Security analysis of quadratic phase based cryptography

Inbarasan Muniraj[1], Changliang Guo[1], Ra'ed Malallah[1, 2], John J Healy[1], John T Sheridan[1]*
[1]School of Electrical and Electronic Engineering, IOE[2], University College Dublin, Ireland.
[2]Physics Department, Faculty of Science, University of Basrah, Garmat Ali, Basrah, Iraq.
Corresponding Author: *john.sheridan@ucd.ie*

ABSTRACT

The linear canonical transform (LCT) is essential in modeling a coherent light field propagation through first-order optical systems. Recently, a generic optical system, known as a Quadratic Phase Encoding System (QPES), for encrypting a two-dimensional (2D) image has been reported. It has been reported together with two phase keys the individual LCT parameters serve as keys of the cryptosystem. However, it is important that such the encryption systems also satisfies some dynamic security properties. Therefore, in this work, we examine some cryptographic evaluation methods, such as *Avalanche Criterion* and *Bit Independence,* which indicates the degree of security of the cryptographic algorithms on QPES. We compare our simulation results with the conventional Fourier and the Fresnel transform based DRPE systems. The results show that the LCT based DRPE has an excellent avalanche and bit independence characteristics than that of using the conventional Fourier and Fresnel based encryption systems.

Keywords: Quadratic Phase Encoding system, linear Canonical transform, Double Random Phase Encryption.

1. INTRODUCTION

The ubiquitous use of multimedia communication systems and the risk of attacks on, the resulting theft of private data from secured systems have led to the demand for ever improving information security techniques. Techniques such as steganography and watermarking have been proposed in which data is hidden; on the other hand, data may be encrypted making it difficult to access without some key or keys [1-3]. Often both processes, i.e., hiding and encryption, are simultaneously employed. Among them, a technique proposed by Refregier *et al* [4], known as Double Random Phase Encryption (DRPE), using 4*f* optical processor has received a greater attention. Principally, this algorithm turns an intensity image into an unreadable format by using two statistically distributed random phase keys that are employed at the spatial and the Fourier domains, respectively. The resulting encrypted data is complex and it cannot disclose any information without decrypting the information using the correct phase keys [4]. In addition to this conventional technique, some its extensions have also been examined in the fractional Fourier domain [5], the Fresnel transform domain [6], the Hartley transform [7], and the Arnold transform based encoding systems [8]. Optical encryption techniques can be implemented as a cryptographic algorithm (digitally) and recently it is shown to be vulnerable for some organized attacks [9-12].

The linear canonical transform (LCT) is a three parameter (α, β, γ) group of linear integral transform, which can be used to model the propagation of the coherent wave field through the paraxial optical systems. Among its special cases are the Fourier transform (FT), the Fractional Fourier transform (FRT), the Fresnel Transform (FST), and the Gyrator Transform (GT) [13]. Since the conventional encryption technique has shown to be vulnerable for phase retrieval based attacks, [14, 15] such as Chosen Ciphertext Attack (CCA), Ciphertext Only Attacks (COA) and Known Plaintext-Ciphertext Attack (KPCA), Gopinath *et al* has proposed a generalized cryptosystem using Quadratic Phase Encoding System [16]. It has been reported that the data is encrypted, in the canonical transformation domain, with the help of two random phase masks, six transformation parameters or four propagation distances and two focal lengths.

Optics and Photonics for Information Processing X, edited by Khan M. Iftekharuddin, Abdul A. S. Awwal, Mireya García Vázquez, Andrés Márquez, Mohammad A. Matin, Proc. of SPIE Vol. 9970, 99700T · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2236644

In principle, the cryptographic algorithms should satisfy some dynamic properties such as Avalanche effect (AE), strict Avalanche effect (SAE), and Bit Independence criterion (BIC) which tell us the relationship between the plaintext and ciphertext [17-19]. To the best of our knowledge, to date, no avalanche effect or bit independence criterion have been investigated for the LCT based DRPE system. Therefore, in this work, we focus analyzing the avalanche effect and bit independence properties of DRPE in the linear Canonical domain. Furthermore, a comparison is made on the systems that based on the Fourier, Fresnel and canonical domain DRPE.

The rest of our paper is organized as follows: In Section 2, we present the backgrounds of the Fourier, the Fresnel and the linear Canonical transform based DRPE, respectively. Then, the concepts of avalanche effect and bit independence are presented in Section 3. In Section 4, we show our simulation results. Finally, we conclude our discussions in Section 5.

2. DOUBLE RANDOM PHASE ENCODING (DRPE)

2.1. The Fourier transform (FT) based DRPE

Optical and digital information security systems, based on double random phase encoding (DRPE) technique, have shown a predominant role in information security. Figure. 1 shows schematic setup of the amplitude encoding (AE) DRPE system [4, 20].

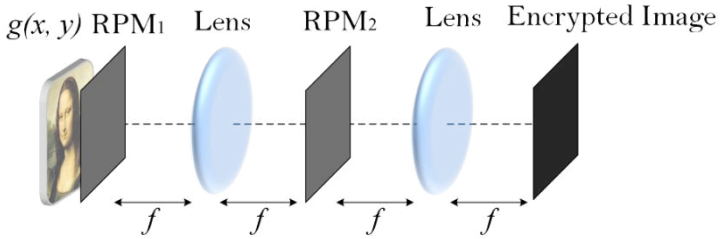

Fig. 1. Optical schematic setup for DRPE in the Fourier domain.

Initially, $g(x,y)$, represents the spatial coordinates of a two dimensional (2D) signal or an image, is being encrypted using two random phase masks. The random phase masks (RPMs) of spatial and frequency domain, $D_1(x,y) = \exp[i2\pi n_1(x,y)]$ and $D_2(x',y') = \exp[i2\pi n_2(x',y')]$ respectively. The phase keys $n_1(x,y), n_2(x',y')$ are statistically independent and uniformly distributed in $[-0.5, 0.5]$ [14, 15]. At first, the input image is multiple by the spatial phase mask, RPM_1, and then the Fourier transform ($\mathcal{F}$) is performed. Later, the resulting image is modulated by the second phase mask, RPM_2, in the frequency domain. Finally, by taking an inverse Fourier transform ($\mathcal{F}^{-1}$) we get the encrypted image, $E(x'', y'')$. Mathematically this process can be defined as follows [14],

$$E(x'', y'') = \mathcal{F}^{-1}\{\mathcal{F}[g(x,y)\times D_1(x,y)]\times D_2(x',y')\} \quad (1)$$

The encrypted image $E(x'', y'')$ is complex and due to the statistical properties of the two random phase masks, $D_1(x,y)$, and $D_2(x',y')$, it is unreadable.

2.2. The Fresnel transform (FST) based DRPE

We briefly analyze the concept of a lens-less optical DRPE encryption system, shown in Fig.2.

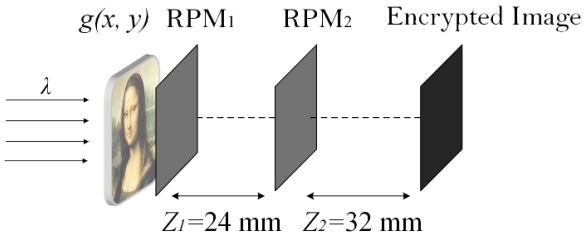

Fig. 2. Optical schematic setup for DRPE in the Fresnel domain.

As shown in Fig. 2, the entire system is illuminated by a plane wave with the operational wavelength λ. First, the primary amplitude image, $g(x,y)$, is modulated with the first random phase mask (RPM_1), which is kept at the input plane and represented as $\exp[in_1(x,y)]$. Then, the Fresnel propagated object wave field is further modulated by the second random phase mask (RPM_2), given by $\exp[in_2(x',y')]$ in the transformed domain. Here, the random phase keys $n_1(x,y)$and $n_2(x',y')$are statistically independent. Finally, the synthesized image produces the final encrypted data at the output plane. Under the Fresnel approximation [21], the encrypted image is given as follows:

$$E(x'',y'') = \Theta_\lambda\{u(x',y')\exp[in_2(x',y')]\,;z_2\}, \tag{2}$$

where $u(x',y') = \Theta_\lambda\{g(x,y)exp[in_1(x,y)];z_1\}$. The symbol Θ_λ stands for the Fresnel transform with respect to the operational wavelength λ at distances z_1 and z_2. Equation (1) shows that the security of an encrypted image $E(x'',y'')$ depends not only on the random phase masks (i.e., RPM_1, RPM_2) but also on the wavelength λ and the positions of the masks (z_1,z_2)[6].

2.3. The linear Canonical Transform (LCT) based DRPE

The LCT is a three-parameter class of linear integral transform and 2D separable LCT is defined as [22]:

$$LCT_{\alpha,\beta,\gamma}\{g(x,y)\} = \iint_{-\infty}^{\infty} g(x,y)\exp\{i\pi[\alpha(x^2+y^2) - 2\beta(ux+vy) + \gamma(u^2+v^2)]\}dxdy \tag{3}$$

Where α,β,γ represents the real canonical transform operators. We briefly describe LCT based AE DRPE system [15]. At first, the primary amplitude image, $g(x,y)$, is modulated with the first random phase mask (RPM_1), which is kept at the input plane, given as $D_1(x,y) = \exp[i2\pi n_1(x,y)]$. Subsequently, the propagated object wave is further modulated by the second random phase mask (RPM_2), given as $D_2(x,y) = \exp[i2\pi n_2(x',y')]$ in the canonical domain. Again, the random phase keys $n_1(x,y)$ and $n_2(x',y')$ are statistically independent. The final encrypted image $E(x'',y'')$ is expressed as follows [15]:

$$E(x'',y'') = L_{\alpha_2,\beta_2,\gamma_2}\{L_{\alpha_1,\beta_1,\gamma_1}\{g(x,y)D_1(x,y)\}\times D_2(x',y')\}. \tag{4}$$

The process of LCT based encryption (i.e., multiplying input image with the first phase mask) can be regarded as scaled FT with additional chirp multiplication $exp\{i\pi\gamma_1(x'^2+y'^2)\}$ [1]. Thus, Eq. (2) can be rewritten as,

$$E(x'',y'') = exp\{i\pi\gamma_2(x''^2+y''^2)\}\mathcal{F}\{\mathcal{F}(g(x,y)\times R_1')\times R_2'\}. \tag{5}$$

A schematic diagram of an optical implement of an LCT based AE DRPE system is given in Fig. 3.

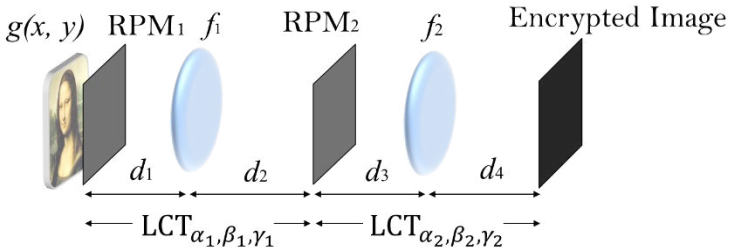

Fig. 3. Optical schematic setup for DRPE in the linear Canonical domain.

The encrypted image is a complex-valued data and resembles a noisy distribution. The decryption process involved, when using this LCT based DRPE system, is given by [15]:

$$g(x,y) = |\mathcal{F}^{-1}\{\mathcal{F}^{-1}\{E(x'',y'')\times\exp[-i\pi\gamma_2(x''^2+y''^2)]\}\times D_2^*\}|. \tag{6}$$

Where $\mathcal{F}^{-1}$ represents an inverse Fourier transform. As it can be seen in Fig. 3, in the LCT based DRPE system, together with the random phase masks (RPMs) also the individual LCT parameters $(\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2)$, which are defined by the system parameters, serve as keys of the cryptosystem. We note that the constants $(\alpha_1, \beta_1, \gamma_1)$ associated with the LCT can be related to the propagation distances d_1, d_2 and focal length f_1 by [15, 22]:

$$\alpha_1 = \frac{d_1 - f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]},$$
$$\beta_1 = \frac{f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]},$$
$$\gamma_1 = \frac{d_2 - f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]}. \tag{7}$$

Similarly, the relation between the second set of LCT parameters $(\alpha_2, \beta_2, \gamma_2)$ and f_2, d_3, d_4 follows those in Eq. 7. In the symmetric 2D separable case, the same parameter values (α, β, γ) are applied in both the horizontal (x) and vertical (y) directions [22].

3. SECURITY ANALYSIS

3.1. Avalanche Criterion (AVAC)

H. Feistel *et al* [23] has first defined the Avalanche Criterion (AVAC) as a desirable property for the Substitution and Permutation networks (SPNs). AVAC is then considered as an important cryptographic property, which says that even a tiny amount of changes in the plaintext (or key) leads to an "Avalanche changes" (i.e., drastic changes) in the ciphertext. Briefly, a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ satisfies AVAC, when a flipped single input bit changes, on average, half of the output bits [24, 25]. For instance, the conventional encryption method (E) can be described as: $C = E(X, K)$ where C represents the ciphertext X, K denotes the plaintext and the key, respectively. Suppose that, perturbation is made in the input texts such that $X \rightarrow X'$ or $K \rightarrow K'$, then the ciphertext will be changed (i.e., C') drastically. Then, the avalanche changes (also known as avalanche effects) can be measured using (two different strings of equal length) Hamming distance (H), which gives the number of changed bits. Let us assume a binary string value for ciphertext $C = 110011001100$ and perturbed ciphertext as $C' = 0011110101$, then the avalanche effect is measured using Hamming distance between C, C' as: $H(C, C') = H(110011001100, 0011110101) = 4$. In order to measure the avalanche effect (AE) that occurs in the encrypted image, when the input image bits are inverted, we use the following equation [19]:

$$AE = \frac{H(C, C')}{Num(C)}, \tag{8}$$

where $Num(C)$ represents the total number of binary bits in the Ciphertext (C) and C' denotes obtained ciphertext when perturbed input texts (i.e., X' or K') are used. We note that, if the value of AE is $\approx 50\%$ (meaning that approximately half of the bits in the ciphertext are changed when only few bit changed in either the plaintext or the keys) this usually means that a satisfactory avalanche effect [19].

3.2. Bit Independence Criterion (BIC)

A. F. Webster *et al* [26] defined the Bit Independence Criterion (BIC) for S-boxes. Briefly, a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ satisfies BIC, if a bit k in the input text (i.e., plaintext or key) is changed, it changes the output bits i and j in the ciphertext, independently. Let suppose that there are M bits in the plaintext and thus it can be changed M times, just by inverting one bit at a time. As a consequence, M different ciphertext can be obtained. Then, the bit independence (BI) between bit j and k in the ciphertext is defined using the absolute correlation coefficient value as [26]:

$$BI\left[C(b_i), C(b_j)\right] = |\text{corr}(\{b_i^1 \dots b_i^m \dots b_i^N\}, \{b_j^1 \dots b_j^m \dots b_j^N\})|, \quad (9)$$

where $C(b_i)$ and $C\left(b_j\right)$ represents the i^{th} and j^{th} bit in the ciphertext and b_i^m and b_j^m denote the values of the i^{th} and j^{th} bits in the ciphertext when the m^{th} bit in the plaintext is changed. We note that, if the value of $BIC\left[C(b_i), C(b_j)\right]$ is closer to 1 (i.e., unity) meaning that the compared bits are strongly correlated (i.e., very similar) else it is uncorrelated (i.e., independent). To measure the BIC on the encrypted image, we used the following expression [19]:

$$BIC[E(X,K)] = \max_{1 \le i,j \le N} BI\left[C(b_i), C\left(b_j\right)\right], \quad (10)$$

Where $i \neq j$ and we note that when $BIC[E(X,K)]$ is lesser than 1 (i.e., $BIC \ll 1$), the encryption satisfies the bit independence criterion.

4. SIMULATION RESULTS

Simulation results obtained, using the security analysis described in the previous section, are now presented. We used 50×50 pixels image (see Fig. 4(a)) in order to measure the avalanche effect and the bit independence. In order to analyze the proposed encryption methods (i.e., FT, FST, LCT based DRPE) in bit units, each pixel value in the input and the encrypted images (see Fig. 5) were converted into a binary representation. We used the standard IEEE 754 double-precision floating-point format (see Fig. 4(b)) to represent our pixel intensity values into the binary numbers [27]. This uses 64 bits (i.e., 1 sign bit, 11 bits for exponent width, and 52 bits for significant digits) as shown in Fig. We note that the sign, exponent bits are same for almost all amplitude values and therefore perturbation was considered only on the last 52 significant bits, without loss of generality [27].

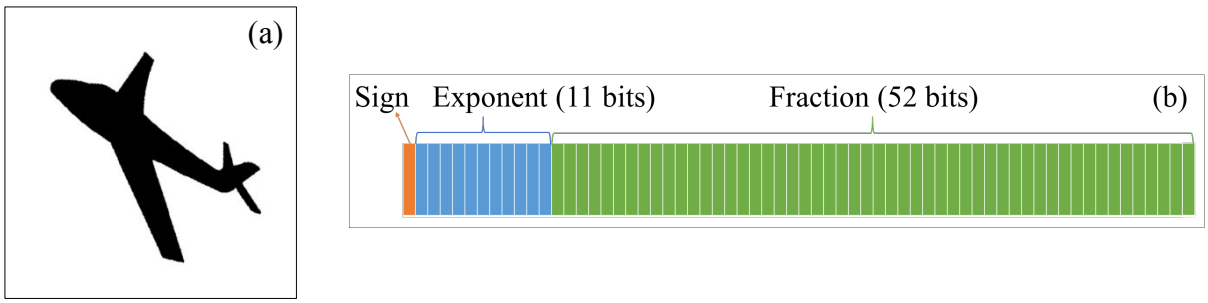

Fig. 4: (a) Grayscale test image used in our simulation and (b) IEEE 754 double-precision binary floating-point format [27].

Figure 5 shows the measured avalanche effect (AE) values, using Eq. (8), plotted against the varying number of flipped bits (i.e., bit units) in the plaintext of the DRPE system in the FT, FST, and LCT domains, respectively. Additionally, we also calculated the AE value, when some bits in the plaintext are perturbed, as a percentage of changed pixel (i.e., pixel values) in the encrypted image. It can be seen from Fig. 5 that the avalanche effect for the LCT based DRPE is better than that of in the Fourier and Fresnel domains. The AE value is 50% for DRPE in the LCT domain, while it is little lower than 50% in the Fresnel domain and when only fewer than 10 bits are flipped in the plaintext, DRPE in the Fourier domain achieves lower AE values. These results interpret the fact that when just 1 bit is inverted in the plaintext, almost all of the ciphertext values will change in the LCT, FST (few bits remain the same) based DRPE, while some of the pixel values would remain the same for DRPE in the Fourier domain. Especially, for the case when less than five bits are flipped in the plaintext we get AE value less than 40%. We note that the reason for this result is that the chirp function [22]. In the FST based DRPE, we use a one chirp function while in the LCT based DRPE we use two chirp functions and that helps the LCT and FST domain to achieve a satisfactory avalanche effect. Whereas, the chirp function becomes

unity in the Fourier domain [13]. As a consequence, the conventional FT based DRPE system did not achieve a satisfactory avalanche effect.

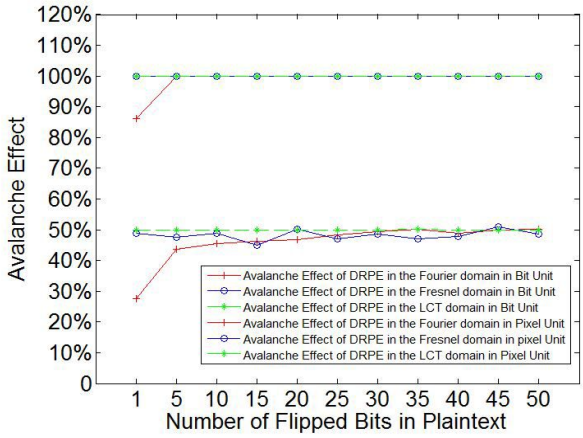

Fig. 5. Simulated results for the Avalanche effect with varying number of perturbed bits in the plaintext. Bit unit refers that the encrypted image is compared in binary units, the Pixel unit represents the encrypted image is compared as pixel values.

Figure 6 shows the calculated avalanche effect values plotted against the varying number of flipped bits in the first and second phase keys of the DRPE system in the FT, FST, and LCT domains, respectively. As it can be seen, when only one bit was flipped in the input keys (i.e., first or second phase key) we get similar AE values as we achieved in Fig. 5. Also, we note that the avalanche value for DRPE in the Fourier domain gets 50% only when more than 15 bits in the key for the first or second phase were flipped. Similarly, in the pixel values, DRPE in LCT, FST domains are stays at 100% while that in the FT based system increases to be 100% after about five bits in the phase keys are changed.

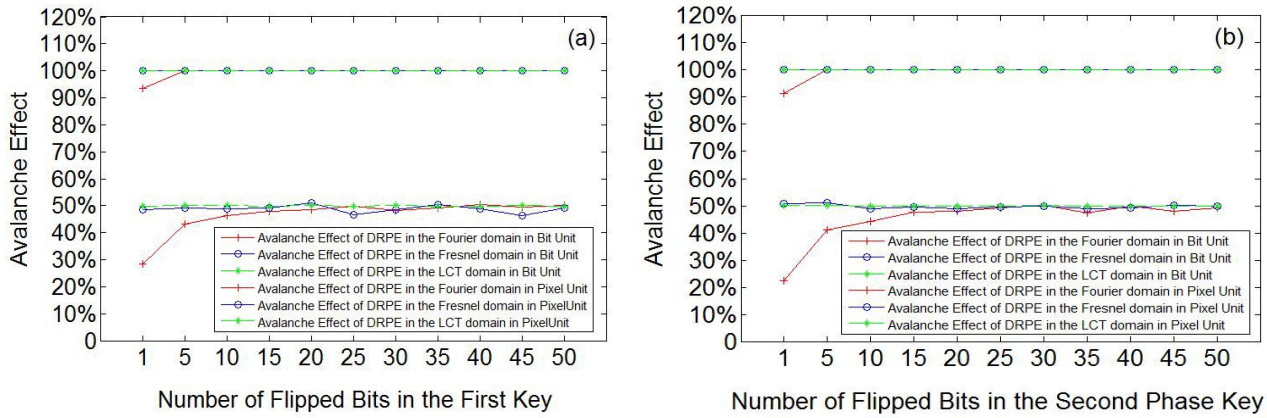

Fig. 6. Simulated results for the Avalanche effect with varying number of bits in the perturbed phase keys. (a) Avalanche effect with bits changed in the first phase key (b) Avalanche effect with bits changed in the second phase key.

For bit independence measurements, we selected 100 bit pairs, at random, from the encrypted amplitude image and calculated BIC for each of the pairs using Eq. 3 and the results were averaged from 100 measurements. Table 1 shows the bit independence results for the FT, FST, and LCT based DRPE system. As it can be seen from the Table 1, the bit

independence values for the DRPE systems, employed in this study, are far away from 1, meaning that the DRPE possess a satisfactory bit independence property. We note that the simulated avalanche effect and bit independence values are calculated by averaging 100 consecutive simulation results.

Table 1. Bit Independence Criterion (BIC) for DRPE in the Fourier, the Fresnel and the Linear Canonical domains.

DRPE system	Perturbed texts in	Bit Independence
FT based DRPE	Plaintext	0.46
	First Phase Key	0.49
	Second Phase Key	0.43
FST based DRPE	Plaintext	0.43
	First Phase Key	0.46
	Second Phase Key	0.42
LCT based DRPE	Plaintext	0.39
	First Phase Key	0.43
	Second Phase Key	0.35

5. CONCLUSION

We presented a method for calculating the avalanche effect and the bit independence property (which are common metrics used in evaluating the block cipher algorithms) on double random phase encryption (DRPE) system in the Fourier (FT), the Fresnel (FST) and the linear Canonical transformation (LCT) domains. Simulation results show that DRPE based LCT system achieves excellent performance in the sense of better avalanche effect and bit independence properties than that both of the Fourier and Fresnel domain based DRPE system. To be more precise, for the avalanche effect property, DRPE in the LCT and FST domains achieve superior results than that in the DRPE in the Fourier domain. Further, we note that, for the comparison purpose, in this work, the additional keys of the FST $(\text{i.e.}, \lambda, z_1, z_2)$ and the LCT based DRPE $(\text{i.e.}, \alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2, f_1, f_2)$ systems were not considered, however, these results will be reported in our future work. Furthermore, avalanche effect and the bit independence analysis will also be carried out on the Photon-counted imaging (PCI) based cryptosystems.

REFERENCES

[1] Alfalou, A., and Brosseau, C., "Optical image compression and encryption methods," Adv. Opt. Photon 1(3), 589-636 (2009).

[2] Liu, S., Guo, C., and Sheridan J. T., "A review of optical image encryption techniques," Opt Laser Technol 57, 327-342 (2014).

[3] Javidi, B., [Optical and digital techniques for information security], Springer, New York, 241-269 (2005).

[4] Refregier, P., and Javidi, B., "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett 20(7), 767-769 (1995).
[5] Unnikrishnan, G., Joseph, J., and Singh, K., "Optical encryption by double random phase encoding in the fractional Fourier domain," Opt. Lett 25(12), 887-889 (2000).
[6] Situ, G., and Zhang, J., "Double random phase encoding in the Fresnel domain," Opt. Lett 29(14), 1584-1586 (2004).
[7] Muniraj, I., Guo, C., Lee, B. G., and Sheridan, J. T, "Interferometry based multispectral photon-limited 2D and 3D integral image encryption employing the Hartley transform," Opt. Exp 23(12), 15907-15920 (2015).
[8] Guo, Q., Liu, Z., and Liu, S., "Color image encryption by using Arnold and discrete fractional random transforms in IHS space," Opt. Las. Engineering 48(12), 1174-1181 (2010).
[9] Carnicer, A., Usategui, M. M., Arcos, S., and Juvells, I., "Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett 30(13), 1644-1646 (2005).
[10] Gopinathan, U., Monaghan, D. S., Naughton, T. J., and Sheridan, J. T., "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Exp 14(8), 3181-3186 (2006).
[11] Liu, W., Yang, G., and Xie, H., "A hybrid heuristic algorithm to improve known plaintext attack on Fourier plane encryption," Opt. Exp 17(16), 13928-13938 (2009).
[12] Peng, X., Zhang, P., Wei, H., and Yu, B., "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett 31(8), 1044–1046 (2006).
[13] Zhao, L., Healy, J. J., and Sheridan, J. T., "Two-dimensional nonseparable linear canonical transform: sampling theorem and unitary discretization," J. Opt. Soc. Am. A 31(12), 2631-2641 (2014).
[14] Guo, C., Liu, S., and Sheridan, J. T., "Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems," Appl. Opt 54(15), 4709-4719 (2015).
[15] Guo, C., Muniraj, I., and Sheridan, J. T., "Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," Appl. Opt 55(17), 4720-4728 (2016).
[16] Unnikrishnan, G., and Singh, K., "Optical encryption using quadratic phase systems," Opt. Commun 193(1-6), 51-67 (2001).
[17] Stallings, W., [Cryptography and network security Principles and Practice], Prentice Hall, New York, Chapter 3, (2011).
[18] Tilborg, H.C.A.V., [Encyclopedia of cryptography and security], Springer, Netherlands, 598-602 (2005).
[19] Moon, I., Yi, F., Lee, Y. H., and Javidi, B., "Avalanche and bit independence characteristics of double random phase encoding in the Fourier and Fresnel domains," J. Opt. Soc. Am. A 31(5), 1104-1111 (2014).
[20] Muniraj, I., Kim, B., and Lee, B. G., "Encryption and volumetric 3D object reconstruction using multispectral computational integral imaging," Appl. Opt. 53(27), G25–G32 (2014).
[21] Goodman, J. W., [Introduction to Fourier Optics], the McGraw-Hill, Chapter 4 (1968).
[22] Healy, J. J., Kutay, M. A., Ozaktas, H. M., and Sheridan, J. T., [Linear Canonical Transforms Theory and Applications], Springer Series in Optical Sciences, 198 (2016).
[23] Feistel, H., "Cryptography and computer privacy," Sci. Am. 228, 15-23 (1973).
[24] Vergili, I., and Yücel, M. D., "Avalanche and bit independence properties for the ensembles of randomly chosen n×n S-boxes," Turk. J. Elec. Eng., 9(2), 137-146 (2001).
[25] Arumugam, G., Lakshmi Praba, and V., Radhakrishnan, S., "Study of chaos functions for their suitability in generating Message Authentication Codes," Appl. S. Comp 7(3), 1064-1071 (2007).
[26] Webster, A. F., and Tavares, S. E., "On the design of S-boxes," Advance in Cryptology: Proc.Crypto'85, Springer-Verlag, Berlin 218, 523-534 (1986).
[27] IEEE, "IEEE standard Floating-Point Arithmetic," IEEE. Std 754™-2008, 1-58 (2008).