 0.1ms, and sampling interval per dimension L of 3. As shown in Fig. 1(a), two different cars (true and false classes for pattern recognition) are used as primary images. Therefore, using Eq. (1), the encrypted images can be generated as depicted in Fig. 1(b). Now, we consider the wireless channel for transmission. From Eqs. (2) to (7), decrypted images with noise and wireless channel fading can be obtained as shown in Figs. 1(c) and (d). We find that the decrypted images with perfect channel estimation have better quality than those without channel estimation.

To show the ability of pattern recognition for wireless transmission, we used non-linear correlation filters [26] such as the k th-law non-linear filter. Figure 2 illustrates the correlation results for each class (true and false classes with and without channel estimations). Fig. 2(a) has the highest correlation peak than others since it is the true class with perfect channel estimation. Without channel estimation, the correlation peak is shrunk as shown in Fig. 2(b). For decrypted images of false class in Figs. 2(c) and (d), there are no peaks on correlation planes. Thus, we can prove that pattern recognition can be implemented in optical encryption with the wireless communication channel by Fig. 2.

To evaluate our method for pattern recognition, we used peak to correlation energy (PCE) [22] as a performance metric. Figure 3 shows the PCE results for each non-linearity (k) of correlation filters. As shown in Fig. 3, decrypted images for true class with perfect channel estimation have the highest PCE values. It implies that the wireless communication of optical encryption with perfect channel estimation has better performance than others. Using our method, information authentication will be implemented correctly.

Fig. 1. Experimental results for true and false classes with 20dB SNR. (a) Primary images, (b) Encrypted images with DRPE, (c) Decrypted images without channel estimation, and (d) Decrypted images with channel estimation

Fig. 2. Non-linear correlation results with 20dB SNR for (a) true class with channel estimation, (b) true class without channel estimation, (c) false class with channel estimation, and (d) false class without channel estimation

Fig. 3. Peak to Correlation Energy for (a) true class with channel estimation, (b) true class without channel estimation, (c) false class with channel estimation, and (d) false class without channel estimation

5. CONCLUSION

In this paper, we have presented the wireless communication of optical encryption with digital modulation and pattern recognition. In wireless communication systems, several factors such as channel noise, channel fading, etc., should be considered to detect correct primary signals. Thus, we have estimated the encrypted information using digital modulation and maximum likelihood detection. Through experiments, we have shown that our method can mitigate wireless channel effects and obtain better received signal for optical encryption. We believe that our method can be applied to wireless communications of optical encryption. In the future, 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. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639-1646, 1993.
- [2] C. Rackoff and D. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Advances in Cryptology: CRYPTO '91 (Lecture Notes in Computer Science Vol. 576)*, J. Feigenbaum, Ed. Heidelberg, Germany: Springer Berlin, 1992, pp. 433-444.
- [3] S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal on Selected Areas in Communication*, vol. 7, no. 4, pp. 467-473, 1989.
- [4] H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Advances in Cryptology: CRYPTO '87 (Lecture Notes in Computer Science Vol. 293)*, C. Pomerance, Ed. Heidelberg, Germany: Springer Berlin, 1988, pp. 340-349.
- [5] 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.
- [6] O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," *Applied Optics*, vol. 38, no. 35, pp. 7288-7293, 1999.
- [7] T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Applied Optics*, vol. 39, no. 26, pp. 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," *Optics & Laser Technology*, vol. 40, no. 4, pp. 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," *Optics and Lasers in Engineering*, vol. 50, no. 10, pp. 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," *Optics Communications*, vol. 283, no. 12, pp. 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," *Optics and Lasers in Engineering*, vol. 49, no. 4, pp. 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," *Applied Optics*, vol. 46, no. 26, pp. 6641-6647, 2007.
- [13] E. Pérez-Cabré, 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.
- [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] T. Ujvári, P. Koppa, M. Lovász, P. Várhegyi, S. Sajti, E. Lorincz, and P. Richter, "A secure data storage system based on phase-encoded thin polarization holograms," *Journal of Optics A: Pure and Applied Optics*, vol. 6, no. 4, pp. 401-411, 2004.
- [16] P. Koppa, "Phase-to-amplitude data page conversion for holographic storage and optical encryption," *Applied Optics*, vol. 46, no. 17, pp. 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," *Optics Communications*, vol. 285, no. 19, pp. 3921-3925, 2012.
- [18] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Optics Letters*, vol. 25, no. 1, pp. 28-30, 2000.
- [19] 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.
- [20] J. W. Goodman, *Statistical Optics*, New York, NY: Wiley, 1985.
- [21] G. M. Morris, "Scene matching using photon-limited images," *Journal of the Optical Society of America A*, vol. 1, no. 5, pp. 482-488, 1984.
- [22] E. A. Watson and G. M. Morris, "Imaging thermal objects with photon-counting detector," *Applied Optics*, vol. 31, no. 23, pp. 4751-4757, 1992.

- [23] F. Xiong, *Digital Modulation Techniques*. Boston, MA: Artech House, 2000.
- [24] M. Pätzold, *Mobile Fading Channels*. New York, NY: John Wiley & Sons, 2002.
- [25] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. Boston, MA: McGraw-Hill, 2008.
- [26] B. Javidi, "Nonlinear matched filter based optical correlation," *Applied Optics*, vol. 28, no. 21, pp. 4518-4520, 1989.

Myungjin Cho

He received his BS and MS degrees in telecommunication engineering from Pukyong National University, Pusan, Korea in 2003 and 2005, respectively, and MS and PhD in Electrical and Computer Engineering from the University of Connecticut, Storrs, Connecticut, USA in 2010 and 2011, respectively. He is an assistant professor at Hankyong National University in Korea. He worked as researcher at Samsung Electronics in Korea from 2005 to 2007. His research

interests are 3D display, 3D signal processing, 3D biomedical imaging, 3D photon-counting imaging, 3D information security, 3D object tracking, and 3D underwater imaging.

In-Ho Lee

He received his BS, MS, and PhD degrees in electrical engineering from Hanyang University, Ansan, Korea in 2003, 2005, and 2008, respectively. He worked for LTE-Advanced standardization in Samsung Electronics Co., from 2008 to 2010. He was a Post-Doctoral Fellow at 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 of Hankyong National University, Anseong, Korea. His present research interests include link-level analysis in multi-hop relaying systems with multiple antennas and precoder design in MIMO systems.